

HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 7.50

Using System Availability Management

Document Number: BACSAM7.50/01

Document Release Date: May 2008

Software Release Date: May 2008



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Third-Party Web Sites

HP provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. HP makes no representations or warranties whatsoever as to site content or availability.

Copyright Notices

© Copyright 2005 - 2008 Mercury Interactive (Israel) Ltd.

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Pentium®, and Intel® Xeon™ are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows NT®, and Windows® XP are U.S registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

Support

You can visit the HP Software Support Web site at: **www.hp.com/go/hpsoftwaresupport**

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Table of Contents

Welcome to This Guide	21
How This Guide Is Organized	21
Who Should Read This Guide	23
Getting More Information	23

PART I: INTRODUCTION TO SITESCOPE

Chapter 1: Introducing SiteScope.....	27
SiteScope Overview	28
Key Features of SiteScope	29
SiteScope Architecture.....	30
SiteScope Monitoring Model.....	31
Setup and Administration	32
Configure SiteScope for Monitoring – Workflow	35
Configure a SiteScope Monitoring Solution Using a Template – Flowchart.....	38

PART II: SYSTEM AVAILABILITY MANAGEMENT

Chapter 2: System Availability Management Administration	41
System Availability Management Administration Overview.....	42
Understanding SiteScope Integration with HP Business Availability Center.....	44
Integrating SiteScope Data with HP Business Availability Center's Configuration Items.....	47
Reporting Discovered Topologies to HP Business Availability Center	50
Accessing SiteScope and Building Permissions Model.....	51
Collect Data on the Performance of an IT Resource.....	53
System Availability Management Administration User Interface	56
Troubleshooting and Limitations	77

Chapter 3: Monitor Deployment Wizard Concepts and Tasks	81
Monitor Deployment Wizard Overview	82
Prerequisites for Running the Monitor Deployment Wizard	84
Monitor Deployment Wizard Templates and Variables	85
Full and Partial Monitor Coverage	87
Wizard Options	88
Monitor Deployment Wizard for Siebel.....	89
Deploy Monitors Using the Monitor Deployment Wizard	90
Template Reference	96
Monitor Deployment Wizard User Interface	104
Chapter 4: Introduction to System Availability Management Reports	113
System Availability Management Reports Overview	113
Working with System Availability Management Reports.....	116
Chapter 5: SiteScope Over Time Reports	119
Understanding SiteScope Over Time Reports	120
Monitor Performance Report	123
Cross-Performance Report.....	126
Adjusting the Cross-Performance Report Scale.....	138
Group Performance Report	139
Status Summary Report	143
Warning Summary Report	144
Error Summary Report.....	146
System Availability Management Data in Custom Reports.....	147
Chapter 6: The Event Log	151
Event Log Overview	152
Display and Customize the Event Log.....	153
Set Additional Filters for SiteScope	155
Viewing Common Event Data in the Event Log Page.....	156
Working with Event Details.....	158
Working with Event History	160

PART III: GENERAL AND ADMINISTRATION

Chapter 7: SiteScope Monitor Tree	165
SiteScope Monitor Tree Overview	166
SiteScope Monitors and HP Business Availability Center Configuration Items.....	166
Copying and Moving SiteScope Objects	168
Navigating and Performing Actions in the Contents Tab and the Monitor Tree.....	170
Monitor Tree User Interface	170
Chapter 8: Views and Categories.....	195
Views and Categories Overview	195
Defining and Managing View Settings	196
Working with Categories	197
Create and Define a New Category	198
Views and Categories User Interface	200
Chapter 9: Preferences.....	207
Preferences Overview	209
General Preferences	211
Infrastructure Settings Preferences	216
Integration Preferences.....	216
Failover Preferences	219
Microsoft Windows Remote Preferences.....	219
UNIX Remote Preferences	220
Log Preferences	221
E-mail Preferences	222
Pager Preferences	222
SNMP Trap Preferences.....	223
Absolute Schedule Preferences	224
Range Schedule Preferences	225
User Preferences.....	226
Credential Preferences.....	229
Configure SiteScope for a Non-English Locale.....	231
Configure SiteScope-HP Business Availability Center Integration Preferences	234
Configure SiteScope to Monitor a Remote Windows Server	236
Configure Credential Preferences.....	243
Monitors Tested for Internationalization	244
SiteScope Log Database Table Structure.....	246
Password Requirement Parameters.....	247
Preferences User Interface	247
Troubleshooting and Limitations	334

Chapter 10: Global Search and Replace	343
Global Search and Replace Overview	343
Perform a Global Search and Replace	345
Global Search and Replace User Interface.....	350
Chapter 11: SiteScope Server Health.....	365
SiteScope Health Overview.....	366
SiteScope Health Group	366
BAC Integration Statistics Monitor	367
SiteScope Log Events Monitor.....	368
SiteScope Monitor Load Monitor	370
SiteScope Server Health Monitor.....	370
Using Log Files.....	371
Using the Audit Log	372
Using the SiteScope Progress Report	373
Analyze SiteScope Health Monitor Data	376
Configure the Audit Log	382
SiteScope Log File Columns	383
Audit Log Entries	384
SiteScope Health User Interface	394
Troubleshooting and Limitations	409

PART IV: SITESCOPE DASHBOARD

Chapter 12: Working with SiteScope Dashboard.....	413
SiteScope Dashboard Overview	414
Dashboard Filter Overview.....	415
Generating a Server-Centric Report	416
Acknowledging Monitor Status.....	417
Accessing SiteScope Tools	418
Customize SiteScope Dashboard	419
Analyze Data in SiteScope Dashboard	421
Monitor Your Microsoft Windows/UNIX Server's Resources	424
Create a Server-Centric Report – Scenario.....	426
Server-Centric Report Measurements.....	429
SiteScope Dashboard User Interface.....	430

PART V: MONITORS

Chapter 13: Working with SiteScope Groups.....	457
SiteScope Groups Overview.....	457
Manage a Group – Workflow	460
New SiteScope Group Page.....	462

Chapter 14: Working with SiteScope Monitors	467
SiteScope Monitors Overview.....	468
SiteScope Monitor Categories.....	469
Monitoring Remote Servers.....	471
Monitoring Group Dependencies	473
Setting Status Thresholds	476
Setting Status Thresholds Using a Baseline.....	478
Deploy a Monitor – Workflow	489
Set Monitor Thresholds Using a Baseline.....	493
Monitors Supported in Windows Environments Only.....	501
Ports Used for SiteScope Monitoring	503
SiteScope Monitors User Interface	507

Chapter 15: Application Monitors	549
Active Directory Replication Monitor Overview	551
ASP Server Monitor Overview	552
Apache Server Monitor Overview	553
BroadVision Application Server Monitor Overview	554
Check Point Firewall-1 Monitor Overview	554
Cisco Works Monitor Overview	555
Citrix Server Monitor Overview	555
ColdFusion Server Monitor Overview	558
COM+ Server Monitor Overview	559
Dynamo Application Server Monitor Overview	561
F5 Big-IP Monitor Overview	561
IIS Server Monitor Overview	562
iPlanet Server Monitor Overview	563
Microsoft Exchange 2003 Mailbox Monitor Overview	566
Microsoft Exchange 2003 Public Folder Monitor Overview	567
Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Overview	568
Microsoft Exchange 2007 Monitor Overview	569
Microsoft Exchange 5.5 Message Traffic Monitor Overview	574
News Monitor Overview	575
Oracle 9i Application Server Monitor Overview	576
Oracle 10g Application Server Monitor Overview	577
Radius Monitor Overview	578
SAP CCMS Monitor Overview	579
SAP CCMS Alerts Monitor Overview	585
SAP Java Web Application Server Monitor Overview	588
SAP Performance Monitor Overview	590
SAP Work Processes Monitor Overview	592
Siebel Application Server Monitor Overview	597
Siebel Log File Monitor Overview	601
Siebel Web Server Monitor Overview	602
SilverStream Server Monitor Overview	604
SunONE Server Monitor Overview	605
Tuxedo Monitor Overview	606
UDDI Monitor Overview	607
VMware Performance Monitor Overview	608
WebLogic Application Server Monitor Overview	610
WebSphere Application Server Monitor Overview	613
WebSphere MQ Status Monitor Overview	617
WebSphere Performance Servlet Monitor Overview	622
Application Monitors User Interface	623

Chapter 16: Database Monitors	723
DB2 Monitor Overview	723
DB2 8.x Monitor Overview	725
Database Counter Monitor Overview	726
Database Query Monitor Overview.....	729
LDAP Monitor Overview	738
Microsoft SQL Server Monitor Overview	739
Oracle Database Monitor Overview	740
Sybase Monitor Overview.....	742
Database Monitors User Interface Settings	743
Chapter 17: Generic Monitors	773
Composite Monitor Overview.....	774
Directory Monitor Overview	774
File Monitor Overview	775
JMX Monitor Overview	776
Log File Monitor Overview.....	779
Script Monitor Overview	781
Web Service Monitor Overview	787
XML Metrics Monitor Overview	791
Generic Monitors User Interface	792
Chapter 18: Network Monitors	823
DHCP Monitor Overview	824
DNS Monitor Overview	825
FTP Monitor Overview	826
Formula Composite Monitor Overview	828
MAPI Monitor Overview	830
Mail Monitor Overview.....	834
Microsoft Windows Dial-up Monitor Overview	834
Network Bandwidth Monitor Overview	837
Ping Monitor Overview.....	838
Port Monitor Overview	839
RTSP Monitor Overview	840
SNMP Monitor Overview	844
SNMP Trap Monitor Overview.....	845
SNMP by MIB Monitor Overview.....	846
Network Monitors User Interface.....	849

Chapter 19: Server Monitors	891
Browsable Windows Performance Counter Monitor	
Overview	892
CPU Utilization Monitor Overview	893
Disk Space Monitor Overview	894
IPMI Monitor Overview	894
Memory Monitor Overview	895
Microsoft Windows Event Log Monitor Overview	897
Microsoft Windows Performance Counter Monitor	
Overview	898
Microsoft Windows Resources Monitor Overview.....	899
Microsoft Windows Services State Monitor Overview.....	903
Service Monitor Overview.....	904
UNIX Resources Monitor Overview	906
Web Server Monitor Overview	906
Server Monitors User Interface.....	907
Chapter 20: Stream Monitors	941
Microsoft Windows Media Player Monitor Overview	942
Microsoft Windows Media Server Monitor Overview	943
Real Media Player Monitor Overview	944
Real Media Server Monitor Overview	944
Stream Monitors User Interface	945
Chapter 21: Web Transaction Monitors	957
eBusiness Transaction Monitor Overview.....	958
Link Check Monitor Overview.....	960
URL Monitor Overview	961
URL Content Monitor Overview.....	965
URL List Monitor Overview	968
URL Sequence Monitor Overview	971
Web Script Monitor Overview	984
Create a URL Sequence.....	994
Web Transaction Monitors User Interface.....	996

PART VI: INTEGRATION MONITORS

Chapter 22: Working with SiteScope Integration	
Monitors	1045
Integration Monitors Overview	1046
Topology Settings.....	1049
Deploy Integration Monitors	1055
List of Deprecated Integration Monitors.....	1057
Troubleshooting and Limitations	1059

Chapter 23: HP OVO Event Monitor	1063
HP OVO Event Monitor Overview	1064
HP OVO Integration Add-on – Workflow	1067
HP OVO Event Monitor User Interface	1075
Chapter 24: HP ServiceCenter Monitor	1079
HP ServiceCenter Monitor Overview	1080
HP ServiceCenter Integration – Workflow	1081
HP ServiceCenter Monitor User Interface	1084
Chapter 25: NetScout Event Monitor	1089
NetScout Event Monitor Overview	1090
System Requirements	1091
NetScout Integration – Workflow	1092
NetScout Event Monitor User Interface	1093
Chapter 26: Technology Database Integration Monitor	1097
Technology Database Integration Monitor Overview	1098
Setup Requirements	1099
Integrate Database Data into HP Business Availability Center	1102
Technology Database Integration Monitor User Interface	1105
Troubleshooting and Limitations	1114
Chapter 27: Technology Log File Integration Monitor	1115
Technology Log File Integration Monitor Overview	1116
Setup Requirements	1117
Integrate Log File Data into HP Business Availability Center	1118
Technology Log File Integration Monitor User Interface	1120
Troubleshooting and Limitations	1129
Chapter 28: Technology SNMP Trap Integration Monitor	1131
Technology SNMP Trap Integration Monitor Overview	1132
Setup Requirements	1133
Integrate SNMP Trap Data into HP Business Availability Center	1134
Technology SNMP Trap Integration Monitor Settings	1136
Troubleshooting and Limitations	1142

Chapter 29: Technology Web Service Integration Monitor	1145
Technology Web Service Integration Monitor Overview	1146
Setup Requirements.....	1147
Check Connectivity to the Technology Web Service	
Integration Monitor.....	1149
Technology Web Service Integration Monitor Settings.....	1150
Troubleshooting and Limitations	1156
Chapter 30: Integration with HP Network Node Manager	1157
Network Node Manager Integration Overview.....	1157
Writing Scripts to Export Network Node Manager Data	1158
Configure Events in Network Node Manager	1159
Chapter 31: Integration Monitor Field Mapping	1161
Integration Monitor Field Mapping Overview	1162
Understanding Field Mapping Structure.....	1163
Configuring Field Mapping for Event Samples.....	1164
Configuring Field Mapping for Measurement Samples.....	1170
Configuring Field Mapping for Ticket Samples	1173
Event Handler Structure	1177

PART VII: TEMPLATES

Chapter 32: SiteScope Templates	1189
SiteScope Templates Overview	1190
Understanding Templates	1192
Template Examples	1194
Planning Templates.....	1195
Working with Template Variables	1197
Counter Selection in Monitor Templates	1202
Updating Template Deployments.....	1206
Configure a SiteScope Monitoring Solution Using a	
Template – Workflow.....	1208
Publish Template Updates to Related Group Deployments	1218
Modify Counter Selection Strings to Use Regular	
Expressions.....	1221
Export and Import a Template.....	1222
Reserved Template Group Types.....	1223
SiteScope Templates User Interface.....	1223

Chapter 33: Auto Template Deployment	1253
Auto Template Deployment Overview	1254
Creating and Working with the XML File	1254
XML File Example and Variables	1255
XML Validator	1259
Publishing Template Changes Using the XML	1259
Deployment Results.....	1262
Deploy a Monitoring Structure Using an XML File	1262
Encrypt Text	1266
Update a Deployment	1267
XML Tag Reference.....	1269
Troubleshooting and Limitations	1272
Chapter 34: SiteScope Solution Templates	1273
Solution Templates Overview	1273
Deploy a SiteScope Solution Template – Workflow.....	1276
Troubleshooting and Limitations	1278
Chapter 35: Active Directory Solution Template.....	1279
Active Directory Solution Overview.....	1279
Deploy the Active Directory Solution Template	1281
Active Directory Solution Template User Interface	1282
Chapter 36: AIX Host Solution Templates	1285
AIX Host Solution Overview	1285
Deploy the AIX Host Solution Template	1287
AIX Host Solution Configuration Requirements	1288
AIX Host Solution Template User Interface	1288
Chapter 37: JBoss Application Server Solution Template.....	1291
JBoss Application Server Solution Overview	1292
Deploy the JBoss Application Server Solution Template	1293
JBoss Solution Configuration Requirements.....	1294
JBoss Solution Template User Interface	1295
Chapter 38: Linux Host Solution Templates	1299
Linux Host Solution Overview	1299
Deploy the Linux Host Solution Template	1301
Linux Host Solution Configuration Requirements.....	1302
Linux Host Solution Template User Interface.....	1302

Chapter 39: Microsoft Exchange Solution Templates	1305
Microsoft Exchange Solution Overview	1306
Deploy Microsoft Exchange Solution Templates	1308
Microsoft Exchange Solution Configuration Requirements	1309
Microsoft Exchange Solution Template User Interface	1310
Chapter 40: Microsoft IIS Solution Template	1313
Microsoft IIS 6 Solution Overview	1314
Deploy the Microsoft IIS Solution Template	1315
Microsoft IIS Solution Configuration Requirements	1316
Microsoft IIS Solution Template User Interface	1316
Chapter 41: Microsoft SQL Server Solution Template	1319
Microsoft SQL Server Solution Overview	1319
Deploy the Microsoft SQL Server 2005 Solution Template	1321
Microsoft SQL Server Solution Configuration Requirements	1322
Microsoft SQL Server 2005 Solution Template User Interface	1323
Chapter 42: Microsoft Windows Host Solution Template	1325
Microsoft Windows Host Solution Overview	1325
Deploy the Microsoft Windows Host Solution Template	1327
Microsoft Windows Host Solution Configuration Requirements	1328
Microsoft Windows Host Solution Template User Interface	1329
Chapter 43: .NET Solution Templates	1331
.NET Solution Overview	1331
Deploy the .NET Solution Template	1333
.NET Solution Configuration Requirements	1334
.NET Solution Template User Interface	1334
Chapter 44: Oracle Database Solution Template	1337
Oracle Database Solution Overview	1338
Deploy Oracle Database Solution Templates	1340
Oracle Database Solution Template Usage Guidelines	1341
Oracle Database Solution Template Tools	1341
Oracle Solution Template User Interface	1344

Chapter 45: SAP Solution Templates	1347
SAP Solution Overview	1348
Deploy the SAP Solution Template	1349
SAP Solution Template Configuration Requirements.....	1350
SAP Solution Template User Interface.....	1351
Chapter 46: Siebel Solution Templates.....	1353
Siebel Solution Overview.....	1354
Deploy the Siebel Solution Template.....	1356
Siebel Solution Configuration Requirements	1357
Siebel Solution Template User Interface	1358
Chapter 47: Solaris Host Solution Templates	1363
Solaris Host Solution Overview	1363
Deploy the Solaris Host Solution Template	1365
Solaris Host Solution Configuration Requirements.....	1366
Solaris Host Solution Template User Interface.....	1366
Chapter 48: WebLogic Solution Template.....	1369
WebLogic Solution Overview.....	1369
Deploy the WebLogic Solution Template	1371
WebLogic Solution Usage Guidelines	1372
Selecting WebLogic Modules for Monitoring	1372
WebLogic Solution Template User Interface.....	1374
Chapter 49: WebSphere Solution Template.....	1377
WebSphere Solution Overview.....	1377
Deploy the WebSphere Solution Template.....	1379
WebSphere Solution Template User Interface	1380

PART VIII: ALERTS AND REPORTS

Chapter 50: SiteScope Alerts 1385
SiteScope Alerts Overview 1386
Creating Alert Actions 1389
Understanding When SiteScope Alerts Are Sent 1390
Customizing Alert Templates 1394
Working with Database Alerts 1396
Working with Disable or Enable Monitor Alerts 1397
Working with E-Mail Alerts 1398
Working with Log Event Alerts 1399
Working with Pager Alerts 1400
Working with Post Alerts 1401
Working with Script Alerts 1402
Working with SMS Alerts 1406
Working with SNMP Trap Alerts 1407
Working with Sound Alerts 1408
Configure an Alert 1409
Customize an Alert’s Message Content 1411
Customize Alert Template Tag Styles 1413
SiteScope Alert Templates Directory 1414
SiteScope Alerts User Interface 1414

Chapter 51: SiteScope Reports 1439
SiteScope Reports Overview 1439
SiteScope Report Types 1441
Working with SiteScope Management Reports 1443
Create a Report 1444
SiteScope Reports User Interface 1446

PART IX: ADVANCED INFORMATION

Chapter 52: Using Regular Expressions 1493
Regular Expressions Overview 1494
Defining a Regular Expression 1495
Matching String Literals 1497
Matching Patterns with Metacharacters 1499
Search Mode Modifiers 1503
Retaining Content Match Values 1505
SiteScope Date Variables 1506
Examples for Log File Monitoring 1511
Problems Working with Regular Expressions 1516

Chapter 53: Monitoring XML Documents	1519
Monitoring XML Documents Overview	1519
Content Matching for XML Documents.....	1520
Using XML Content Match Values in Monitor Configurations	1522
Chapter 54: Writing Scripts for Script Alerts.....	1523
Writing Scripts for Script Alerts Overview	1523
Working with Scripts in SiteScope	1524
Passing Data from SiteScope to a Script	1526
Chapter 55: UNIX Operating System Adapters	1529
SiteScope UNIX Operating System Adapters Overview	1530
Add an Adapter.....	1530
UNIX Adapters Provided with SiteScope.....	1531
Adapter File Format	1532
Adapter Command List	1534
Chapter 56: SiteScope Monitoring Using Secure Shell (SSH)	1541
SiteScope and SSH Overview	1542
Configuring Remote Windows Servers for SSH Monitoring.....	1545
Configure Remote UNIX Servers for SSH monitoring	1546
Configure Remote Windows Servers for SSH monitoring	1549
Chapter 57: Working with SSH Clients.....	1563
Integrated Java SSH Client Overview	1564
External SSH Client Overview	1566
Configure the Integrated Java SSH Client.....	1569
Configure the External SSH Client.....	1572
Chapter 58: Creating Custom Properties	1581
Custom SiteScope Properties Overview.....	1582
Working with Custom Monitor Properties.....	1582
Working with Custom Display Columns.....	1584
Displaying Custom Properties in Custom Columns.....	1585
Create Custom Properties.....	1585
Custom Monitor Property and Column Definition Syntax	1590
Chapter 59: Tools for Troubleshooting	1593
SiteScope Tools Overview.....	1593
SiteScope Tools User Interface.....	1597

Table of Contents

Welcome to This Guide

This guide describes how to use the System Availability Management application to monitor the enterprise IT infrastructure.

This chapter includes:

- ▶ How This Guide Is Organized on page 21
- ▶ Who Should Read This Guide on page 23
- ▶ Getting More Information on page 23

How This Guide Is Organized

The guide contains the following parts:

Part I Introduction to SiteScope

Introduces SiteScope and provides an overview of the SiteScope key features, architecture, and monitoring model. In addition, it describes a working order for using SiteScope to monitor your organization's IT infrastructure.

Part II System Availability Management

Describes how to use System Availability Management Administration from within HP Business Availability Center to register, configure, and maintain multiple SiteScopes. It also describes using the Monitor Deployment Wizard and System Availability Management reports.

Part III General and Administration

Describes the SiteScope's general and administrative functions, including the monitor tree, preferences, Views and Categories, and the Global Search and Replace Wizard.

Part IV SiteScope Dashboard

Describes how to use the SiteScope Dashboard tab to view the latest real-time monitor data and to customize the display of monitor results.

Part V Monitors

Describes how to configure each type of SiteScope monitor.

Part VI Integration Monitors

Describes how to configure each type of integration monitor, including troubleshooting issues relating to monitoring EMS environments with SiteScope.

Part VII Templates

Describes how to use templates to efficiently deploy, maintain, and update monitoring solutions, including groups, monitors, remote servers, and alerts. It also describes deploying SiteScope monitoring for commonly used IT applications using solution templates.

Part VIII Alerts and Reports

Describes how to use SiteScope Alerts to send notifications of an event or change of status in your infrastructure, and how to create SiteScope Reports to define the monitor parameters, time interval, or summary data you want to measure.

Part IX Advanced Information

Describes how to use regular expressions, monitor XML documents, write script alerts, customize alert templates, create and customize adapter files for UNIX monitoring, use Secure Shell (SSH) connection for remote server monitoring, configure clients working with SSH, customize monitor properties, and use SiteScope tools to troubleshoot and diagnose resource and monitor configuration problems.

Who Should Read This Guide

This guide is intended for the following users of HP Business Availability Center:

- ▶ HP Business Availability Center administrators
- ▶ HP Business Availability Center application administrators
- ▶ HP Business Availability Center data collector administrators
- ▶ HP Business Availability Center end users

Readers of this guide should be knowledgeable about enterprise system administration, infrastructure monitoring systems, and SiteScope, and have familiarity with the systems being set up for monitoring. In addition, readers who are integrating with HP Business Availability Center should be familiar with HP Business Availability Center and enterprise monitoring and management concepts.

Getting More Information

For a complete list of all online documentation included with HP Business Availability Center, additional online resources, information on acquiring documentation updates, and typographical conventions used in this guide, see the *HP Business Availability Center Deployment Guide* PDF.

Welcome to This Guide

Part I

Introduction to SiteScope

1

Introducing SiteScope

This chapter introduces the SiteScope monitoring model.

This chapter includes:

Concepts

- ▶ SiteScope Overview on page 28
- ▶ Key Features of SiteScope on page 29
- ▶ SiteScope Architecture on page 30
- ▶ SiteScope Monitoring Model on page 31

Tasks

- ▶ Setup and Administration on page 32
- ▶ Configure SiteScope for Monitoring – Workflow on page 35
- ▶ Configure a SiteScope Monitoring Solution Using a Template – Flowchart on page 38

SiteScope Overview

HP SiteScope is an agentless monitoring solution designed to ensure the availability and performance of distributed IT infrastructures—for example, servers, operating systems, network devices, network services, applications, and application components. This Web-based infrastructure monitoring solution is lightweight, highly customizable, and does not require that data collection agents be installed on your production systems.

SiteScope has over 90 types of monitors that can monitor utilization, response time, usage, and resource availability of a variety of host types and application platforms. SiteScope can be configured to alert whenever it detects a problem in the IT infrastructure. There are several types of alert actions, such as sending e-mail messages, paging, sending Simple Network Management Protocol (SNMP) traps, or executing a script.

You can create a report for a single monitor, several monitors, or even several monitor groups. SiteScope reports display information about how the servers and applications you are monitoring have performed over time. SiteScope reports are important tools in monitoring and troubleshooting operational performance and availability and reviewing the monitored environment.

SiteScope provides different tools, such as templates, the Publish Template Changes wizard, and automatic template deployment that enable you to develop a standardized set of monitor types and configurations into a single structure. SiteScope templates can be speedily deployed across the enterprise and quickly updated to ensure that the monitoring infrastructure is compliant with the standards set in the template. SiteScope also includes alert types that you can use to communicate and record event information in a variety of media. You can customize alert templates to meet the needs of your organization.

SiteScope monitors key aspects of its own operability and identifies monitor configuration problems and critical server load. It also monitors its own integration and data events when configured to report to HP Business Availability Center.

Key Features of SiteScope

SiteScope has the following features:

- ▶ **Agentless monitoring.** SiteScope monitors without the deployment of agent software on the servers to be monitored. This function makes deployment and maintenance of SiteScope relatively simple compared to other performance monitoring solutions.
- ▶ **Enterprise-ready architecture.** SiteScope provides failover capabilities, simultaneous monitoring of large number of systems, and support for secure connections.
- ▶ **Simple installation and deployment.** SiteScope is installed on a single server running as a service or a process. This results in quick installation and easy monitoring configuration.
- ▶ **Infrastructure performance and availability monitoring.** SiteScope has over 90 types of monitors. SiteScope can monitor utilization, response time, usage, and resource availability of a variety of host types and application platforms.
- ▶ **Standardized monitor deployments and updates using templates.** SiteScope templates, the Publish Template Changes wizard, and automatic template deployment provide an enterprise solution for standardizing the monitoring of the different IT elements in your enterprise. Templates speed the deployment of monitors across the enterprise through the single-operation deployment of groups, monitors, alerts, remote servers, and configuration settings in a single structure that can be repeatedly deployed and updated.
- ▶ **Proactive alerting.** SiteScope can be configured to alert whenever it detects a problem in the IT infrastructure. There are several types of alert actions, such as sending e-mail messages, paging, sending Simple Network Management Protocol (SNMP) traps, or executing a script.
- ▶ **Self-monitoring.** SiteScope monitors key aspects of its own operability and identifies monitor configuration problems and critical server load. It also monitors its own integration and data events when configured to report to HP Business Availability Center.

- ▶ **Customization capabilities.** SiteScope allows for display of customizations of groups and monitors by using custom data fields and HTML-sensitive description tags. In addition, SiteScope allows for the customization of alert text and report configurations by using templates and user-defined variables.
- ▶ **Intuitive administration.** SiteScope reduces the time spent managing a monitoring environment by providing a user friendly browser-based interface for viewing and administering of the monitoring platform.

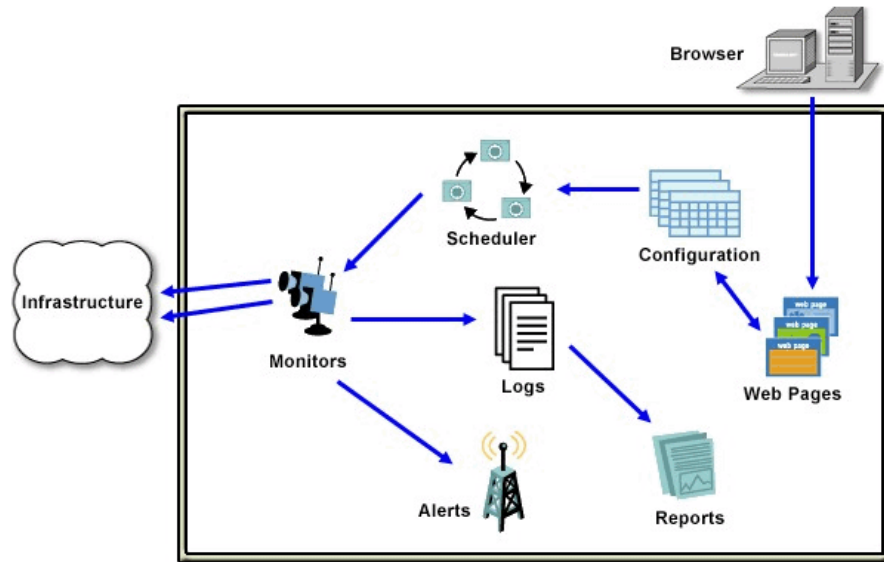
SiteScope Architecture

SiteScope's Web-enabled architecture allows for the creation and ongoing administration of a scalable monitoring environment. It consists of the following components:

- ▶ **Browser-based interface.** Manages end user status information requests, configuration change requests, and access control.
- ▶ **Scheduler.** Coordinates the running of monitors, alert creation, and report generation.
- ▶ **Monitors.** Collect performance and availability information about the system being monitored.
- ▶ **Alerts.** Notifications of exceptions, failures, and status change events in the system being monitored.
- ▶ **Reports.** A historical representation of monitored data for trending and analysis purposes.

SiteScope Monitoring Model

The SiteScope monitoring model is displayed in the diagram below.



SiteScope architecture is comprised of the following key components:

- ▶ **Groups.** A group is a container for monitoring assets. Groups may contain subgroups and are used to organize monitors. Groups are created prior to monitors.
- ▶ **Monitors.** A monitor checks the status of server components, key application processes, log files, or network devices, to name a few. It collects data based on selected metrics and displays a status of good, warning, or error with respect to the configured thresholds.
- ▶ **Alerts.** An alert is an action triggered by a change in the status of a monitored asset. Alerts notify required users when negative events or failures occur. An alert can be sent to a variety of media including e-mail, pager, Short Message Service (SMS) messages, or an SNMP trap.

- ▶ **Reports.** A report is a historical representation of monitored data. SiteScope offers a variety of reports from quick monitor reports to detailed management reports. Reports enable you to track trends and operational performance and to troubleshoot problems.

Setup and Administration

This task describes a suggested working order for preparing to use SiteScope.

This task includes the following steps:

- ▶ “Log in to SiteScope” on page 32
- ▶ “Enter your SiteScope License” on page 32
- ▶ “Configure the SiteScope Restart Schedule” on page 33
- ▶ “Create a SiteScope User Account” on page 33
- ▶ “Configure the SiteScope E-mail Preferences Server” on page 33
- ▶ “Adjust Log Preferences” on page 33
- ▶ “Install Middleware Drivers” on page 34
- ▶ “Configure SiteScope to Report to HP Business Availability Center” on page 34
- ▶ “Configure Connection Profiles for Remote Servers” on page 34
- ▶ “Configure Credential Preferences” on page 34
- ▶ “Results” on page 34

1 Log in to SiteScope

Type the SiteScope address in a Web browser. The default address is:
`http://localhost:8080/SiteScope.`

2 Enter your SiteScope License

If you did not enter your SiteScope license information during installation, enter it in the General Preferences page. For details on the user interface, see “License Number” on page 249.

3 Configure the SiteScope Restart Schedule

Restarting the SiteScope server is necessary for clearing problems and resetting monitors. You can select a schedule used for restarting SiteScope in the General Preferences page. Selecting a convenient restart schedule helps minimize or avoid gaps in monitoring coverage and data. For details on the user interface, see “SiteScope restart schedule” on page 252.

4 Create a SiteScope User Account

The Administrator Account is the default account that is active when the product is installed. It has full privileges to manage SiteScope and is the account that all users who access the product use unless you restrict the account. Create and configure other user accounts based on the requirements of the organization. For details on this topic, see “User Preferences” on page 226.

Note: If no user name and password are defined for the administrator user, SiteScope skips the Login page and automatically logs in.

5 Configure the SiteScope E-mail Preferences Server

Configure the SiteScope E-mail Preferences e-mail server with an administrator's e-mail address and specify a mail server that SiteScope can use to forward e-mail messages and alerts to users. For details on the user interface, see “E-mail Preferences” on page 222.

6 Adjust Log Preferences

If necessary, adjust Log Preferences to set the number of days of monitor data that are retained on the SiteScope server. By default, SiteScope deletes logs older than 40 days. If you plan to have monitor data exported to an external database, prepare the database, the necessary drivers, and configure the Log Preferences as applicable. For details on the user interface, see “Log Preferences” on page 221.

7 Install Middleware Drivers

Install middleware drivers for connectivity with remote databases and applications for those monitors that require drivers. For details, see the help for the specific monitor.

8 Configure SiteScope to Report to HP Business Availability Center

To enable logging of SiteScope monitor data to Business Availability Center, configure SiteScope to report to HP Business Availability Center. For details on this topic, see “Integration Preferences” on page 216.

9 Configure Connection Profiles for Remote Servers

Specify the connection method for the remote servers you want to monitor in accordance with your security requirements. For details on enabling SiteScope to monitor data on remote Windows servers, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236. For details on enabling SiteScope to monitor data on remote UNIX servers, see “UNIX Remote Preferences” on page 220.

10 Configure Credential Preferences

Configure and manage credentials for SiteScope resources in a centralized location, and have SiteScope automatically supply that information when you configure those resources using Credential Preferences. For details on this topic, see “Configure Credential Preferences” on page 243.

11 Results

You are now ready to use SiteScope.

- ▶ For a workflow on creating a basic monitoring structure in SiteScope, see “Configure SiteScope for Monitoring – Workflow” on page 35.
- ▶ For a workflow on how to create and develop templates to help speed the deployment of monitoring using standardized group structure, naming conventions, and configuration settings, see “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208.

Configure SiteScope for Monitoring – Workflow

This task describes the working order for creating a basic monitoring structure in SiteScope.

Note: It is more efficient to use SiteScope templates, the Publish Template Changes wizard, and automatic template deployment for standardizing the monitoring of the different IT elements in your enterprise. For a flowchart that shows the steps involved in configuring a monitoring solution using a template, see “Configure a SiteScope Monitoring Solution Using a Template – Flowchart” on page 38. For details on the workflow, see “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208.

This task includes the following steps:

- “Prerequisites” on page 36
- “Create a Group” on page 36
- “Create Monitor Instances” on page 36
- “Set Monitor Thresholds” on page 36
- “Set Monitor Dependencies” on page 36
- “Set Up Monitor and Group Alerts” on page 37
- “Set Up Monitor and Group Reports” on page 37
- “Results” on page 37

1 Prerequisites

Check that the post-installation administration tasks have been performed before configuring SiteScope for monitoring. For details on how to perform this task, see “Setup and Administration” on page 32.

2 Create a Group

Create group containers to make deployment of monitors and associated alerts manageable and effective for your environment and organization. For details on how to perform this task, see “Manage a Group – Workflow” on page 460.

3 Create Monitor Instances

Select the monitor instances you want to add to the group. For details on how to perform this task, see “Deploy a Monitor – Workflow” on page 489.

4 Set Monitor Thresholds

Set thresholds for one or multiple monitors using a baseline, or manually set logic conditions that determine the reported status of each monitor instance.

- ▶ For details on how to set monitor thresholds using a baseline, see “Set Monitor Thresholds Using a Baseline” on page 493.
- ▶ For details on how to set monitor thresholds manually, see “Threshold Settings” on page 518.

5 Set Monitor Dependencies

Build dependencies between groups and key monitors to help control redundant alerting. For details on this topic, see “Monitoring Group Dependencies” on page 473.

6 Set Up Monitor and Group Alerts

Create alerts to send notification of an event or change of status in some element or system in your infrastructure. For details on how to configure alerts, see “Configure an Alert” on page 1409.

7 Set Up Monitor and Group Reports

Create reports to display information about how the servers and applications you are monitoring have performed over time. For details on how to create reports, see “Create a Report” on page 1444.

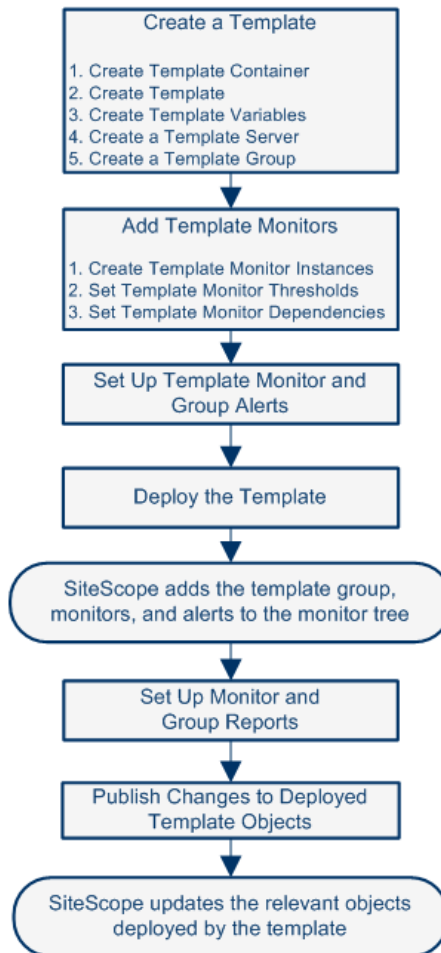
8 Results

SiteScope adds the monitors, alerts, and reports to the specified container in the monitor tree.

Configure a SiteScope Monitoring Solution Using a Template – Flowchart

The flowchart below shows the steps required to configure a SiteScope monitoring solution using SiteScope templates and the Publish Template Changes wizard. Templates are used to standardize a set of group structures, monitor types and configuration settings into a single structure that can be repeatedly deployed and updated.

For details on the workflow, see “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208.



Part II

System Availability Management

2

System Availability Management Administration

This chapter includes the main concepts, tasks, and reference information for System Availability Management Administration.

This chapter includes:

Concepts

- ▶ System Availability Management Administration Overview on page 42
- ▶ Understanding SiteScope Integration with HP Business Availability Center on page 44
- ▶ Integrating SiteScope Data with HP Business Availability Center's Configuration Items on page 47
- ▶ Reporting Discovered Topologies to HP Business Availability Center on page 50
- ▶ Accessing SiteScope and Building Permissions Model on page 51

Tasks

- ▶ Collect Data on the Performance of an IT Resource on page 53

Reference

- ▶ System Availability Management Administration User Interface on page 56

Troubleshooting and Limitations on page 77

System Availability Management Administration Overview

You install SiteScope on designated host machines with access to the applications and operating systems to be monitored. SiteScope collects key performance measurements on a wide range of back- and front-end infrastructure components, including Web, application, database, and firewall servers.

SiteScope can be accessed as a standalone application or using System Availability Management Administration from within HP Business Availability Center. (Windows-based and Solaris-based SiteScope installations both work with Windows-based or Solaris-based HP Business Availability Center servers.)

System Availability Management enables you to register, configure and maintain your SiteScope Servers. You can configure and manage multiple SiteScopes from within HP Business Availability Center. The System Availability Management Administration interface enables you to configure SiteScope monitors, alerts, and reports and to make any other configuration changes for the SiteScope. All the configuration changes that are done from HP Business Availability Center are reflected in the SiteScope itself.

System Availability Management enables you to:

- ▶ Add SiteScopes to System Availability Management Administration. For details on the user interface, see “New SiteScope Page” on page 65.
- ▶ Copy group, monitor, report, and alert instances from one SiteScope to another SiteScope using copy/paste. For details on this topic, see “Copying and Moving SiteScope Objects” on page 168.
- ▶ Synchronize a SiteScope’s settings with another SiteScope by copying settings, preferences, and template files using the Sync SiteScope wizard. For details on the user interface, see “Sync SiteScopes Wizard - Select Source and Targets Page” on page 71.
- ▶ Perform a Global Replace operation across multiple SiteScopes. For details on the user interface, see “Global Search and Replace Wizard” on page 351.

- View accessibility information and summary information regarding registration status of the SiteScope to Business Availability Center, licence points, sample reporting rates, monitor run rates and health of the SiteScopes. For details on the user interface, see “System Availability Management Administration” on page 57.
- Run the Monitor Deployment Wizard to deploy monitors onto configuration items in Business Availability Center’s CMDB. (This feature is not available to users accessing SiteScope from HP Operations Manager.) For details on this topic, see “Monitor Deployment Wizard Concepts and Tasks” on page 81.

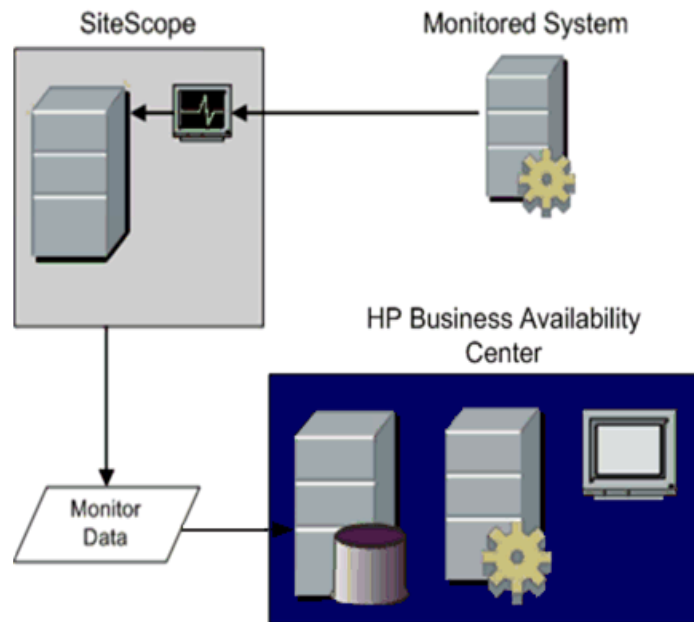
Understanding SiteScope Integration with HP Business Availability Center

Note: This section is relevant only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center.

SiteScope, as a standalone application, is an agentless solution for IT infrastructure performance and availability monitoring. SiteScope can also be used as a data collector for HP Business Availability Center. HP Business Availability Center collects data about end-users, business processes, and systems.

When registered as a data collector to HP Business Availability Center, the data and measurements collected by SiteScope monitors can be passed on to the HP Business Availability Center database for use in reports and analysis. Monitor data can be sent for all monitors or for selected monitors.

The following diagram illustrates the use of SiteScope as a data collector for HP Business Availability Center.



HP Business Availability Center includes a System Availability Management Administration page. This function allows you to manage SiteScope monitor configurations for one or more SiteScope servers through a central console. This level of SiteScope integration is separate from the integration of SiteScope monitor data with HP Business Availability Center.

There are two main aspects of compatibility between SiteScope and HP Business Availability Center. The first is data logging which is the process of logging data collected by SiteScope to HP Business Availability Center for the purposes of real-time status, reporting, Service Level Management, and so forth. The second aspect of compatibility is monitor configuration which refers to configuring SiteScope (including deploying monitors) from within HP Business Availability Center. Beginning with HP Business Availability Center version 7.0 and SiteScope version 9.0, the configuration done within Business Availability Center is done using System Availability Management Administration. Prior to these versions, the configuration within Business Availability Center was done in Monitor Administration.

The following table contains compatibility information regarding these two aspects of compatibility and the various combinations of SiteScope and HP Business Availability Center releases.

- 1 = Data logging support
- 2 = Configuration support
- X = Not supported

SiteScope Version	HP Business Availability Center Version				
	7.50	7.0	6.5	6.1	6.0
SiteScope 9.50	1,2	1,2	1	1	1
SiteScope 9.0	1,2	1,2	1	1	1
SiteScope 8.5	1	1	1,2	1,2	1,2
SiteScope 8.2	1	1	1,2	1,2	1,2
SiteScope 8.1.2 (recommended version for 6.1)	1	1	1,2	1,2	1,2
SiteScope 8.1, 8.1.1	1	1	1,2	1,2	1,2
SiteScope 8.0 SP2	1	1	1,2	1,2	1,2
SiteScope 8.0, 8.0 SP1	1	1	1	1	1

When SiteScope is registered as a data collector reporting data to HP Business Availability Center, it may also be accessed as a standalone product.

Integrating SiteScope Data with HP Business Availability Center's Configuration Items

Note: This section is relevant only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center.

When a monitor instance is added to a SiteScope reporting data to Business Availability Center, that monitor creates a corresponding configuration item (CI) in the HP Universal CMDB. For details on understanding configuration items, see “Configuration Items (CI)” in *Model Management*.

The SiteScope monitors that populate the Universal CMDB include both actual monitors and the groups in which they are created. Actual monitors instances are represented in the Universal CMDB as monitor CIs. Monitor CIs receive data from the corresponding SiteScope monitor instance and use the data to calculate Key Performance Indicator (KPI) status. SiteScope groups are represented as group CIs in the Universal CMDB and receive KPI status from the monitor CIs created by the monitors they are running.

You can also create relationships between SiteScope monitors and any existing, logical CI in the Universal CMDB. This relationship enables the monitor to pass KPI status to the CI to which it is attached.

This relationship can be created:

- ▶ For selected environments, by SiteScope automatically discovering the application's topologies and populating the UCMDB with the relevant CIs. For details, see “Reporting Discovered Topologies to HP Business Availability Center” on page 50.
- ▶ For most monitors, by SiteScope sending host data to Business Availability Center and connecting those hosts using the **Monitored by** relationship in IT Universe Manager or in View Manager's Instance View Editor. For details, see “Working with Relationships” in *Model Management*.

- ▶ For existing CIs, by using the **Monitor Deployment Wizard** which uses the existing CI property data in the CMDB to create monitors, groups, and remote servers. For details on using the wizard, see “Monitor Deployment Wizard Overview” on page 82.
- ▶ For any monitor instance, by manually selecting the **Link to Monitor CI** option when creating a monitor instance. For details on this option, see “Link Monitor to CI” on page 524.
- ▶ For integration environments, by using the Integration Monitors to create custom topologies to report to Business Availability Center. For details on using Integration Monitors, see “Working with SiteScope Integration Monitors” on page 1045.

Aging of CIs in CMDB

In the CMDB, CIs that have had no activity over a period of time are removed from the database. The CIs created from SiteScope data are also subject to this aging policy. However, SiteScope prevents the CIs it has sent to Business Availability Center from being removed by synchronizing the data it sends to Business Availability Center. When this synchronization occurs, it refreshes the data for those CIs and creates activity on the CIs.

For details on setting the time interval for topology synchronization, see “Topology Settings” on page 69. For details on the Aging Mechanism, see “Working with CIs” in *Model Management* in the HP Business Availability Center Documentation Library.

Note:

- ▶ Synthetic monitors and groups created by the EMS integration monitors that use Measurement field mapping are subject to the aging process regardless of the synchronization.
 - ▶ If you delete a CI from CMDB you must perform a resynchronization or a hard synchronization of SiteScope (in Integration Preferences), or you must wait for a restart of SiteScope so the CI is restored to the CMDB. This is due to the CI cache in SiteScope that prevents SiteScope from sending an unchanged CI twice. If you perform a hard synchronization, all the configuration data is deleted from CMDB and then added again. For details, see “BAC/OM Preferences Available Operations” on page 282.
-

Reporting Discovered Topologies to HP Business Availability Center

Note: This section is relevant only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center, and only when the SiteScope is reporting to HP Business Availability Center version 7.50 or later.

SiteScope can discover the hierarchy of the monitored entities of selected environments. These hierarchies of the monitored entities are represented by topologies that SiteScope reports to HP Business Availability Center. The CIs within the topologies correspond to the hosts, servers, and applications that SiteScope monitors, and are created in HP Business Availability Center's CMDB. Monitor and measurement CIs are also created and SiteScope reports their status to Business Availability Center. The relationships between the CIs are defined by the topology reported by SiteScope.

Supported Environments

This direct integration between SiteScope and Business Availability Center is available only for selected environments. For details on the specific topologies SiteScope reports for the applicable monitors, see:

- “SAP CCMS Topology Settings” on page 583
- “SAP Work Processes Topology Settings” on page 595
- “Siebel Application Server Topology Settings” on page 600
- “Siebel Web Server Topology Settings” on page 603
- “Web Service Topology Settings” on page 790

For details on the Topology Settings user interface, see “Topology Settings” on page 69.

Accessing SiteScope and Building Permissions Model

Note: This section is relevant only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center, and only when the SiteScope is reporting to HP Business Availability Center version 7.50 or later.

System Availability Management Administration builds a permissions model for each Business Availability Center user accessing SiteScope. That permissions model is based on the Business Availability Center user's permissions for SiteScope objects and not on the user's permissions as defined in SiteScope.

When assigning permissions to users in Business Availability Center for accessing a SiteScope through System Availability Management Admin, be aware that the permissions in Business Availability Center have been mapped to the equivalent permissions in SiteScope. The permissions model maps between the types of permissions available in SiteScope to what can be granted in Business Availability Center.

There are several differences between the Business Availability Center permissions model and SiteScope standalone permissions:

- ▶ Business Availability Center permissions enables granting permissions per group instance. In SiteScope standalone, permissions are granted onto groups as an object and do not have the instance granularity that exists in Business Availability Center.

For example, a user can have permissions within Business Availability Center to view or change specific instances of SiteScope groups with no permission to access other SiteScope groups.

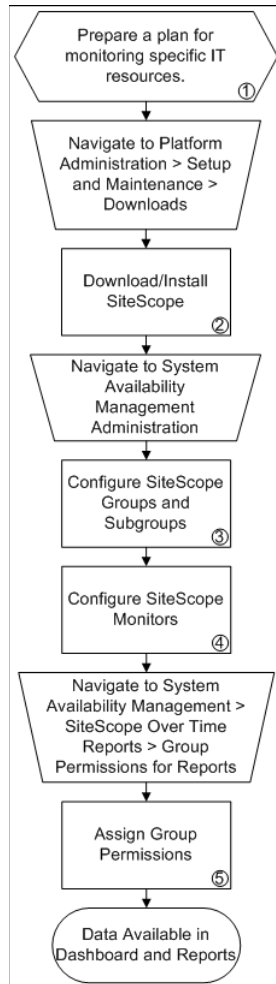
- ▶ SiteScope enables specific types of permissions onto object types, such as the ability to enable/disable whereas in Business Availability Center the operations are standard for all objects and include view, change, add, and full control. In this case, enable/disable is mapped to Business Availability Center's change permission.

- When applying permissions in Business Availability Center onto SiteScope objects, you can hover over an operation to see a description of how it maps to the permissions available to users of SiteScope standalone.
- Only a user at the Administrator level in SiteScope standalone has the necessary permissions to add a SiteScope to System Availability Management Administration in Business Availability Center.

Collect Data on the Performance of an IT Resource

Note: This section is relevant only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center.

The flowchart below describes the process required to set up and use SiteScope to collect data on the performance of IT infrastructure components. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.



Ref. No.	Comment
1	<p>Prepare a plan that maps out the specific IT infrastructure resources about which you want to collect data. Include information about the business processes that are affected by the specified infrastructure components (for example, business processes—being monitored by Business Process Monitor—that are running on an application server against which you plan to run SiteScope monitors).</p>
2	<p>Download and save the SiteScope installation files (for Windows or Solaris) to a local or network drive. Install SiteScope on machines designated to run the SiteScope data collector. You can run multiple SiteScopes from multiple platforms. For more information, see the <i>HP SiteScope Deployment Guide</i> PDF.</p>
3	<p>Add the SiteScope to System Availability Management Administration and configure the SiteScope’s integration preferences. For details, see “New SiteScope Page” on page 65, and “Integration Preferences User Interface” on page 278.</p> <p>Create groups and subgroups to organize the monitors to be deployed. For example, you can create groups of locations, server types, network resources, and so forth. For more information, see “New SiteScope Group Page” on page 462.</p>
4	<p>When configuring monitors, verify that HP BAC Logging settings are set as required. You can use the Monitor Deployment Wizard to deploy monitors onto existing CIs in the CMDB. You can also use Solution Templates to configure predefined sets of monitors on specific systems. For more information, see “SiteScope Solution Templates” on page 1273.</p> <p>Once defined, the SiteScope and its groups and monitors are added as CIs to the CMDB and are automatically attached to the relevant monitor views, from where they can be added to other views. During monitor configuration, you can associate the monitor with existing CIs using Link Monitor to CI Settings (for example you can attach the CPU monitor to an existing logical CI representing a machine whose CPU is being monitored).</p> <p>The data from the SiteScope is available in Dashboard and Service Level Management.</p>
5	<p>For each defined user, assign permissions to view SiteScope groups and their subgroups in System Availability Management reports and custom reports. For more information, see “System Availability Management Administration (SAM Admin)” in <i>Platform Administration</i>.</p>

System Availability Management Administration User Interface

This section describes:

- ▶ System Availability Management Administration on page 57
- ▶ New SiteScope Page on page 65
- ▶ Sync SiteScopes Wizard - Select Source and Targets Page on page 71




Note: System Availability Management Administration is available only to those users accessing SiteScope from HP Business Availability Center.





System Availability Management Administration

<p>Description</p>	<p>System Availability Management Administration is a portal within HP Business Availability Center that enables you to add SiteScope servers to an HP Business Availability Center system and to access those SiteScope servers.</p> <p>The SiteScopes are represented as nodes in the tree in the left pane.</p> <ul style="list-style-type: none"> ▶ When you highlight the root node, the right pane displays the System Availability Management functions, including summary information for the SiteScopes. ▶ When you highlight a SiteScope in the tree, the right pane displays that SiteScope's Dashboard and you can perform any function within the SiteScope. <p>To access: Select Admin > System Availability Management.</p>
<p>Important Information</p>	<p>Each SiteScope is listed by name with an icon displaying its current connection status to HP Business Availability Center.</p> <p>You access the SiteScope server by highlighting the name of the server in the list in the left pane.</p>

List of SiteScope Servers - Left Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<SiteScope server name>	<p>Represents an individual SiteScope server.</p> <p>The name includes a tooltip that displays the following data:</p> <ul style="list-style-type: none"> ▶ Health. Health status of the SiteScope server represented by a status icon. ▶ Mode. Whether the SiteScope is currently hosted by the HP Business Availability Center. ▶ Points. The number of license points in use by the SiteScope. ▶ Remote server. The number of remote servers being monitored by this SiteScope. ▶ Operating system. The type of OS on which the SiteScope is running. ▶ High Availability server. The name of the server used by this SiteScope for failover.
	<p>Icon accompanying the SiteScope name indicating that the SiteScope is registered to HP Business Availability Center and fully accessible from System Availability Management Administration. A SiteScope with this status is considered 'hosted' by HP Business Availability Center.</p>
	<p>Icon accompanying the SiteScope name indicating that the SiteScope is registered to HP Business Availability Center but not available for configuring. A SiteScope with this status reports data to HP Business Availability Center but can be configured only when accessing the SiteScope standalone.</p>
	<p>Icon accompanying the SiteScope name indicating that the existing SiteScope profile is empty and there is no running SiteScope associated with it.</p>

GUI Element	Description
	Icon accompanying the SiteScope name indicating that the integration between HP Business Availability Center and the SiteScope has been reset. The profile remains in HP Business Availability Center and can be used to prepare history reports. Data, however, is not reported to HP Business Availability Center applications.
	Click to add a SiteScope. Opens the New SiteScope page.
	Click to edit the properties of the highlighted SiteScope's connection to this HP Business Availability Center. Opens the Edit SiteScope page.
	Click to delete the highlighted SiteScope from this HP Business Availability Center.

Context Menu Options

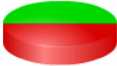

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

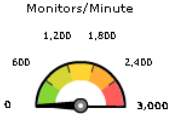
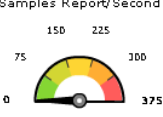


Menu Item	Description
New SiteScope	When highlighting the root node, click to add a SiteScope to the list of SiteScopes that are accessible to this HP Business Availability Center. Opens the New SiteScope page.
Edit SiteScope	Click to edit the properties of the highlighted SiteScope's connection to this HP Business Availability Center. Opens the Edit SiteScope page.
Delete SiteScope	Click to delete the highlighted SiteScope from this HP Business Availability Center.

Summary Information - Right Pane

<p>Description</p>	<p>When you highlight the root node, the right pane displays the summary information for all the SiteScopes accessed by this HP Business Availability Center.</p> <p>To access: Select Admin > System Availability Management and highlight the root node in the left pane.</p>
<p>Important Information</p>	<p>You access the SiteScope server by highlighting the name of the server in the list in the left pane or by clicking the name of the SiteScope in the table.</p> <p>The graphs displayed at the top of the page are a summary of all the SiteScopes listed.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):





GUI Element	Description
<p>Health</p> 	<p>Graph represents the overall health status of the listed SiteScopes. Each SiteScope represents its proportionate section of all the SiteScopes attached to HP Business Availability Center.</p>
<p>Points Used/Total</p> 	<p>Gauge represents the current monitor points that are in use by all the registered and configurable (hosted) SiteScopes versus the total points available for this installation.</p> <p>Note: The points displayed are per individual SiteScope. You cannot share license points among SiteScopes but you can shift a license key from one SiteScope to another. Delete the license key from the SiteScope that no longer uses that license and enter the same license key in the SiteScope that you want to use the license. For details on entering license information, see “SiteScope General Preferences User Interface” on page 248.</p>

GUI Element	Description
 <p>Monitors/Minute</p> <p>0 600 1,200 1,800 2,400 3,000</p>	<p>Gauge represents the total runs per minute and is calculated by taking the sum of all monitor runs per minute for all the hosted SiteScopes versus the number of hosted SiteScopes times 1000 (the maximum number of monitor runs per minute).</p>
 <p>Samples Report/Second</p> <p>0 75 150 225 300 375</p>	<p>Gauge displaying the rate of samples being reported from all SiteScopes to HP Business Availability Center. The maximum number of samples per second is determined by the HP Business Availability Center deployment.</p>
	<p>You can adjust the width of the table's columns by dragging the borders of the column to the right or the left.</p> <p>Click to reset the table columns' width to its default setting.</p>
	<p>Click to open the Select Columns dialog box and select the columns you want displayed in the table.</p>
<p>Global Search and Replace</p>	<p>Click to open the Global Search and Replace Wizard to update properties across multiple SiteScopes. For details on the user interface, see “Global Search and Replace Wizard” on page 351.</p>
<p>Sync SiteScopes</p>	<p>Click to open the Sync SiteScope Wizard to copy preferences, settings, and configuration files between SiteScopes. For details on the user interface, see “Sync SiteScopes Wizard - Select Source and Targets Page” on page 71.</p>

SiteScope Summary Table

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Table Column	Description
Display Name	The name give to the SiteScope when it was added to System Availability Management Admin.
Points Used/Total	The number of license points currently being used by the SiteScope versus the total license points available.
Deployed Monitors	The number of monitors configured the specific SiteScope server.
Monitors/Minute	The number of monitor runs per minutes.
Remote Targets	Displays the number of remote servers being monitored by this SiteScope.
OS	The operating system on which the SiteScope is running.
Version	The version of the SiteScope software.
Samples/Report	Displays the rate of samples reported from this SiteScope to HP Business Availability Center.
HA Status	Displays whether the failover SiteScope installation is running or not and whether the failover SiteScope is running instead of the primary SiteScope.

Table Column	Description
Health	<p>Indicates the status of the SiteScope itself. The following are the available status levels:</p> <ul style="list-style-type: none">  OK. All performance measurements are within the OK threshold level.  Warning. At least one performance measurement is within the Warning range, but no measurements are within the Error or Poor range.  Error/Poor. At least one performance measurement is within the Error or Poor range. This indicates either of the following: <ul style="list-style-type: none"> ▶ the performance measurement has a value, but at poor quality level ▶ there is no measurement value due to some error  No thresholds breached. No thresholds were defined for the monitor, so no status is assigned.
MDW	<p>Click to access the Monitor Deployment Wizard. You use the wizard to deploy monitors from the SiteScope onto existing CIs in HP Business Availability Center. For details on this topic, see “Monitor Deployment Wizard Concepts and Tasks” on page 81.</p>

Optional Columns for SiteScope Summary Table

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Table Column	Description
Last Report Time	The last time monitor data was reported to Business Availability Center, displayed in format: Day Month Date Hours:Minutes:Seconds.
Host Name	The host name or IP address of the machine on which the SiteScope is currently running.
Port Number	The port number used to communicate with SiteScope. Default value: 8080

Table Column	Description
Inaccessible Profile	Displays if this SiteScope profile was added to System Availability Management Administration without a running SiteScope server registered to it. This means that the profile name was added to the database but there is no connection to the SiteScope from HP Business Availability Center until the actual registration from the SiteScope server.
Use SSL	Displays whether this SiteScope is using a secure communication through HTTPS.
Profile Name	The name to identify this SiteScope for HP Business Availability Center operations and reports. Note: If no value is entered, the Display Name entered in the Main Settings is used.
GMT Offset	The GMT Offset set for the SiteScope profile used for reports and aggregation purposes.
Enable Reporting to HP BAC	Displays whether the SiteScope is enabled to forward measurements to HP Business Availability Center.
GW Server Name	The name or IP address of HP Business Availability Center's Gateway server.
Failover Host	Displays the host name of the failover server if one has been installed for this SiteScope.
Description	The description of this SiteScope as entered when adding the SiteScope to System Availability Management Administration.

New SiteScope Page

Description	Use to add an existing SiteScope to this HP Business Availability Center. You can determine whether the SiteScope is hosted by System Availability Management or if it just reports data to HP Business Availability Center.
Important Information	Once a SiteScope is added to the System Availability Management page, it is assigned a connectivity status. Only a user who is defined with Administrator permissions in SiteScope standalone can add that SiteScope to System Availability Management Administration.
Useful Links	“System Availability Management Administration” on page 57

The New SiteScope Page includes the following areas:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Display Name	Type a descriptive name representing this SiteScope in System Availability Management Admin. This name identifies the SiteScope in the list of SiteScopes in the left pane and in the summary list in the right pane.
Host Name	Type the host name or IP address of the machine on which SiteScope is currently running.

GUI Element	Description
Port Number	Type the port number used to communicate with SiteScope. Default value: 8080
Inaccessible Profile	Use this box to create a profile for a SiteScope that is not currently accessible from HP Business Availability Center. Creating the profile in this way adds the profile name to the database but there is no connection to the SiteScope from HP Business Availability Center until the actual registration from SiteScope. Example: Type a profile name for a SiteScope to report data to HP Software-as-a-Service. HP Software-as-a-Service cannot access the SiteScope until it has been registered from the SiteScope.

Distributed Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Gateway Server name/IP address	By default, this box displays the name or IP address of the Gateway server. Note: Modify this box only if the HP Business Availability Center has a distributed deployment and the Gateway server is installed on different machines. In this case, enter the name or IP address of the Core server.
SiteScope agent machine location	Type the SiteScope agent machine location. If no value is entered, the default is used.
Gateway Server authentication user name	Type the login user name used to access the Gateway server. If no value is entered, the default is used.
Gateway Server authentication password	Type the password used to access the Gateway server. If no value is entered, the default is used.

Advanced Settings

GUI Element	Description
SiteScope user name	Type the user name needed to connect to the SiteScope.
SiteScope password	Type the SiteScope login password if the SiteScope you are adding has been set up with a password.
Failover Host	If a failover server has been installed for this SiteScope, enter the host name. Note: There is no validation to check if there is a failover SiteScope running on this host.
Description	Type a description for this SiteScope.

Profile Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Use SSL	Select to secure the communication of the SiteScope API through a secure HTTPS. Selecting this option requires you to configure your SiteScope to run with SSL.
Profile name	Type a name to identify this SiteScope for HP Business Availability Center operations and reports. If no value is entered, the Display Name entered in the Main Settings is used.
GMT offset	Select the GMT Offset for the SiteScope profile used for reports and aggregation purposes.
Profile database name	Select the database (Microsoft SQL) or schema (Oracle) into which the profile information is saved.
Web server authentication user name	Type the user name for the authentication (basic authentication and protocol) of the Web server security options.
Web server authentication password	Type the password for the authentication of the Web server security options (basic authentication and protocol).

GUI Element	Description
Web server use SSL	Select this option for the Web server to use https protocol over a secure connection.
Proxy name/IP address	If SiteScope uses a proxy to connect to the HP Business Availability Center server, enter the IP address.
Proxy user name	If SiteScope uses a proxy to connect to the HP Business Availability Center server, enter the user name for the proxy.
Proxy password	If SiteScope uses a proxy to connect to the HP Business Availability Center server, enter the password for the proxy.
Enable Reporting to BAC	<p>Enables reporting SiteScope measurements to HP Business Availability Center.</p> <p>You can clear this option to temporarily disable reporting from this SiteScope to HP Business Availability Center.</p> <p>Default value: Selected. Can be cleared only in edit mode and not when adding a SiteScope.</p>

Topology Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Topology resynchronization time interval	<p>The number of days for SiteScope to synchronize topology data with Business Availability Center.</p> <p>The topology information SiteScope reports to Business Availability Center is synchronized when SiteScope restarts after this time interval has been reached. SiteScope restarts by default every 24 hours.</p> <p>Default value: 7 (days)</p> <p>Note: All topologies created by SiteScope and stored in CMDB are subjected to the aging process. To prevent aging, see “Aging of CIs in CMDB” on page 48.</p>
Default topology probe domain	<p>Enter the default domain of the SiteScope topology probe.</p> <p>Note: You must restart SiteScope if you change this setting.</p>
Topology receiver port	<p>Enter the topology receiver port used in Business Availability Center.</p> <p>Default value: 8080</p> <p>Note: You must restart SiteScope if you change this setting.</p>
Topology receiver SSL port	<p>Enter the topology receiver SSL port used in Business Availability Center.</p> <p>Default value: 443</p> <p>Note: You must restart SiteScope if you change this setting.</p>

Note: The following settings can only be modified in the user interface, and not from the <SiteScope root directory>\conf\ems\jython.properties file:

- **Default topology probe domain** (appilog.collectors.domain)
- **Topology receiver port** (serverPort)
- **Topology receiver SSL port** (serverPortHttps)

If you modified these settings from the properties file in a previous version of SiteScope (the property name is shown in brackets), these changes are lost when upgrading to SiteScope 9.50 and you must reconfigure the settings in the user interface. If you modified the remaining settings, these changes are lost when upgrading to SiteScope 9.50, and you must reconfigure the settings in the <SiteScope root directory>\discovery\discovery_agent.properties file.

Sync SiteScopes Wizard - Select Source and Targets Page

<p>Description</p>	<p>Use this wizard to synchronize settings from different SiteScopes by copying files and settings from one SiteScope to another.</p> <p>To Access:</p> <p>Select Admin > System Availability Management and click Sync SiteScopes.</p> <p>Use the Select Source and Targets page to select the source SiteScope from which to copy settings and the target SiteScope to which to copy settings.</p>
<p>Important Information</p>	<ul style="list-style-type: none"> ▶ This wizard can be used to copy the settings configured for a SiteScope to another SiteScope. ▶ To copy groups, monitors, alerts, or reports from one SiteScope to another SiteScope, use the Copy and Paste to another SiteScope option in the monitor tree's context menu. ▶ The Select Source and Targets page lists only those SiteScopes that: <ul style="list-style-type: none"> ▶ are version 9.0 or higher ▶ have been added to System Availability Management ▶ are currently accessible to HP Business Availability Center
<p>Wizard Map</p>	<p>The Sync SiteScopes wizard includes: Sync SiteScopes Wizard - Select Source and Targets Page > Select Types to Sync > Select Instances to Sync > Summary Page.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<p>Source SiteScope</p>	<p>Select the SiteScope from which to copy settings or files. You can select only one SiteScope from which to copy.</p> <p>Once a SiteScope is selected as the source, it cannot be selected as a target.</p> <p>Note: Only those SiteScopes appear for which the current user has at least view permissions as applied in Permissions Management. For details on this topic, see “Operations” in <i>Platform Administration</i>..</p>
<p>Target SiteScope</p>	<p>Select the SiteScopes to which to copy settings or files. You can select multiple SiteScopes as the target of the synchronization.</p> <p>Note: Only those SiteScopes appear for which the current user has at least change permissions as applied in Permissions Management. For details on this topic, see “Operations” in <i>Platform Administration</i>..</p>

Select Types to Sync

<p>Description</p>	<p>Use this page to select those objects, settings, or files to copy from one SiteScope to other SiteScopes.</p> <p>You can copy preferences, views, and categories. Only those objects appear that have been configured in the source SiteScope.</p>
<p>Important Information</p>	<p>You can use the Select All, Clear Selection, and Invert Selection buttons to modify your selections.</p>
<p>Wizard Map</p>	<p>The Sync SiteScopes wizard includes: Sync SiteScopes Wizard - Select Source and Targets Page > Select Types to Sync > Select Instances to Sync > Summary Page.</p>

SiteScope Objects

The following are the objects that can be copied from one SiteScope to other SiteScopes:

GUI Element	Description
<p>Preferences</p>	<p>Copy the preferences configured in the source SiteScope to the target SiteScope. Only those preferences that have been configured in the source SiteScope appear here. If no preferences or instances of preference types have been defined in the source SiteScope, there are no preferences listed here.</p> <p>The following preferences can be selected for the sync operation:</p> <ul style="list-style-type: none"> ➤ E-mail preferences ➤ Pager preferences ➤ SNMP trap preferences ➤ Absolute schedule preferences ➤ Range schedule preferences <p>For details on types of preferences, see “Preferences” on page 207.</p> <p>Example: Copy the absolute schedules that have been configured in the source SiteScope to the target SiteScope. You can then use those same absolute schedules when scheduling monitors to run (while configuring or editing monitors) in the target SiteScope.</p>

GUI Element	Description
Categories	<p>Copy the categories configured in the source SiteScope to the target SiteScope. If no categories have been defined in the source SiteScope, there are no categories listed here.</p> <p>For details about using categories in SiteScope, see “Working with Categories” on page 197.</p> <p>Example: A category defining operating system with values of Windows, Linux, and so forth has been defined in the source SiteScope. These same categories can be copied for use in the target SiteScope.</p>
Templates	<p>Copy the templates configured in the source SiteScope to the target SiteScope. If no templates have been defined in the source SiteScope, there are no templates listed here.</p> <p>For details about working with templates in SiteScope, see “SiteScope Templates Overview” on page 1190.</p>

SiteScope Files

The following are the files that can be copied from one SiteScope to other SiteScopes:

GUI Element	Description
SNMP Template Files	<p>Templates that can be selected when creating an SNMP trap alert action.</p> <p>Select to copy all the files in the following folder path: <SiteScope root directory>\templates.snmp.</p>
Certificate Template Files	<p>Select to copy all the files in the following folder path: <SiteScope root directory>\templates.certificates.</p>
Post Template Files	<p>Templates that can be selected when creating a post alert action.</p> <p>Select to copy all the files in the following folder path: <SiteScope root directory>\templates.post.</p>
OS Template Browsable Files	<p>Select to copy all the files in the following folder path: <SiteScope root directory>\templates.os\browsable.</p>

GUI Element	Description
OS Template Files	Select to copy all the files in the following folder path: <SiteScope root directory>\templates.os.
Mail Reports Template Files	Select to copy all the files in the following folder path: <SiteScope root directory>\templates.history.
Mail Template Files	Templates that can be selected when creating an e-mail alert action. Select to copy all the files in the following folder path: <SiteScope root directory>\templates.mail.
Sound Template Files	Templates that can be selected when creating a sound alert action. They include the media files that create the sound for a triggered alert. Select to copy all the files in the following folder path: <SiteScope root directory>\templates.sound.
Scripts Remote Files	Select to copy all the files in the following folder path: <SiteScope root directory>\scripts.remote.
Scripts Files	Scripts that can be selected when creating a script alert action. Select to copy all the files in the following folder path: <SiteScope root directory>\scripts.
MIB Files	Select to copy all the files in the following folder path: <SiteScope root directory>\templates.mib.

Select Instances to Sync

Description	This page displays a tree with all the instances of the type of file or object selected in the Select Types to Sync page. You can then select specific instances of the file type or object type you want copied from the source SiteScope to the target SiteScopes.
-------------	--

Important Information	<p>You can use the Select All, Clear Selection, and Invert Selection buttons to modify your selection of file or object instances.</p> <p>When you finish making your selections, click Finish.</p>
Wizard Map	<p>The Sync SiteScopes wizard includes: Sync SiteScopes Wizard - Select Source and Targets Page > Select Types to Sync > Select Instances to Sync > Summary Page.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Files/objects tree>	<p>Use the tree to select or clear specific instances occurring in the source SiteScope of the file type or object type you want to copy to the target SiteScope. The tree lists all instances of the selected file type or object type that occur in the source SiteScope.</p> <p>Default value: All instances of every file or object selected in the Select Types to Sync page are selected. Clear the check box next to an instance to remove it from the sync operation.</p>
Override existing instances	<p>Select this option for the sync action to override any instances of the same name in the target SiteScopes with the selected instances.</p> <p>If this option is cleared and during the sync operation, an instance of the object or type with the same name is found in the target, the sync operation does not copy the instance onto the target SiteScope.</p> <p>Example: You selected Absolute Schedule Preferences in the Select Type to Sync page and the target SiteScope has an absolute schedule with the same name as in the source SiteScope:</p> <ul style="list-style-type: none"> ▶ If this option is selected, the target's absolute schedule is overwritten with the properties of the schedule in the source SiteScope. ▶ If this option is cleared, the target's absolute schedule maintains its properties and is not overwritten.

Summary Page

Description	Displays the number of objects or files successfully copied to the target SiteScopes. If any objects or files failed to copy to the target SiteScopes, this number is also displayed.
Wizard Map	The Sync SiteScopes wizard includes: Sync SiteScopes Wizard - Select Source and Targets Page > Select Types to Sync > Select Instances to Sync > Summary Page .

Troubleshooting and Limitations

Receive a 408 error when attempting to access SiteScope user interface from System Availability Management Administration.

Possible Solution 1: Add the SiteScope machine's URL to trusted sites in Internet Explorer's options and restart all browsers.

Possible Solution 2: Configure the browser to accept cookies from the SiteScope server.

Reverse integration does not work.

Possible Solution: Type the SiteScope machine name in the **SiteScope agent machine location** field when adding a SiteScope to System Availability Management.

Page cannot be displayed due to 404 error.

This error may occur because there is no access from the browser machine to SiteScope (pinging the machine also does not work). The SiteScope host may be changed to a fully qualified host name after adding the SiteScope to System Availability Management Administration.

Possible Solution: If there is no DNS configured for the network, you can configure SiteScope to report its IP address to HP Business Availability Center. Open the <SiteScope root directory>\groups\master.config file, and enter the SiteScope machine's IP address in the `_sisHostNameOverride` property.

To solve the problem on the browser's machine, you can add the SiteScope machine name with IP to the host's file in the `//WINDOWS/system32/drivers/` directory on the HP Business Availability Center machine.

Flash components (summary graphs) are not displayed in the System Availability Management Administration page.

Possible solution: Install flash on the client browser.

Error while adding a SiteScope to System Availability Management Administration in the Add SiteScope page.

While adding the SiteScope to System Availability Management Administration, an error occurs and you want to change the **Display name** field to try to add the SiteScope again. The **Profile name** field, which is used in Business Availability Center reports, Dashboard, and so forth, is defined from the **Display name** field. The **Profile name** may still have the default value from the first time you tried adding the SiteScope.

Possible solution: If you change the **Display name** field or **Host name** field after an error during initially trying to add the SiteScope, you should change all the fields that get their default values from those fields, for example **Profile name**.

Error while opening the SiteScope user interface when SiteScope is unable to access the HP Business Availability Center permissions application.

The following error message is displayed: "The SiteScope interface failed to open because SiteScope was unable to access the HP Business Availability Center's permissions application using http://<your BAC server>/topaz/ url. SiteScope needs this access to build the permission model before granting access to the SiteScope interface. Check your network configuration and verify that SiteScope can access HP Business Availability Center."

Possible Solution 1: Check your network configuration.

Possible Solution 2: Add the IP address of the HP Business Availability Center server to the `etc\hosts` file on the SiteScope machine.

3

Monitor Deployment Wizard Concepts and Tasks

This chapter includes the main concepts, tasks and reference information for the Monitor Deployment Wizard.

Note: The Monitor Deployment Wizard is available only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center.

This chapter includes:

Concepts

- ▶ Monitor Deployment Wizard Overview on page 82
- ▶ Prerequisites for Running the Monitor Deployment Wizard on page 84
- ▶ Monitor Deployment Wizard Templates and Variables on page 85
- ▶ Full and Partial Monitor Coverage on page 87
- ▶ Wizard Options on page 88
- ▶ Monitor Deployment Wizard for Siebel on page 89

Tasks

- ▶ Deploy Monitors Using the Monitor Deployment Wizard on page 90

Reference

- ▶ Template Reference on page 96
- ▶ Monitor Deployment Wizard User Interface on page 104

Monitor Deployment Wizard Overview

The Monitor Deployment Wizard provides a monitoring solution for existing Business Availability Center configuration item (CI) data using SiteScope templates. The wizard uses SiteScope templates to deploy monitors, groups, and remote servers with the existing and discovered CI data from the CMDB. For details on understanding CIs, see “Configuration Management Database (CMDB)” in *Reference Information*.

SiteScope templates enable you to deploy group and monitor configurations across multiple infrastructure elements with a minimal number of configuration steps. For details, see “SiteScope Templates” on page 1189.

The Monitor Deployment Wizard uses SiteScope’s template functionality to create a monitoring solution for the CIs in your CMDB. When you select CIs to monitor using the Monitor Deployment Wizard, the wizard automatically matches templates to the selected CIs based on the CI type selected. You can also select additional templates to apply to the selected CIs for your specific monitoring requirements. For details on which templates are deployed onto which CI types, see “Template Reference” on page 96.

The CMDB may already include CI data that can be used for monitor deployment. These properties may have been entered while adding the CI to the IT Universe model or may have been discovered by the Discovery Manager. For details, see “Populate an Instance View” in *Model Management*. The wizard is also able to retrieve the data from the CMDB for the selected CIs and use that data when deploying the SiteScope templates.

HP Business Availability Center enables you to use that data to create SiteScope monitors, groups, and remote servers for existing CIs in the CMDB.

The Monitor Deployment Wizard:

- ▶ enables you to select CIs onto which to deploy the SiteScope templates
- ▶ recognizes the CIs onto which a SiteScope monitor can be deployed
- ▶ recognizes which templates to deploy onto which CIs

- enables you to refine the selection of templates to deploy onto CIs
- checks the CI for existing monitors and measurements that match the monitoring solution to be deployed by the template and enables you to handle duplicate monitoring
- imports the configuration item's properties that have been defined in Universal CMDB Administration into the monitor's properties and creates remote servers on SiteScope
- uses template variables to enable you to enter data for monitor properties that are not imported from the configuration item's definition
- creates in the CMDB a **monitored by** relationship between the monitored CI and the created monitor

Example of Monitor Deployment

For example, an Oracle database has been added as a CI to the IT Universe model in CMDB. You can use the Monitor Deployment Wizard to deploy the Oracle Database monitor onto the CI. The wizard imports the following properties that are defined for the server in the CMDB:

- database server IP address or server name
- database user name
- database password
- database port
- database SID

If a partial Discovery was run during the Discovery process, the wizard prompts you to enter values for some of the variables that are necessary for the deployment of the monitors.

Prerequisites for Running the Monitor Deployment Wizard

Before running the Monitor Deployment Wizard, you must run the relevant discovery jobs to discover CIs and populate views. For details on the Discovery process, see “Discovery and Dependency Mapping – Overview” in *Discovery and Dependency Mapping Guide*.

After you have discovered the relevant CIs in your business environment, you can select one of the pre-defined views populated by the Discovery jobs. Alternatively, you can create a view manually for the purpose of running the Monitor Deployment Wizard. It is recommended to create a **Host Credentials** view which contains hosts with credentials. This can help to streamline the process of selecting the relevant hosts to be monitored in the Select CIs to Monitor step of the wizard.

Note: Do not create a view in which the same CI appears more than once. If you select a view in which the same CI appears more than once, the selection of the whole view in the wizard fails.

To create a Host Credentials view:

- 1** Select **Admin > Universal CMDB > Modeling > View Manager**.
- 2** From the Views pane, right-click the Root folder in the tree.
- 3** Select **New** from the context menu. The Create New View dialog box opens.
- 4** Type **Host Credentials** in the View Name window.
- 5** From the CI Types pane, expand the System branch of the tree. Click and drag the Host CI type into the Editing pane.
- 6** From the CI Types pane, expand the Software Element branch of the tree. Click and drag the Shell CI type into the Editing pane.
- 7** Holding down the CTRL key, select both the Host and Shell nodes in the Editing pane. Right-click one of them and select **Add Relationship**. The Add Relationship dialog box opens.

- 8 In the Add Relationship dialog box, click **Advanced**. Select **Container Link** from the tree in the relationship window. Click **OK**.
- 9 Right-click the shell node in the Editing pane and select **Node Condition** from the context menu. The Node Condition dialog box opens.
- 10 In the Node Condition dialog box, clear the **Visible** check box and click **OK**.
- 11 Click the **Save** button from the toolbar to save the view.

For details on creating views, see “Create New View/View Properties Dialog Box” in *Model Management*.

Note: In the Select CIs to Monitor step of the wizard, you can select CIs to monitor from many different views, but a specific CI may be selected only once, even if it appears in more than one view.

Monitor Deployment Wizard Templates and Variables

The Monitor Deployment templates appear by default in the monitor tree in a container called **Monitor Deployment Wizard Templates**. This container and the templates and variables within it should not be edited or deleted.



Only advanced users with a thorough knowledge of working with templates should attempt to edit any of the variables or to add variables to the templates. For details, see “SiteScope Templates” on page 1189.

Monitor Template Variables

The templates associated with the selected CIs have variables which must be filled in before the wizard can deploy them. The system fills in most of the variables automatically by checking the CI information or the results of the Discovery process. Other variables are not filled in by the system because the data was missing from the CI information, the Discovery process did not run completely, or because the data is dependent on the user. You must fill in the missing information for any selected monitor templates. You also have the option of not deploying the template by clearing the template selection if you do not know the variable values.

Selecting Templates

Once a CI is selected, all the relevant templates are matched to the CI.

In the step for entering variable values, a check box appears next to each monitor template associated with that CI. By default, if there is any missing data for the variables in a template, that template is not selected for deployment. This enables the wizard to streamline the deployment process.

You can select or clear templates for deployment. If you select a template for deployment but fail to enter the missing data for its variables, an error message appears and the wizard cannot proceed until you enter the data. If you leave any templates unselected, a warning message appears to alert you that there are unselected templates but you can choose to proceed with the wizard anyway. This applies to all unselected templates, whether data was entered for them or not.

Manual Template Matches

The wizard enables you to select other templates for deployment that were not automatically mapped by the wizard. For example, you may want to use an existing template that includes log file monitoring that is set to search for a specific string that would be relevant for host CIs in your environment. You can choose to deploy that template onto the host CIs you selected in the Select CIs to Monitor page.

You may also want to select a CI type that does not have a template associated with it and deploy an existing template onto that CI.

If you have matched additional monitor templates to be deployed onto CI types that are not in those predefined in the wizard, you can save these matches for future use when the same Business Availability Center user runs the wizard.

Also, if you removed templates that were matched by the wizard for specific CIs and chose to save matching, those templates are not matched to the selected CIs the next time the same Business Availability Center user runs the wizard.

For details, see “Save Matching” on page 108.

Full and Partial Monitor Coverage

For each selected CI, the Monitor Deployment Wizard checks whether the CI already has a monitored by relationship with any monitor CIs that are equivalent to the monitor instances that would result from the wizard deploying the templates mapped for that CI. It further checks the actual measurements within the monitor CIs and determines if the monitoring solution deployed by the wizard duplicates the monitors that exist for the selected CI.

If the CI onto which you want to deploy the monitoring solution already contains all of the same monitor and measurement instances, the CI is considered **fully covered**. If the CI has only part of the monitors and measurements already deployed, the CI is considered **partially covered**.

You can choose to clear fully or partially covered CIs and disable them for the deployment. Or, you have the option of continuing with the deployment and handling the duplicate monitors in the final step of the wizard. If, in the final step of the wizard, duplicate monitors on CIs were detected and the wizard successfully deployed templates onto these CIs, a **Handle Duplicates** button is displayed and enables you to delete these monitors, disable them or leave them in tact as duplicated monitors.

Wizard Options

CI Group Hierarchy Option

When you deploy templates using the Monitor Deployment Wizard, you can choose to create a CI group hierarchy which mirrors the CI hierarchy in the selected view in HP Business Availability Center. This means that SiteScope groups are created to correspond to the parent and grandparent CIs of the CI being monitored. These groups are arranged in a tree structure identical to the one that contains the actual CIs in the selected view in HP Business Availability Center.

SiteScope Remote Preferences

The SiteScope templates used in the Monitor Deployment Wizard are configured with template remotes which create remote server preferences in SiteScope for use by other SiteScope monitors. The remote servers created can be found in SiteScope under **Preferences > Microsoft Windows Remote Preferences** (for Windows monitors) and **Preferences > Unix Remote Preferences** (for UNIX monitors). For details on remote preferences, see “Microsoft Windows Remote Preferences User Interface” on page 285 and “UNIX Remote Preferences User Interface” on page 291.

When the wizard deploys a template with remote server definitions for a physical monitor (for example, a CPU monitor), a remote preference is created with the name of the host (the host DNS name) plus the username. When deploying a template with a remote server that already exists in SiteScope’s remote preferences, SiteScope uses the existing remote and does not create another remote preference. For details on creating remote preferences with templates, see “SiteScope Templates” on page 1189.

Reporting

The final step of the Monitor Deployment Wizard consists of the Deployment Results page which displays information about the successful and unsuccessful monitor deployments. The report contains the names of the selected CIs and the monitors selected for deployment. The deployment status is indicated for each monitor.

The report can be exported to a PDF or a CSV file. These reports include detailed information displaying all the created groups, monitors, and alerts, including the exact location where they can be found in SiteScope. These reports are useful for large deployments. For example, when hundreds of CIs are selected in the wizard, the resulting deployment can include thousands of new objects added to the SiteScope. For details, see “Deployment Results Page” on page 111.

Note: After running the Monitor Deployment Wizard, the deployed monitors are not run immediately, but rather within the defined frequency scheduled for the monitor.

Monitor Deployment Wizard for Siebel

You can use the Monitor Deployment Wizard to monitor your Siebel environment. The view to use for the wizard is the **Siebel Enterprise** view. The wizard can identify the Siebel configuration items in the CMDB and deploy a set of pre-configured monitors onto those items. The monitors include those that are specifically designed to monitor Siebel, as well as generic monitors that can monitor the performance of your Siebel network.

For details on the available templates used for the Siebel environment, see “Siebel Solution Templates” on page 1353.

For reference information on the Siebel monitor template and configuration items, see “Template Reference for Siebel” on page 99.

Deploy Monitors Using the Monitor Deployment Wizard

This task describes the steps involved in deploying monitors using the Monitor Deployment wizard.

This task includes the following steps:

- ▶ “Run Discovery” on page 90
- ▶ “Begin Running the Wizard” on page 90
- ▶ “Enter Missing Data for Selected CIs” on page 92
- ▶ “Check the Configuration Summary and Deploy Monitors” on page 93
- ▶ “Review the Deployment Results and Export the Report” on page 94

1 Run Discovery

Prior to deploying monitors with the Monitor Deployment Wizard, you must discover the CIs in your system and populate views.

It is recommended that you create a Host Credentials view for the purpose of running the Monitor Deployment Wizard. For details on this topic, see “Prerequisites for Running the Monitor Deployment Wizard” on page 84. While this is not mandatory, it is recommended so that the necessary credentials exist to access the servers.

2 Begin Running the Wizard

Begin running the wizard. For details on the user interface, see “Monitor Deployment Wizard” on page 104. The first step is to select CIs to monitor using the View Explorer. For details on the user interface, see “Select CIs to Monitor Page” on page 106.

After selecting CIs to monitor, you can select monitor templates to apply to them using the Templates Selection dialog box. For details on the user interface, see “Templates Selection Dialog Box” on page 107.

Example:

Welcome

The Monitor Deployment Wizard deploys pre-configured templates onto the configuration items in your CMDB. The wizard:

- Enables you to deploy monitors onto selected CIs using pre-configured templates
- Imports the configuration item's properties from the CMDB into the monitor's properties
- Uses template variables to enable you to enter data for monitor properties

Getting Started:

- Select CIs from the views in your CMDB. Modify your selection to include only the CIs you want monitored.
- Enter the variable data required to deploy the templates. The wizard automatically imports the CI's properties from the CMDB and fills the template variables, it is required only to fill missing data.
- Review the configurations for all the monitors the wizard is creating for each CI in a selected view.

For more information, open the Help.

Select CIs to Monitor

Select a view and highlight a CI within the view. Click the right arrow to perform deployment on the highlighted CI. The tree on the right displays the selected CIs.

The interface includes a 'Browse' section with a search bar and a 'View' dropdown menu currently set to 'NetworkTopology'. Below this, a tree view displays the 'NetworkTopology' view expanded, showing three configuration items (CIs) with IP addresses: '16.44.49.0' (highlighted), '16.59.58.0', and '16.59.60.0'. To the right, another tree view shows the 'All' view expanded, displaying the selected CI '16.44.49.0'. Navigation arrows are visible between the two trees. At the bottom, there is a 'Templates Selection' button.

3 Enter Missing Data for Selected CIs

On the third page of the wizard, select the monitor templates to deploy and enter any missing data for them. For details on the user interface, see “Enter Required Data for CIs Page” on page 109.

Example:

Enter Required Data for Selected CIs

Enter the required data in the fields below to ensure the successful creation of all monitors. All fields must be filled.
Only CIs that lack required data are expanded

CI	Variable	Value
IT Department		
<input checked="" type="checkbox"/> NT Monitors(37 pts)	host_dnsname	<input type="text" value="1.2.3.4"/>
	host_username	<input type="text" value="user1"/>
	host_password	<input type="password" value="*****"/>
	nt_domain	<input type="text" value="domain1"/>
16.59.57.155		
<input checked="" type="checkbox"/> Host Monitors(1 pts)	Host DNS Name	<input type="text" value="16.59.57.155"/>
<input type="checkbox"/> NT Monitors(37 pts)	Host DNS Name	<input type="text" value="16.59.57.155"/>
	host_username	<input type="text"/>
	host_password	<input type="password"/>
	nt_domain	<input type="text"/>

4 Check the Configuration Summary and Deploy Monitors

On the fourth page of the wizard, review the final configuration summary and select a SiteScope group on which to deploy the templates. Click **Finish** to complete the wizard and deploy the monitors. For details on the user interface, see “Final Configuration Summary Page” on page 110.

Example:

Final Configuration Summary

In this page you can review the configuration before deployment.
For each CI a list of templates is displayed together with a number of monitors and estimated license points per template.

Total number of license points available on SiteScope server is 9545 (required number of points is 29).

CI Name / Template Name	Monitors to be created	License Points
<ul style="list-style-type: none"> [-] app1 <ul style="list-style-type: none"> [-] lob1 <ul style="list-style-type: none"> [-] Host <ul style="list-style-type: none"> Host Monitors 	1	1
<ul style="list-style-type: none"> [-] 16.59.61.0 <ul style="list-style-type: none"> [-] labm1amrnd06 <ul style="list-style-type: none"> 16.59.61.134 <ul style="list-style-type: none"> NT Monitors Host Monitors 	1 1	27 1
6 CIs with total of 3 templates	3	29

Monitors will be deployed on the SiteScope Group:

SiteScope

Create CI group hierarchy (creates groups in SiteScope according to the CI hierarchy name under the selected deployment group)



5 Review the Deployment Results and Export the Report


On the last page of the wizard, review the results of the deployment and, if necessary, retry deploying those template that failed to deploy. In this page, you can also handle duplicate monitors that were deployed. Optionally, you can export the deployment results to a .pdf or a .csv file. For details on the user interface, see “Deployment Results Page” on page 111.

Example:

Deployment Results

Summary of successful deployments:
 7 templates were deployed for 4 CIs
 Total number of deployed monitors is: 7

CI Name	Object Name	Status
 Siebel WSE <input type="checkbox"/>	<input type="checkbox"/> Siebel Web Server Extension <input type="checkbox"/> Siebel Web Server Extension for labm1sbl03	Failed to commit - uniqueness violation - the name 'Siebel Web Server Extension for labm1sbl03' exists in requested destination
<input type="checkbox"/> Siebel Web Server Extension for labm1sbl03		Unknown

Modify failed monitors properties and retry creation

Allows the user to disable or delete duplicate monitors

Handle Duplicate Monitors

Please select desired action for the duplicated monitors below.

CI Name / Monitor Name	Select Desired Action
<input type="checkbox"/> ami-il.mercury.global - Fully monitored	
<input type="checkbox"/> Ping ami-il.mercury.global(Ping)	<input checked="" type="radio"/> Leave Intact <input type="radio"/> Disable <input type="radio"/> Delete
<input type="checkbox"/> Windows Resources on ami-il.mercury.global(Windows Resources)	<input type="radio"/> Leave Intact <input checked="" type="radio"/> Disable <input type="radio"/> Delete
<input type="checkbox"/> Windows Resources on ami-il.mercury.global(Windows Resources)	<input type="radio"/> Leave Intact <input type="radio"/> Disable <input checked="" type="radio"/> Delete
<input type="checkbox"/> Ping ami-il.mercury.global(Ping)	<input checked="" type="radio"/> Leave Intact <input type="radio"/> Disable <input type="radio"/> Delete
<input type="checkbox"/> crazy - Fully monitored	
<input type="checkbox"/> Windows Resources on crazy(Windows Resources)	<input type="radio"/> Leave Intact <input checked="" type="radio"/> Disable <input type="radio"/> Delete
<input type="checkbox"/> Ping crazy(Ping)	<input checked="" type="radio"/> Leave Intact <input type="radio"/> Disable <input type="radio"/> Delete
<input type="checkbox"/> Ping crazy(Ping)	<input type="radio"/> Leave Intact <input checked="" type="radio"/> Disable <input type="radio"/> Delete
<input type="checkbox"/> Windows Resources on crazy(Windows Resources)	<input type="radio"/> Leave Intact <input type="radio"/> Disable <input checked="" type="radio"/> Delete

Template Reference

The Monitor Deployment Wizard is enabled by a series of templates preconfigured in the SiteScope monitor tree.

Template Reference Table

Following is a table listing all the configuration items onto which the Monitor Deployment Wizard can deploy templates. The table lists the templates and CI types, the monitors which are deployed, the monitor properties imported from the CMDB, and the variable definitions that are either imported from the CMDB or defined within the wizard.

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Apache server	Apache	Apache Server monitor	server name or IP address	application_IP
			application port (default value is 8080)	application_port
IIS server	IIS	IIS Server monitor	server name or IP address	application_IP
			host password	host_password
			user name	host_username
			NT domain	nt_domain
Host	Host	Ping monitor	dns name	host_dnsname
	Windows			
	UNIX			
	Network			
	Switch			
	Router			
	switch-router			

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Windows server	Windows	Microsoft Windows Resources monitor	dns name	host_dnsname
				host_password
				host_username
				nt_domain
UNIX	UNIX	CPU and Memory monitor, UNIX Remote server		connection_method
			dns name	host_dnsname
				host_os
				host_password
		host_username		
Microsoft SQL server	sqlserver	Microsoft SQL Server monitor	server name or IP address	application_IP
				nt_domain
				SqlServerHost Password
				SqlServerHost UserName

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Oracle database	Oracle	Oracle Database monitor	server name or IP address	application_IP
			application password (default value is manager)	application_password
			application user name (default value is system)	application_user name
			database port (default value is 1521)	database_dbport
			database SID	database_dbsid
UDDI	UDDI Registry	UDDI Server	data_name	data_name
			business_name	business_name
Web Services	Web Service	WSDL	method_name	method_name
				method_ns
			ParamUrl	ParamUrl
				port
			purl	purl
				service_name
			soap_action	soap_action
WsdUrl	WsdUrl			

Template Reference for Siebel

Following are tables listing all the Siebel configuration items onto which the Monitor Deployment Wizard can deploy monitors. The Siebel templates are divided according to groups. The table lists the CI Templates and CI types, the monitors which are deployed, the monitor properties imported from the CMDB, and the variable definitions that are either imported from the CMDB or defined within the wizard.

Siebel Application Server Monitor

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Application Server	Application Server	Siebel Application Server log	Server_Name	Server_Name
			Siebel_Root_Dir	Siebel_Root_Dir
			Siebel_Logical_Instance_Name	Siebel_Logical_Instance_Name
		Siebel Application Server	Application	Application
			Gateway	Gateway
			Enterprise	Enterprise
			Username	Username
			Server_Manager_Path	Server_Manager_Path
	PASSWORD	PASSWORD		
	Database	Siebel Enterprise Integration Manager process (growth rate)	Database_Connection_URL	Database_Connection_URL
			Database_Driver	Database_Driver
			Database_UserName	Database_UserName
			Database_Server_Name	Database_Server_Name
			PASSWORD	PASSWORD

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Application Server <i>cont'd</i>	Database <i>cont'd</i>	Siebel Transaction Logging process (is enabled)	Database_UserName	Database_UserName
			Database_Driver	Database_Driver
			Database_Connection_URL	Database_Connection_URL
			Database_Server_Name	Database_Server_Name
			Database_PASSWORD	Database_PASSWORD
		Siebel Transaction Router process (growth rate)	Database_UserN ame	Database_UserName
			Database_Driver	Database_Driver
			Database_Conn ection_URL	Database_Connection_URL
			Database_Server _Name	Database_Server_Name
			Database_PASS WORD	Database_PASSWORD
		Siebel Workflow Rules process (growth rate)	Database_UserN ame	Database_UserName
			Database_Driver	Database_Driver
			Database_Conn ection_URL	Database_Connection_URL
			Database_Server _Name	Database_Server_Name
			Database_PASS WORD	Database_PASSWORD

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Application Server Host	Host	Disk Space	Server_Name	Server_Name
		Ping	Server_Name	Server_Name
		Memory	Server_Name	Server_Name
		CPU Utilization	Server_Name	Server_Name
		Directory log	Server_Name	Server_Name
			Siebel_Root_Dir	Siebel_Root_Dir
		Service Siebel Server	Server_Name	Server_Name
			Enterprise	Enterprise
			Server_Logical_Instance_Name	Server_Logical_Instance_Name
		Directory	Server_Name	Server_Name
Siebel_Root_Dir	Siebel_Root_Dir			
Siebel Component	Siebel Component	Siebel Component log	alias	alias
			Server_Name	Server_Name
			Application	Application
			Siebel_Root_Dir	Siebel_Root_Dir
			Siebel_Logical_Instance_Name	Siebel_Logical_Instance_Name
		Siebel Component	alias	alias
			Username	Username
			Enterprise	Enterprise
			Application	Application
			Gateway	Gateway
			Server_Manager_Path	Server_Manager_Path
			Server_Logical_Instance_Name	Server_Logical_Instance_Name
			PASSWORD	PASSWORD
			Group_Name	Group_Name
			data_name	data_name

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Component Group	Siebel Component Group	Siebel Component Group on	alias	alias
			Server_Logical_Instance_Name	Server_Logical_Instance_Name
			Enterprise	Enterprise
			Application	Application
			Gateway	Gateway
			data_name	data_name
			Server_Manager_Path	Server_Manager_Path
			Server_Name	Server_Name
PASSWORD	PASSWORD			

Siebel Gateway Monitors

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Gateway Server Host	Host	CPU Utilization	Server_Name	Server_Name
		Directory	Server_Name	Server_Name
			Siebel_Root_Dir	Siebel_Root_Dir
		Disk Space	Server_Name	Server_Name
		Memory	Server_Name	Server_Name
		Ping	Server_Name	Server_Name
		Service	Server_Name	Server_Name

Siebel Web Server Monitors

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Web Server Extension	Siebel Web Server Extension	Service	Server_Name	Server_Name
		Siebel Web Server	Server_Name	Server_Name
			Application	Application
			Username	Username
			PASSWORD	PASSWORD
		URL	Server_Name	Server_Name
			Application	Application
			Username	Username
			PASSWORD	PASSWORD
		Siebel Web Server Host	Host	CPU Utilization
Directory	host_dnsname			host_dnsname
	Siebel_Root_Dir			Siebel_Root_Dir
Disk Space	host_dnsname			host_dnsname
Memory	host_dnsname			host_dnsname
Ping	host_dnsname			host_dnsname
Service	host_dnsname	host_dnsname		
Web Server	Web Server	IIS Server	host_dnsname	host_dnsname
		Port 80	host_dnsname	host_dnsname

Monitor Deployment Wizard User Interface

This section describes:

- ▶ Monitor Deployment Wizard on page 104

Note: The Monitor Deployment Wizard is available only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center.

Monitor Deployment Wizard

Description	<p>Enables you to deploy SiteScope monitors using the configuration item data from the CMDB using pre-defined templates.</p> <p>To access: Select Admin > System Availability Management. Right-click the required SiteScope server or group and select Monitor Deployment Wizard or click the Monitor Deployment Wizard icon in the Summary page next to the required SiteScope server.</p>
Important Information	<p>The wizard is accessible only if you have a running SiteScope hosted in System Availability Management Administration.</p> <p>After running the Monitor Deployment Wizard, the deployed monitors do not begin to run immediately, but rather within the defined monitor running frequency time. You must give the system time to implement all the updates.</p>
Included in Tasks	<p>“Deploy Monitors Using the Monitor Deployment Wizard” on page 90</p>

Useful Links	“Monitor Deployment Wizard Concepts and Tasks” on page 81
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

Welcome Page

Description	Describes the wizard.
Important Information	An error message appears when you attempt to proceed to the next page if: <ul style="list-style-type: none"> ▶ the SiteScope you selected is not available or ▶ the CMDB is not available For general information about the Monitor Deployment Wizard, see “Monitor Deployment Wizard” on page 104.
Useful Links	“Work with the SiteScope Source Adapter – Workflow” in <i>Model Management</i> .
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

Select CIs to Monitor Page

Description	Enables you to select CIs onto which to deploy the SiteScope monitors.
Important Information	<p>If a CI appears under more than one view in the left pane, you cannot select it more than once in the selection that appears in the right pane, even if you attempt to select it from different views.</p> <p>The wizard checks for full and partial monitor coverage of the selected CIs. You have the option of deploying the template onto these CIs and handling duplicate monitors.</p>
Useful Links	<p>“Monitor Deployment Wizard Templates and Variables” on page 85</p> <p>“Full and Partial Monitor Coverage” on page 87</p>
Wizard Map	<p>The Monitor Deployment Wizard contains:</p> <p>Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets):



GUI Element	Description
<View Explorer>	<p>The Select CIs to Monitor page uses the standard View Explorer functionality to select CIs in the left pane and move them to the right pane. For details, see “View Explorer User Interface” in <i>Model Management</i>.</p> <p>Note: The wizard cannot create monitors for the following CIs:</p> <ul style="list-style-type: none"> ➤ CIs that do not have a matching template for deploying a monitor type ➤ CIs that are monitor CIs, generally those appearing in the monitor view <p>If you selected any CIs of these types, a warning message appears when you attempt to proceed to the next step of the wizard.</p>

Templates Selection Dialog Box

Description	<p>Enables you to apply templates to CI Types which were not automatically matched by the wizard.</p> <p>To access: Click the Templates Selection button from the Select CI to Monitor step of the Monitor Deployment Wizard.</p>
Important Information	<p>The Monitor Deployment Wizard automatically matches templates to the CI Types of the selected CIs. You can add additional templates manually in this dialog box. To select multiple templates to add, use the CTRL key. The selected templates are added to all of the selected CI Types.</p>

Useful Links	“Monitor Deployment Wizard Templates and Variables” on page 85
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click to add the selected templates in the left pane to the CI selection in the right pane.
	Click to remove selected templates from the CI selection.
<Template list>	The left pane lists all the available templates in the wizard. The child objects are the monitors that are deployed by the template.
<CI Type Selection>	The right pane lists the CI Types of all the CIs selected in the Select CI to Monitor step of the Monitor Deployment Wizard. If the wizard was able to match templates to the selected CI Types, the CI Type is listed with the applicable template as a child object.
Save Matching	Select the check box to save your template selection as a preference. This includes those templates that are selected manual for CI types and those that are cleared from the automatic selection of the wizard. The manually adjusted templates selection is matched to the selected CIs automatically the next time the same Business Availability Center user runs the wizard.
Restore Defaults	Click to reset the list and remove all the added templates from the CI Types (the ones added automatically by the wizard remain).

Enter Required Data for CIs Page

Description	Enables you to fine tune your template selection for specific CIs and fill in the missing information for those templates.
Important Information	If data is missing for any selected templates, an error appears and you are unable to proceed to the next step. If any templates are unselected, a warning appears before you proceed to the next step that informs you that there are unselected templates. This applies whether data is filled in for the unselected templates or not.
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Expanded CI list>	The CIs that are missing required data are expanded. (If no CIs are missing data, this section does not appear.)
<Unexpanded CI list>	CIs that are not missing data are not expanded. You can optionally expand the CIs to modify the data. (If all CIs are missing data, this section does not appear.)
CI column	Each template for each CI is displayed separately with the relevant number of license points for that template. Select the check box for the CI and template combinations for which you want to deploy monitors.

GUI Element	Description
Variable column	The variables for templates with missing data are listed in the Variable column.
Value column	Type the missing data in the Value column for all the selected templates. You can tab between the fields and enter the required data in the available fields. (You do not need to enter missing data for templates that are not selected.)

Final Configuration Summary Page

Description	Displays a list of the monitors about to be deployed and enables you to select the SiteScope group onto which they are deployed.
Important Information	Above the table, a note displays the total number of license points available on the SiteScope server (after the current action is complete). If the number of license points required for the current action exceeds your available points, a warning appears to tell you to remove some of the selected templates.
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

The following elements are included (unlabeled GUI elements are shown in angle brackets>):



GUI Element	Description
CI Name/Template Name column	Lists each selected CI with its templates.
Monitors to be Created column	Indicates the number of monitors being created for each template.

GUI Element	Description
License Points column	Indicates the number of SiteScope license points required for each monitor.
SiteScope Group selection window	To select the SiteScope group under which the monitors are deployed, click Browse and select a group from the tree in the Choose Target SiteScope Group dialog box. Note: If you attempt to deploy the same monitor on the same CI in the same group twice, the deployment fails with a unique name error. However, you may select a different group under which to deploy that monitor onto that CI.
Create CI group hierarchy	Select the check box to create a CI group hierarchy. This creates SiteScope groups under the target group with the identical hierarchy of the CIs. For details, see “CI Group Hierarchy Option” on page 88.

Deployment Results Page

Description	Displays a summary of the successful and unsuccessful template deployments.
Important Information	The deployment of monitors occurs at the template level. This means that if the deployment fails for any of the template elements (monitor, group, remote, or alert), no other monitors in the template are deployed. When you deploy a physical monitor (for example, a CPU monitor), a remote server with the same name is also created if such a remote server does not already exist under Remote Preferences (Microsoft Windows or UNIX).
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click to export the Monitor Deployment Wizard Summary page to a PDF. This report includes all created entities in SiteScope displaying the deployment directory and status. It also displays the status of duplicate monitors.
	Click to export the Monitor Deployment Wizard Summary page to a CSV file. This report includes all created entities in SiteScope displaying the deployment directory and status. It also displays the status of duplicate monitors.
CI Name column	Lists the names of the selected CIs.
Object Name column	Lists the monitors selected for deployment onto a given CI.
Status column	Indicates whether the deployment succeeded or not.
Retry Failed Deployments	Click Retry Failed Deployments to re-attempt to deploy those monitors whose deployment failed by modifying the data entered in the Type Required Data for CIs page. Note: This button appears only if there were failed deployments.
Handle Duplicate Monitors	If duplicate monitors were deployed, click Handle Duplicate Monitors to open the Handle Duplicate Monitors dialog box. For each duplicate monitor listed, you can select to leave it intact, disable it, or delete it. If all the monitors are to be handled in the same way, you can use the Leave All Intact, Disable All or Delete All buttons at the bottom of the page. For details on understanding duplicate monitors, see “Full and Partial Monitor Coverage” on page 87.

4

Introduction to System Availability Management Reports

HP System Availability Management reports enable you to monitor system availability data across the entire enterprise.

Note: The System Availability Management reports are available only to HP Business Availability Center users.

This chapter includes:

Concepts

- System Availability Management Reports Overview on page 113
- Working with System Availability Management Reports on page 116

System Availability Management Reports Overview

You use the System Availability Management application to view and analyze reports based on the performance data collected by the SiteScope data collector and stored in the HP Business Availability Center database.

In addition, using SiteScope Infrastructure Monitors, you can integrate data collected by enterprise management systems (such as BMC Patrol, Tivoli, Concord, and NetIQ) into HP Business Availability Center, and view the data in System Availability Management reports.

System Availability Management utilizes data collected by SiteScope and enables you to:

- ▶ monitor system availability across the entire enterprise infrastructure from a centralized, real-time perspective
- ▶ apply a business perspective to system management
- ▶ view data at the application level rather than viewing numerous low-level system metrics
- ▶ view information about events collected from external applications or software and SiteScope events

Note:

- ▶ You access the System Availability Management reports from the System Availability Management application in the Applications menu.
 - ▶ For details on working with HP Business Availability Center reports, see “Working in Reports” in *Reports*.
-

This section includes the following topics:

- ▶ “Report Access and Permissions” on page 114
- ▶ “Data Aggregation” on page 115
- ▶ “List of Available System Availability Management Reports” on page 115

Report Access and Permissions

The availability of report data to a specific user is dependent on the profile access permissions granted that user. Furthermore, access to specific data within a profile may also be filtered by using the group permission filters. For details on granting permissions, see “Permissions Overview” in *Platform Administration*. For details on defining group permission filters, see “System Availability Management Administration (SAM Admin)” in *Platform Administration*.

Data Aggregation

HP Business Availability Center uses data aggregation to make data handling and management more efficient and to improve the speed and performance of report generation. For information about data aggregation in HP Business Availability Center, see “Data Aggregation” in *Reference Information*.

List of Available System Availability Management Reports

The following reports are available:

Tab Name	Description	For Details, See...
SiteScope Over Time Reports	View and analyze reports, based on data collected by SiteScope, that help you track the performance of your infrastructure machines and provide insight into application availability and performance.	“SiteScope Over Time Reports” on page 119
Event Log	View event data over time, events that happened at a specific time, the details of a specific event, and event history.	“The Event Log” on page 151
User Reports	Provides tools for creating, and displays, reports that are tailored to the specific monitoring requirements of your organization or business unit. Report data is based on Business Process Monitor, WebTrace/Traceroute Monitor, SiteScope, and Custom data.	“User Reports” on page 181

Working with System Availability Management Reports

System Availability Management reports help you identify server resource usage trends, as well as bottlenecks and other server-related issues that may be contributing to application performance problems. You can continually monitor report data to identify poor server performance or to spot developing trends that may lead to server performance problems.

Alternatively, when you become aware of an application performance problem with your application (for example, after analyzing End User Management reports or receiving an alert), you can use System Availability Management reports to help you identify, or rule out, infrastructure machine-related issues as the root cause of the problem. By analyzing the infrastructure machine resource usage data for the same time period during which the performance problem occurred, you can assess whether one or more infrastructure machine resource measurements are outside normal performance thresholds for that time period.

This section includes the following topics:

- ▶ “Color Coding in Reports” on page 116
- ▶ “Improving Report Generation Times” on page 117

Color Coding in Reports

System Availability Management reports use the following colors when displaying color-coded performance levels:

Color	Description
Green	All measurements fell within the OK threshold range.
Yellow	At least one measurement fell within the minor threshold range, but no measurements fell within the critical threshold range.
Red	At least one measurement fell within the critical threshold range.
Gray	No measurement data reported.

Improving Report Generation Times

Note to HP Software-as-a-Service customers: This section is not relevant for HP Software-as-a-Service customers.

To optimize the performance of System Availability Management report generation, we recommend that a database administrator perform an update statistics procedure on the database on a regular basis. The regularity of the update depends on the amount of data generated by the applications you are monitoring.

► **Microsoft SQL Server users:**

- for a small site, you should update once every three to four days
- for a medium site, you should update daily
- for a large site, you should update every four hours

For details on Microsoft SQL Server maintenance, see “Maintenance Plan” in the *HP Business Availability Center Database Guide* PDF.

► **Oracle Server users.** Analyze all tables according to database size.

For details on optimizing performance in Oracle, see “Collecting Statistics for Databases” in the *HP Business Availability Center Database Guide* PDF.

5

SiteScope Over Time Reports

This chapter describes SiteScope Over Time reports which are based on data collected by the SiteScope data collector.

Note: The System Availability Management reports are available only to HP Business Availability Center users.

This chapter includes:

Concepts

- Understanding SiteScope Over Time Reports on page 120
- Monitor Performance Report on page 123
- Cross-Performance Report on page 126
- Adjusting the Cross-Performance Report Scale on page 138
- Group Performance Report on page 139
- Status Summary Report on page 143
- Warning Summary Report on page 144
- Error Summary Report on page 146
- System Availability Management Data in Custom Reports on page 147

Understanding SiteScope Over Time Reports

You use the SiteScope Over Time reports to view and analyze infrastructure machine-related data collected by the SiteScope data collector and stored in the HP Business Availability Center database. You cross-reference this data with transaction performance problems, such as slow transaction response times and failed transactions, to understand the root cause of application performance issues.

The contents of SiteScope Over Time reports depend on the types of SiteScope monitors and measurements that are defined in System Availability Management Administration.

HP Business Availability Center users can use group permissions filters to control the data that System Availability Management reports display. This enables filtering data that may be irrelevant to a specific user, making reports more manageable and report generation faster. For details, see “System Availability Management Administration (SAM Admin)” in *Platform Administration*.

Note:






- For details on generating reports, see “Working in Reports” in *Reports*.
 - Certain System Availability Management reports can be added to custom reports. For details, see “System Availability Management Data in Custom Reports” on page 147.
 - Data collected by the SiteScope data collector can also be viewed in trend reports. Trend reports enable you to compare multiple measurements from different data sources on the same graph. For details, see “Trend Reports Wizard” in *Reports*.
 - To avoid affecting the correctness of system availability data during the Daylight Savings Time change (forward or backward), it is recommended to define downtime or to schedule an event during the time change period. For more information on scheduling Downtime and Events, see “Downtime/Event Scheduling” in *Platform Administration*.
 - If a SiteScope contains many measurements, report generation can take a few minutes.
-

The following System Availability Management reports are available:

Report	Description	For Details, See...
Monitor Performance Report	Displays the best- or worst-performing SiteScope monitors across various SiteScope categories.	page 123
Cross-Performance Report	Displays data from more than one SiteScope server filtered by monitored servers, monitor types, and measurements.	page 126
Group Performance Report	Displays the infrastructure machine resource usage data for the monitors in the selected group and its subgroups.	page 139
Status Summary Report	Displays a quick snapshot of the performance of monitored infrastructure machines, organized by SiteScope group.	page 143
Warning Summary Report	Displays a list of the monitors, for the selected group and its subgroups, whose measurements fell within the minor threshold level during the selected time period.	page 144
Error Summary Report	Displays a list of the monitors, for the selected group and its subgroups, whose measurements fell within the critical threshold level during the selected time period.	page 146

Monitor Performance Report

You create the Monitor Performance report to view the best- or worst-performing SiteScope monitors across various SiteScope categories, such as monitor type, monitored server, or monitor title. You can create a Monitor Performance report for multiple SiteScope profiles.

Monitor Title	Server Name	Group	Profile Name	Warning	Error	Total Runs	Quality
Siebel Server Manager: sblapp1	sblapp1	Siebel Group	PRF_S	0%	100%	13150	
URL Sequence: G...ope monitoring	demo.sitescope.com	Application monitors subgroup	PRF_S	0%	100%	9191	
SNMP Trap listener	app1	SNMP Subgroup	PRF_S	0%	100%	6590	
URL Content: demo.sitescope.com	demo.sitescope.com	Application monitors subgroup	PRF_S	0%	0.61%	2622	
URL: demo.sitescope.com	demo.sitescope.com	Application monitors subgroup	PRF_S	0%	0.23%	1327	

This section includes the following topics:

- ▶ “Create the Monitor Performance Report” on page 123
- ▶ “Understanding the Monitor Performance Report” on page 124

Create the Monitor Performance Report

To view the Monitor Performance report, you specify the criteria on which you want the report to be based and create the report.

To create the Monitor Performance report:

- 1** Access the Monitor Performance report: **Applications > System Availability Management > SiteScope Over Time Reports > Monitor Performance.**
- 2** Select the SiteScope for which you want to view the report.
- 3** In the **Monitor title** and **Server name** boxes, specify the monitors (by their title, as defined in SiteScope) and/or servers on which you want the custom report data to be based.

Leave a box empty to instruct HP Business Availability Center to base the report on all values.

If required, you can use the wildcard asterisk symbol (*) to instruct HP Business Availability Center to base the report on a subset of all values. For example, if you are using the naming convention `cpu_<servername>` to name all CPU monitors in SiteScope, specify `cpu*` to instruct HP Business Availability Center to include all CPU monitors in the custom report.

Note: Using the wildcard asterisk symbol (*) as the first character in the string slows report generation times, as HP Business Availability Center is unable to use the Index tables when querying the database.

- 4 From the **Monitor type** list, select the monitor on which you want the report data to be based. To base the report on all monitors, choose **All types**.
- 5 Specify whether you want HP Business Availability Center to display the worst- or best-performing monitors, and choose the number of monitors to be displayed in the report.
- 6 Click **Generate** to create the report.

Understanding the Monitor Performance Report

The Monitor Performance report displays the following information:

- **Monitor Title.** The monitor title. Hold the pointer over the tooltip to view the full monitor title.
- **Server Name.** The name of the monitored server. Hold the pointer over the tooltip to view the full server name.
- **Group.** The group or subgroup in which the monitor is defined. Hold the pointer over the tooltip to view the path from the displayed group or subgroup to the root group. Click the group or subgroup name to open the management page for the group in SiteScope.
- **Profile Name.** The name of the SiteScope profile in which the monitor is defined.
- **Warning.** The percentage of measurement instances that return a critical-level threshold status.

- **Error.** The percentage of measurement instances that return an error-level threshold status.
- **Total Runs.** The total number of measurement instances SiteScope ran for the selected time range.
- **Quality.** A color-coded representation of quality. Hold the pointer over the tooltip to view the exact percentage for each colored section of the bar.

Monitors are sorted in the report by quality, which is derived using a formula that takes into account the measurement values returned for the monitor during the specified time range relative to the measurement threshold ranges configured in SiteScope.

The formula used is: $1 - ((0.35 * W + 0.5 * E) / (G + W + E))$, where G, W, and E represent the number of measurements that occurred during the selected time range whose value was within the OK, Warning, and Error threshold range, respectively. The formula returns values from 0.5 to 1, inclusively. The better a monitor performs, the closer its value is to 1. For example, a monitor with 25% error and 75% OK values would be displayed as better than a monitor with 100% Warning values.

Note: The Monitor Performance report does not use raw data. All data in the report is based on aggregated data.

Cross-Performance Report

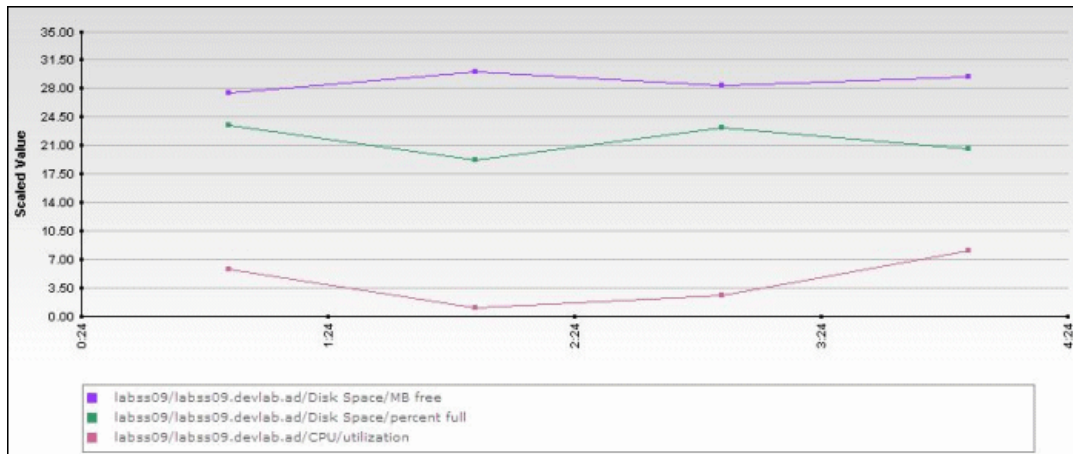
The Cross-Performance reports can be displayed in the following formats:

- ▶ **Graph per measurement.** For details, see “Graph Per Measurement” on page 133.
- ▶ **One graph for all measurements.** For details, see “One Graph for All Measurements” on page 134.
- ▶ **Table view.** For details, see “Table View” on page 135.

You can rescale a SiteScope cross-performance report to make it more relevant to what you are measuring. For details, see “Rescaling a Cross-Performance Report” on page 136.

You can view data from more than one SiteScope. You can filter the data by monitored servers, monitor type or title, and measurements.

For example, you can display the behavior of a measurement running on several monitored servers, or the behavior of several measurements from various types of monitors running on one monitored server.



Note: If you are running a SiteScope Log File or Database Query monitor that is monitoring a different machine, you should select the SiteScope machine running the monitors in the Servers list, and not the monitored machine (the target machine where the log file or database is located).

You can rescale the report to make it more relevant to what you are measuring.

This section includes the following topics:

- “Create a SiteScope Cross-Performance Report” on page 128
- “Graph Per Measurement” on page 133
- “One Graph for All Measurements” on page 134
- “Table View” on page 135
- “Rescaling a Cross-Performance Report” on page 136
- “Examples” on page 137

Create a SiteScope Cross-Performance Report

To view the SiteScope Cross-Performance report, specify the time period and granularity, the filters, the type of report, and create the report.

To create the SiteScope Cross-Performance report:

- 1 Access the SiteScope Cross-Performance report: **Applications > System Availability Management > SiteScope Over Time Reports > SiteScope Cross-Performance**.
- 2 Select the time period and the granularity with which you want to run the report. For details, see “Time Range and Granularity Bar” in *Reports*.

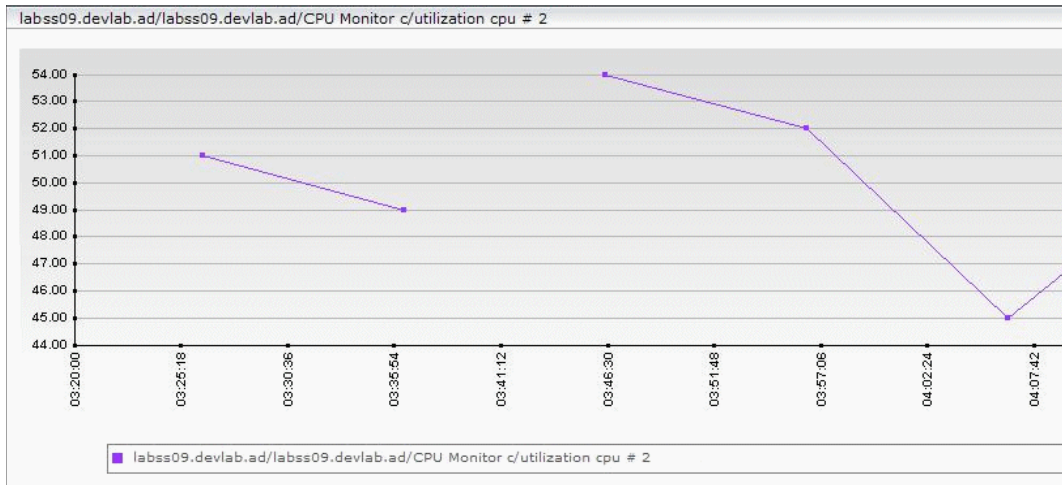
The granularity determines how many measurement samples are displayed in the report for each time interval. By default, the number of samples is limited to the maximum value of the **Max Data Points in Report** setting (32 by default for all reports where you can specify the granularity).

Note: You can change these settings in the Infrastructure Settings Manager. To modify these settings, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **End User/System Availability Management** and locate **Max Data Points in Report** in the **End User/System Availability Management - Data** table. For details on using the Infrastructure Settings Manager, see “Infrastructure Settings” in *Platform Administration*.

You can choose to view raw data on the given report by selecting the **Raw Data** option on the time period and granularity bar. There are several factors to keep in mind when choosing this option:

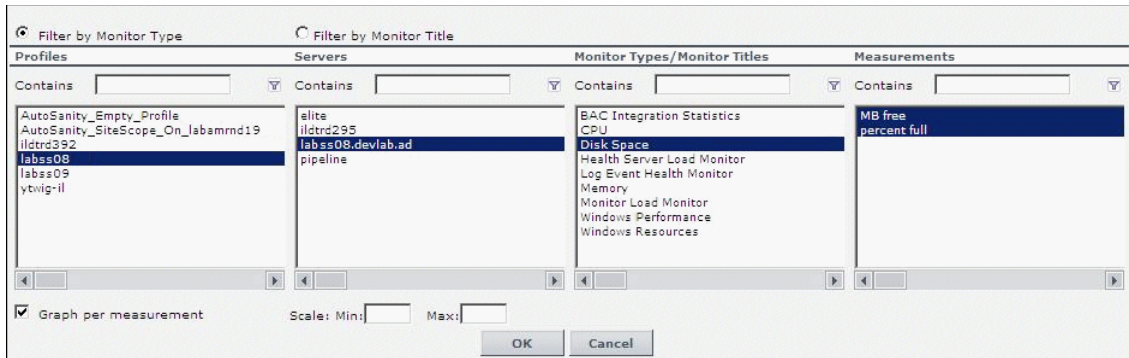
- A point on the graph appears when there is a change in the data value or measurement frequency from the previous time point on the graph. However, if there has been no change in either of these areas over the course of one hour, a point is nevertheless displayed on the graph.
- A straight line on the graph with no points indicates the following:
 - There has been no change in the value of the incoming data from the previous time point on the graph.

- There has been no change in the frequency that the incoming data is measured in since the previous time point on the graph.
- A gap in the graph indicates that no data has been retrieved for the specific time period.



- 3** Choose whether to display the monitor type or title when selecting the component to add to the report:
- **Monitor type.** Displays the type of monitor, for example, Ping, CPU.
 - **Monitor title.** Displays the name given to the specific monitor, for example, ping: myserver, CPU finance_server.

4 Filter the data you want to include in the report:



- ▶ From the **Profile** list (sorted alphabetically), select one or more SiteScope profiles.
- ▶ From the **Server** list, select one or more servers. The list includes all monitored servers associated with the selected profiles, in alphabetical order.
- ▶ Depending on whether you chose **Filter by Monitor Type** or **Filter by Monitor**, the **Monitor Types/Monitor Titles** list displays monitor types or monitor names, associated with the selected profiles and servers, in alphabetical order. Select one or more monitors.
- ▶ From the **Measurements** list, select one or more measurements. The list includes the measurements that are associated with the selected profiles, servers, and monitor types, in alphabetical order.

If you select a measurement for which data exists from more than one group or profile for the same target server, the data is averaged together in the report. For example, if you have two SiteScope profiles each containing two groups, and in three of those groups the Ping monitor is set up to monitor the same server, if you select both profiles and the round trip time measurement, all round trip time data collected from all three groups in both profiles is displayed in the report as an average value.



Note: To list all the elements whose name includes the string, type a string in one of the **Contains** boxes and click the filter button.

- 5** To consolidate data per measurement, select **Graph per measurement**. For details, see “Graph Per Measurement” on page 133 and “One Graph for All Measurements” on page 134. This option is selected by default.
- 6** If required, type scale information in the **Scale Min** and **Max** boxes. For details, see “Rescaling a Cross-Performance Report” on page 136.
- 7** Click **Generate** to create the report. The filter area of the page closes and the report opens.
- 8** You can print the report, send it by e-mail, or open it in CSV or PDF format. For details, see “Format Options” in *Reports*.

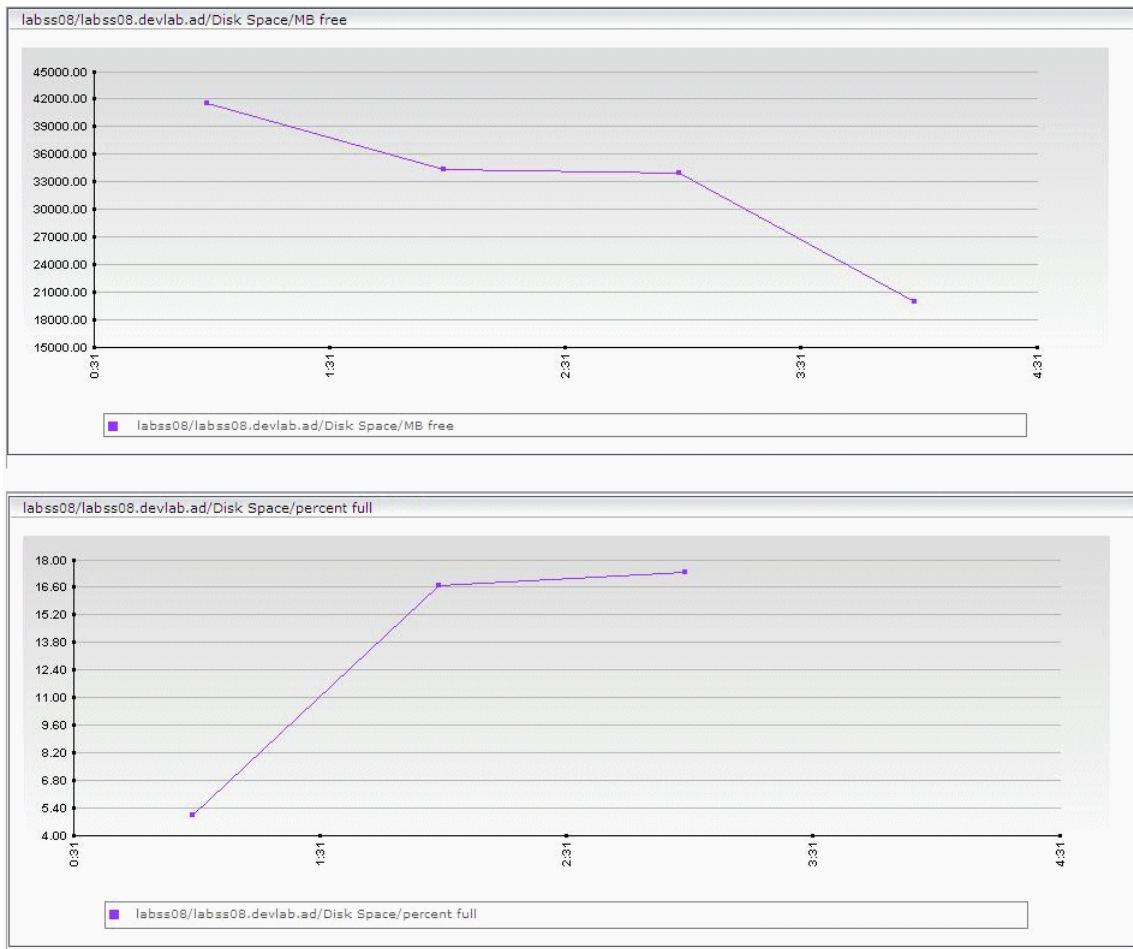
Note:

- ▶ You cannot create a report if you have not selected at least one measurement.
 - ▶ In certain reports the selected time range is displayed along the x-axis. System Availability Management breaks down the time range according to segments, which differ depending on the selected time range. For details on how System Availability Management breaks down each time range in reports where time is displayed along the x-axis, see “Report Times” in *Reference Information*.
 - ▶ Depending on the time range you select, System Availability Management generates reports using either raw data or aggregated data. The text: **Note: Report uses aggregated data** is displayed in the report when aggregated data is used. For details on how System Availability Management determines when to use aggregated data, see “Data Aggregation” in *Reference Information*.
 - ▶ The number of selected profiles are calculated after you click **Generate**. You can choose up to 10 profiles. If these numbers exceed the allowed limit, a message is displayed.
-

Graph Per Measurement

If you select the **Graph per measurement** box, System Availability Management displays each measurement in a separate graph. The graph legend displays the server on which the measurement is running.

The graph legend displays information about the servers. The x-axis displays date and time information and the y-axis displays the measurement value and the monitor type. For example, the following graph displays two measurements running on the labss08 server.

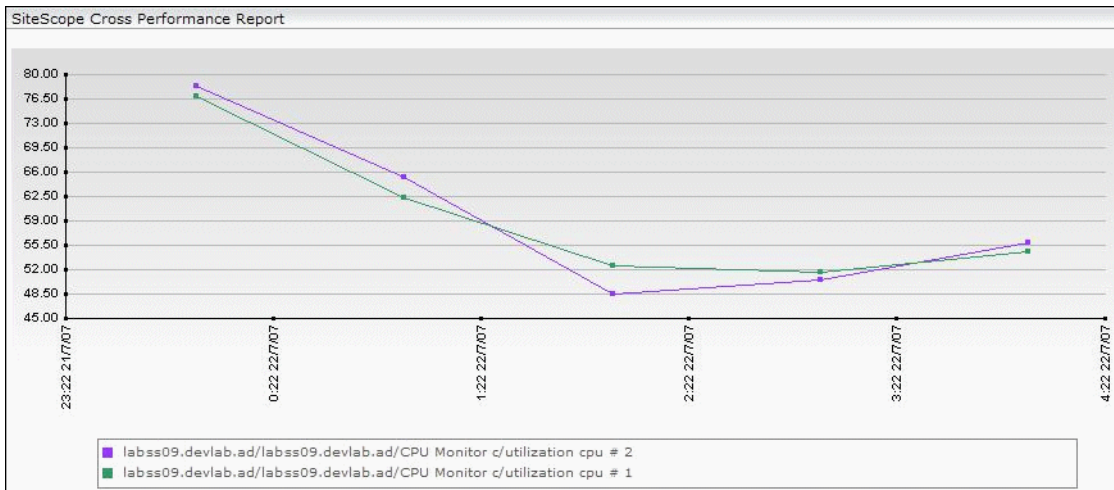


One Graph for All Measurements

If you clear the **Graph per measurement** box, System Availability Management displays one graph for all measurements.

The graph legend displays the measurement value and the monitor type. The x-axis displays the date and time information, and the y-axis shows the measurement values.

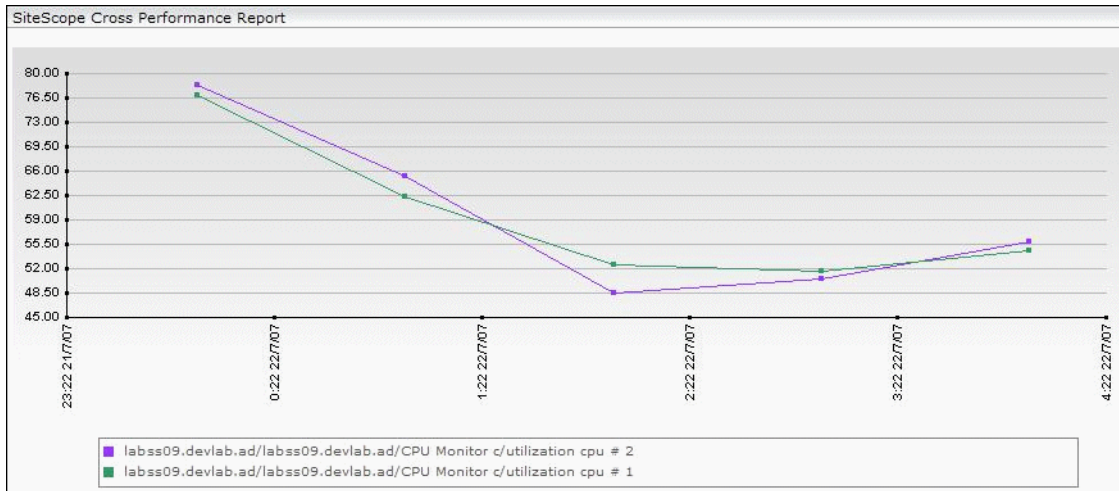
For example, the following graph displays three measurements running on one of the servers.



Each graph displays data for a given measurement. A new graph is created for each different measurement with the title `<server_name> continued`.

Table View

If you select **View as table**, the report displays the data in table format. Each table displays the measurement name (including the servers on which the measurement is running, the data and time of the measurement, and the value of the measurement. Click on the column header of the column you want to sort the table by, either in ascending or descending order.



Tables display the following information:

- ▶ **Measurement Name.** The name of the measurement, including the server on which it is running.
- ▶ **Date.** The date and time of the measurement.
- ▶ **Value.** The value of the specific measurement.

Rescaling a Cross-Performance Report

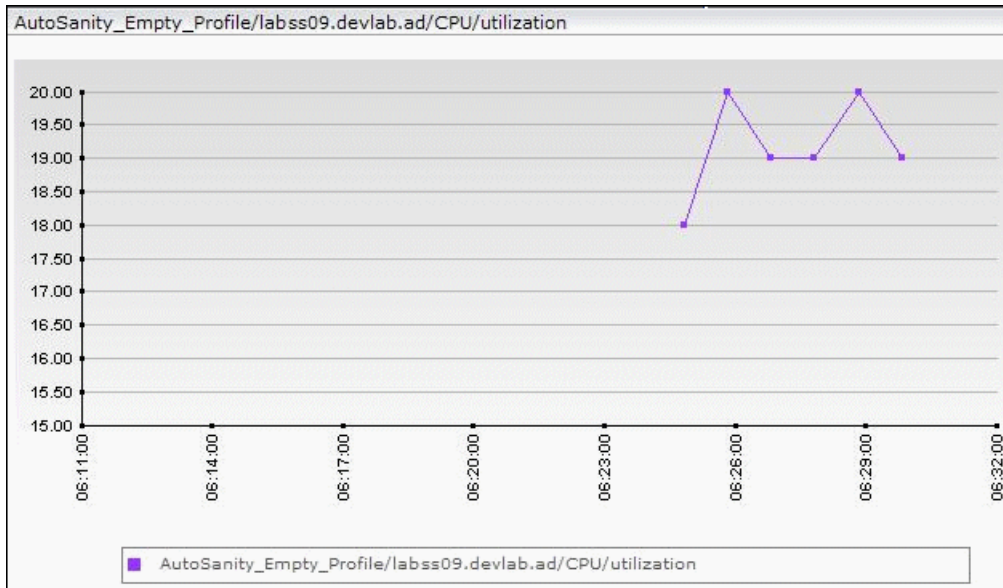
Cross-performance reports are generally scaled so that the lowest y-axis value is zero and the highest y-axis value is the highest result of the data.

You can rescale the report to make it more relevant to the measurement. For example, to measure CPU utilization, you can rescale the report so that the y-axis range is 0 to 100.

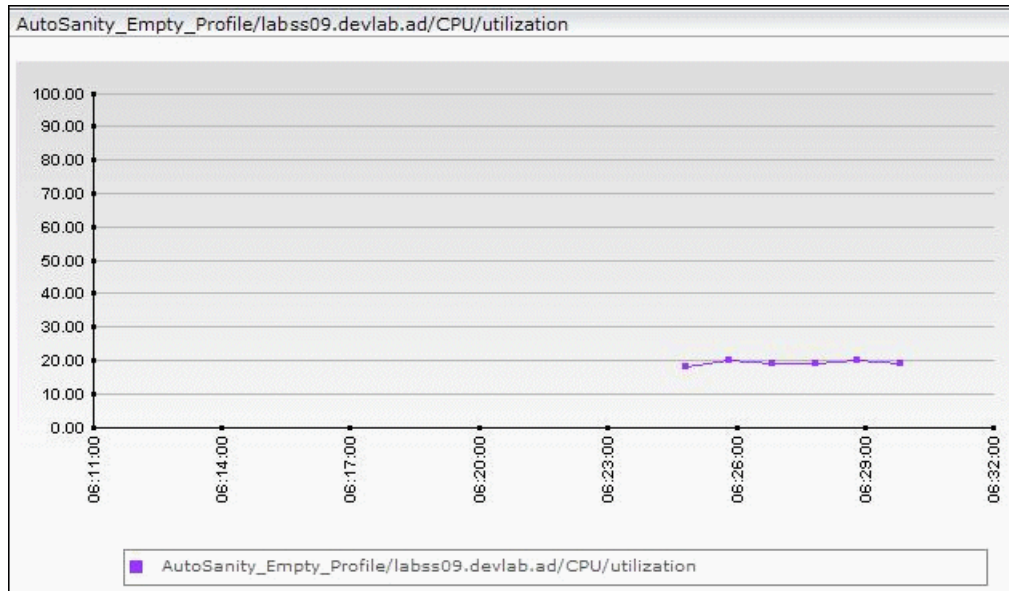
Note: If the data values of a monitor are outside the minimum or maximum configured values of the graph, the data points are displayed outside the boundaries of the graph.

To rescale the report, specify a minimum, a maximum, or both a minimum and a maximum value in the **Scale Min** and **Max** boxes.

For example, the original report displays as follows:



To rescale the range to 0-100, type **0** in the Scale Min box and **100** in the Max box, or type **100** in the Max box. The report redisplay as follows:



Examples

You can use the SiteScope Cross-Performance reports to identify a problem in a server. For example, select the SiteScope profile that refers to the SiteScope that samples the problematic server, select the relevant server, the monitor types (**CPU**, **memory**, and so on), the measurements that can help find the problem (**utilization**, **pages/sec**, **percent used**, and so on), and create the report.

You can also compare memory usage in several servers. For example, select the SiteScope profile that refers to the SiteScope that samples the servers you want to compare, the relevant servers, the **memory** monitor type, the **pages/sec**, **percent used**, and **MB free** measurements, and then create the report to compare the memory usage.

You can find out if a sub-system needs an additional server. For example, select the SiteScope profile that refers to the SiteScope that samples all servers in your sub-system, select all the servers of your sub-system, the **CPU** monitor type, the **utilization** measurements, and create the report to see whether the sub-system needs an additional server.

Adjusting the Cross-Performance Report Scale

Measurement values in the cross-performance report are displayed along the y-axis using a normalized scale. By default, HP Business Availability Center automatically sets the scale factor for each measurement. If required, you can manually modify the scale factor for any measurement in the Selected Measurements table, for example, to better view multiple measurements whose data values span a wide range. For details, see “Rescaling a Cross-Performance Report” on page 136.

When you manually modify the scale factor, HP Business Availability Center scales measurement values by dividing the actual value by the value chosen in the scale list. Thus, a value of 100 with a scale setting of 0.1 is shown as 1000 along the y-axis. A value of 100 with a scale setting of 10 is shown as 10 along the y-axis.

For example, if at a given point in time Measurement A (whose scale value is set to "Auto") has a value of 10 and Measurement B (whose scale value is set to 0.1) has a value of 90, the y-axis displays a range from 0-1000 to accommodate both values. If both measurements' scale settings are set to "Auto," the y-axis values ranges from 0-100.

Group Performance Report

You create the Group Performance report and its subreports to view data that helps you spot trends in server performance that could lead to application performance problems. You can also analyze whether slow or failed transactions are being caused by server resource bottlenecks or other infrastructure machine-related problems.

This section includes the following topics:

- “Group Performance” on page 139
- “SiteScope Performance” on page 139
- “SiteScope Data Over Time” on page 141





Group Performance

The Group Performance table is the top level of the report. For each group, the table displays a color-coded quality level, the number of subgroups, and the number of included measurements. The quality-level indicators enable you to see how monitors in the defined groups are performing. Click a group name to create the SiteScope Performance subreport.

SiteScope Performance

The SiteScope Performance subreport displays a list of measurements collected by SiteScope for the specified group, over the selected time range. If the specified group contains subgroups, these are displayed at the top of the page. Click the subgroups to view their SiteScope Performance subreports.

The SiteScope Performance subreport displays the following information:

SiteScope Measurements for Group: test					
	Monitor Title	Measurement Name	Host Name	Avg. Value	Errors / Total
<input type="checkbox"/>	 Ping: sift	round trip time	sift	0.01	0 / 67
<input type="checkbox"/>	 Ping: sift	% packets good	sift	100.0	0 / 67
<input type="checkbox"/>	 CPU Utilization on nack	utilization	nack	-	101 / 101
<input type="checkbox"/>	 Memory	pages/sec	nack	-	97 / 97

- ▶ **Check box.** An enabled check box at left indicates that there is monitor data that can be viewed in the SiteScope Data over Time report. For details on generating this report, see “SiteScope Data Over Time” on page 141.
- ▶ **Status.** The status column, to the left of the monitor title, displays measurement threshold icons, which indicate whether the average measurement is within the OK, Warning, or Error range, as reported by SiteScope. You define measurement thresholds for each measurement when you configure the monitor in the System Availability Management area in the Administration Console.
- ▶ **Monitor Title.** The monitor title.
- ▶ **Measurement Name.** The name of the measurement. Click the link to create the SiteScope Data over Time report for that measurement. HP Business Availability Center displays the link only if data exists for the selected time range. For details on the SiteScope Data over Time report, see “SiteScope Data Over Time” on page 141.
- ▶ **Host name.** The name of the SiteScope host machine.
- ▶ **Avg. Value.** The average value of each listed measurement, or counter, for the specified time period.
- ▶ **Last Value (Updated).** The last received SiteScope measurement, as well as the most recent date and time that SiteScope received the measurement (shown in parentheses). HP Business Availability Center displays the date and time in italics if the current time frame is different from the displayed date and time.

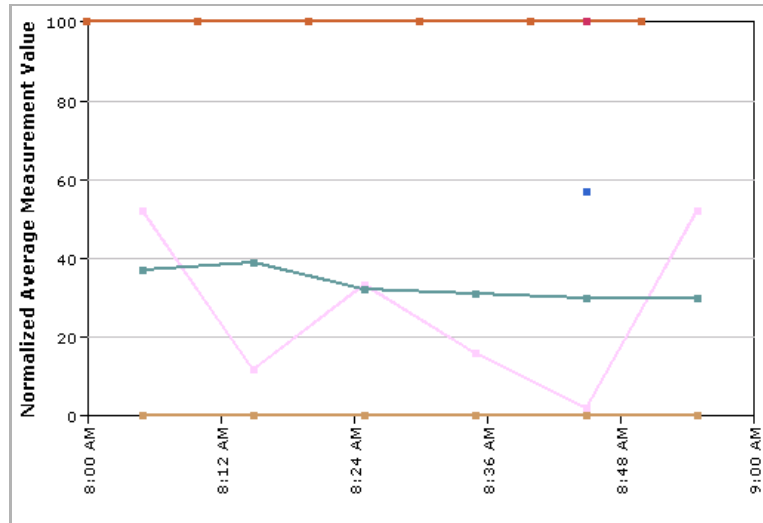
If no value was collected within the past four hours, no value is displayed.

If the last received SiteScope measurement returned the Error status, HP Business Availability Center displays the term Error in the Last Value (Updated) column.

- ▶ **Errors/Total.** The number of errors that occurred while collecting measurement data, out of the total number of measurements taken during the defined time period. Click the link to view a list of errors that returned measurement error messages. HP Business Availability Center displays the link only if errors occurred.

SiteScope Data Over Time

The SiteScope Data Over Time report displays specific measurement data over the selected time range. You can view this report for a single measurement, or for several measurements simultaneously.



Note: You can add the SiteScope Data over Time report to custom reports. For details, see “Custom Reports Wizard” in *Reports*.

To view the SiteScope Data over Time subreport for one measurement:

- 1** Click a measurement in the **Measurement Name** column in the SiteScope Performance subreport. HP Business Availability Center generates and displays the SiteScope Data over Time subreport.
- 2** Place your cursor over a point in the graph to see a tooltip with measurement details.
- 3** Click the **View as Table** link to view the data in table format.

To view the SiteScope Data over Time subreport for several measurements:

- 1** In the SiteScope Performance subreport, select the check boxes beside the measurements that appear in the multi-measurement graph.
- 2** Click the **Generate** button at the bottom of the table. HP Business Availability Center generates and displays the multi-measurement SiteScope Data over Time subreport. You use the color codes to identify each measurement in the graph.

The y-axis of the merged graph is a normalized scale from 0-100. HP Business Availability Center uses the following formula to convert the original y-axis value to a value in the merged y-axis:

$$[\text{original y-axis value}] \times [\text{scale value}] = \text{y-axis value in merged graph}$$

Place the pointer over a point in the graph to view a tooltip with measurement details, including the measurement's original value.

- 3** Click the **View as Table** link to view the data in table format. The table displays actual measurement values, not normalized values.

Status Summary Report



You create the Status Summary report and its subreport to get an overall view of the performance of defined SiteScope groups and the monitors defined therein.

This section includes the following topics:

- “SiteScope Status Summary” on page 143
- “SiteScope Uptime Details” on page 143

SiteScope Status Summary

The SiteScope Status Summary table is the top level of the report. For each SiteScope group in the selected profile, the report displays a color-coded quality level, the number of subgroups, and the number of included measurements. The quality-level indicators enable you to get a quick snapshot of how monitors in the defined SiteScope groups are performing.

	Group Name	Number Of Subgroups	Number Of Measurements
	Examples	4	0
	Group1	1	60

Click a group name to create the SiteScope Uptime Details subreport.

SiteScope Uptime Details

The SiteScope Uptime Details subreport displays OK, Minor, and Critical information for each monitor in the group, over the selected time range, enabling you to determine the overall performance trend of a given monitor. If the specified group contains subgroups, these are displayed at the top of the page. Click subgroups to view their SiteScope Uptime Details subreports.

SiteScope Uptime for Group: Net_Mon			
Monitor Title	Uptime %	Warning %	Error %
Ping Intranet	88.889	0.0	11.111
Network Interface	100.0	0.0	0.0
Ping: www.freshwater.com	100.0	0.0	0.0

The SiteScope Uptime Details subreport displays the following data:

- ▶ **OK %.** The percentage of measurement instances that completed successfully.
- ▶ **Minor %.** The percentage of measurement instances whose values fell within the Minor threshold level.
- ▶ **Critical %.** The percentage of measurement instances whose values fell within the Critical threshold level.

Warning Summary Report



You create the Warning Summary report and its subreport to identify the SiteScope groups whose measurements fell within the minor threshold level during the selected time period.

This section includes the following topics:

- ▶ “Warning Summary” on page 144
- ▶ “Warning Details Report” on page 145

Warning Summary

The Warning Summary table is the top level of the report. For each SiteScope group in the selected profile, the report displays a color-coded quality level, the number of subgroups, and the number of included measurements. The quality-level indicators enable you to get a quick snapshot of how monitors in the defined SiteScope groups are performing.

	Group Name	Number Of Subgroups	Number Of Measurements
	Examples	4	0
	Group1	1	60

Click a group name to create the Warning Details subreport.

Warning Details Report

The Warning Details subreport displays minor status information for each measurement instance of each monitor in the group, over the selected time range. If the specified group contains subgroups, these are displayed at the top of the page. Click subgroups to view their SiteScope Warning Details subreports.

Time	Monitor Title	Measurement Name	Status
7/24/04 7:47 AM	alerts	Number o...d Agents	0.0
7/24/04 7:47 AM	alerts	Received...l Alerts	0.0
7/24/04 7:37 AM	alerts	Number o...d Agents	0.0
7/24/04 7:37 AM	alerts	Received...l Alerts	0.0

The Warning Details subreport displays the following data:

- ▶ **Time.** The date and time of the measurement instance.
- ▶ **Monitor Title.** The monitor to which the measurement is associated.
- ▶ **Measurement Name.** The measurement instance whose threshold fell within the Minor level.
- ▶ **Status.** The value of the measurement.

Note: System Availability Management displays raw data only in the SiteScope Warning Details report. Aggregated data is not used. Therefore, if raw historical data is removed from the profile database using the Purging Manager, you are unable to view data in the SiteScope Warning Details report for the time period for which the data was removed.

Error Summary Report



You create the Error Summary report and its subreport to identify the SiteScope groups whose measurements fell within the critical threshold level during the selected time period.

This section includes the following topics:

- “Error Summary” on page 146
- “Error Details” on page 146

Error Summary

The Error Summary table is the top level of the report. For each SiteScope group in the selected profile, the report displays a color-coded quality level, the number of subgroups, and the number of included measurements. The quality-level indicators enable you to get a quick snapshot of how monitors in the defined SiteScope groups are performing.

	Group Name	Number Of Subgroups	Number Of Measurements
	Examples	4	0
	Group1	1	60

Click a group name to create the Error Details subreport.

Error Details

The Error Details subreport displays error status information for each measurement instance of each monitor in the group, over the selected time range. If the specified group contains subgroups, these are displayed at the top of the page. Click subgroups to view their Error Details subreports.

Time	Monitor Title	Measurement Name	Status
7/22/04 11:11 PM	IIS on san3	Web Serv...Web Site	Anonymous Use...equests n/a,
7/22/04 11:11 PM	IIS on san3	Web Serv...Web Site	Anonymous Use...equests n/a,
7/22/04 11:11 PM	IIS on san3	Web Serv...c!_Total	Anonymous Use...equests n/a,
7/22/04 11:11 PM	IIS on san3	Web Serv...Web Site	Anonymous Use...equests n/a,

The Error Details subreport displays the following data:

- **Time.** The data and time of the measurement instance.
- **Monitor Title.** The monitor to which the measurement is associated.
- **Measurement Name.** The measurement instance whose threshold fell within the Error level.
- **Status.** Error information as reported by SiteScope.

Note: System Availability Management displays raw data only in the SiteScope Error Details report. Aggregated data is not used. Therefore, if raw historical data was removed from the profile database using the Purging Manager, you are unable to view data in the SiteScope Error Details report for the time period for which the data was removed.

System Availability Management Data in Custom Reports

You can add System Availability Management reports to custom reports from the User Reports tab. For details, see “Custom Reports Wizard” in *Reports*.

This section includes the following topics:

- “Monitor Performance Report” on page 147
- “SiteScope Data Over Time Report” on page 148
- “Group Performance Report” on page 148
- “Overall Performance Report” on page 148

Monitor Performance Report

To add this report to a custom report, select the SiteScope Monitor Performance component type in the Custom Report Manager. For details on the Monitor Performance report, see “Monitor Performance Report” on page 123.

SiteScope Data Over Time Report

To add this report to a custom report, select the Reports component type in the Custom Report Manager, then select the SiteScope Reports category from the Add Component dialog box. For details on the SiteScope Data over Time report, see “SiteScope Data Over Time” on page 141.

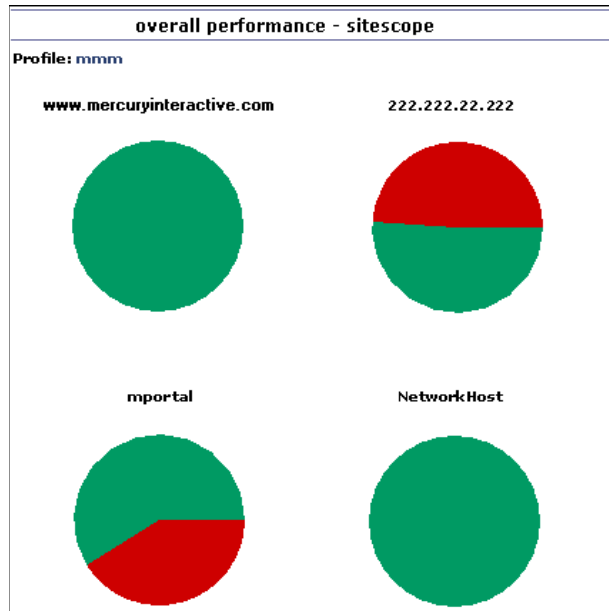
Group Performance Report

To add this report to a custom report, select the Reports component type in the Custom Report Manager, choose the SiteScope Reports category from the Add Component dialog box, then select SiteScope Profile Summary from the Type list. For details on the Group Performance report, see “Group Performance Report” on page 139.

Overall Performance Report

The Overall Performance report is based on SiteScope data, and is only available in custom reports. To add it to a custom report, select **Reports** in the **Component type** list in the Custom Report Manager page and click **Add Component**. Select the **SiteScope Reports** in the **Category** list from the Add Component dialog box, and then select **Overall Performance** in the **Type** list.

You view the Overall Performance report to get a quick snapshot of the performance of the monitored infrastructure machines in the selected SiteScope profiles. The chart displays—for the SiteScope profiles and defined time frame—a pie chart for each element of the infrastructure that SiteScope is monitoring.



To get additional information, point to a segment to view a tooltip describing the exact number and percentage of measurements for each segment of the chart.

6

The Event Log

The HP System Availability Management event log displays SiteScope events, as well as events collected from external applications or software by enterprise management systems (EMS) using SiteScope.

Note: The Event Log is available only to HP Business Availability Center users.

This chapter includes:

Concepts

- Event Log Overview on page 152

Tasks

- Display and Customize the Event Log on page 153
- Set Additional Filters for SiteScope on page 155

Reference

- Viewing Common Event Data in the Event Log Page on page 156
- Working with Event Details on page 158
- Working with Event History on page 160

Event Log Overview

The event log enables you to view event data over time, events that happened at a specific time, the details of a specific event, and (where possible) the event history.

The type of event that is collected depends on what is defined as an event in the external applications or software. Event types can be warnings, alerts, user logins, and so on.

The event log displays event data that is common to all data sources: the severity of the event, the application or software from which the event is collected, the time the event occurred, the hierarchy of the event source, the name (or the IP address) of the host or device that caused the event, the status or type of event, and the external system description of the event.

You can filter the events for a specific time frame, data source, severity, and target name. For details, see “Display and Customize the Event Log” on page 153.

You can then drill down to the common data to display data that is specific to the data source where the event occurred (for details, see “Working with Event Details” on page 158) and to display the history of a specific event (for details, see “Working with Event History” on page 160).

The event log enables you to diagnose specific issues in real time and to create trend reports.

Display and Customize the Event Log

The Event Log page displays the logs of events that are sent to the system (for details, see “Displaying the Event Log” on page 153). You can use filters (time frame, data source, severity, and target name) to display specific information. If you select the SiteScope data source, you can then select additional filters: SiteScope profile, groups, and monitor type (for details, see “Set Additional Filters for SiteScope” on page 155).

When you create the event log, the Event Log page displays the events sorted by the time of their occurrence in descending order. It also shows columns that are common to all the data sources that can send events (for details, see “Viewing Common Event Data in the Event Log Page” on page 156). The data of the SiteScope data source is filtered according to SiteScope Profile permissions (for details, see “Permissions Overview” in *Platform Administration*).

The Event Log page has two areas: the filter and action area and the data table.

This section includes the following topics:

- “Displaying the Event Log” on page 153
- “Customizing Event Logs” on page 154

Displaying the Event Log

You can display the logs of events sent to HP Business Availability Center.

To display the Event Log:

- 1** Select **Applications > System Availability Management > Event Log** to display the Event Log page.
- 2** Select the time period for which you want to gather information to display in the report in the **View** list. For details, see “Time Range and Granularity Bar” in *Reports*.

- 3 Click **Active Filters**, if you want to edit the filters. Only one or **All** data sources can be selected in the Event Source tab. If no data source exists, only **All** appears in the list. **SiteScopeAlert** or **SiteScopeStatusChange** data sources appear only if the current user has permissions to view at least one SiteScope profile. Severities are pre-defined. By default, all check boxes are selected.

If you select **SiteScopeAlert** or **SiteScopeStatusChange**, the SiteScope Filters window opens. For details, see “Set Additional Filters for SiteScope” on page 155.

- 4 Click one of the action buttons to print, e-mail, or open a report in Excel or PDF format. For details, see “Format Options” in *Reports*.
- 5 Click **Generate** to create the report.

Note: If the number of events that occur during the specified time frame is larger than the maximum number of events that can be displayed in the report, a message is displayed. To reduce the number of events, select a more specific time range. For example, to see events for the past week, select the individual days of the week.

Customizing Event Logs

You can change the default setting of the maximum number of rows that can be displayed in the page. You can also change the maximum number of events that can be listed in the event log.

To change the maximum number of rows displayed in a page:

When there are too many events to display in one page of a table, a paging bar is automatically displayed.

- 1 Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Application**, select **End User/System Availability**, and locate the **Max Table Rows** in the **Event Reports** table.
- 2 Modify the value to the required number of rows per page.

To change the maximum number of rows displayed in the Event Log:

The maximum number of rows that can be displayed in the Event Log is 1000, by default.

- 1 Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Application**, select **End User/System Availability**, and locate the **Max Fetched Rows** in the **Event Reports** table.
- 2 Modify the value to the required number of rows per Event Log.

Set Additional Filters for SiteScope

If you select a SiteScope data source in the active filter, an additional filter is automatically provided to filter the data by SiteScope profile, group, and monitor type.

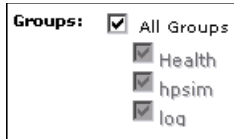
Event Log	
<u>Active Filters:</u>	Event Source: SiteScopeAlert, Severity: All, Target: * (Clear All)
<u>SiteScope Filter:</u>	Monitor Type: All Monitor Types Profile: All Profiles (Clear All)
To generate a report, click the Generate button.	

To work with additional filters for SiteScope data sources:

- 1 Click **SiteScope Filters**, to open the **SiteScope Filter** page.
- 2 Select the type of monitor in the **Monitor Type** list. The default is **All Monitor Types**.
- 3 Select the SiteScope profile in the **Profile** list. The default is **All Profiles**. To view events of interest regarding the profile or group permissions, select one of the profiles in the **Profile** list. The list of groups allowed for the selected profile is displayed. For details on profile or group permissions, see “Permissions Overview” in *Platform Administration*.

Note: If you select **All Profiles**, your profile or group permissions are not applied to the displayed events.

- 4 If available, select the required group in the group tree. Select **All Groups** if you want to select all the groups in the tree. When a tree CI changes its status (from selected to unselected or from unselected to selected) the status of the whole sub-tree changes.



Viewing Common Event Data in the Event Log Page

The event data common to all event data sources is displayed in this table. The data is sorted by time in descending order.

To sort the report by a column, click the column title (an arrow appears in the column title to indicate whether the sort is descending or ascending).







Click a value in a specific row to add this selection to the active filter. The addition is reflected in the display.

Active Filters: Event Source: All, Severity: All, Target: etoile [\(Clear All\)](#)

Severity	Event Source	Time ▾	Hierarchy	Target Name
	SiteScopeAlert	11/4/04 7:54 AM	kuku:CPU alert	etoile
	SiteScopeAlert	11/4/04 7:54 AM	kuku:CPU alert	etoile
	SiteScopeAlert	11/4/04 7:53 AM	kuku:CPU alert	etoile
	SiteScopeAlert	11/4/04 7:53 AM	kuku:CPU alert	etoile

Each row in the table contains the data associated with one event:

- **Severity.** The icon and its tooltip display the severity of the event.

Icon	Severity
	Unknown
	OK
	Warning
	Minor
	Major
	Critical

- **Event Source.** The application or software from which the event is collected. Event sources can be: HP OVO, Remedy ARs, SitescopeAlert, SitescopeAlertStatusChange, Tivoli TEC, BMC Patrol, CA Unicenter, HP SIM, Compaq Insight Manager, Whatsup, or Compaq Insight Manager, depending on the external systems that sent the events to HP Business Availability Center.
- **Time.** The time when the event occurred. By default, the data sorted in this column is in descending order.
- **Hierarchy.** The hierarchy description of the event source. It can include the path to where the event occurred in the area, sub area, or instance and/or the event depending on the application or software from which the event is collected. Depending on the data source, the hierarchy can have two to four branches. If the hierarchy is very long, this field displays the shortened string and the tooltip displays the complete hierarchy.
- **Target Name.** The name or the IP address of the host or device that caused the event.
- **Status.** The status or type of the event. If the hierarchy is very long, the value is shortened and the tooltip displays the full hierarchy.

- **Description.** The event description. If the description is very long, the value is shortened and the tooltip displays the full hierarchy.



To view additional data for this event, click the **Event Details** button to open the Event Details page. For details, see “Working with Event Details” on page 158.



To view details about the event history data, click the **History** button to open the Event History page. For details, see “Working with Event History” on page 160.

Note: By default, some data sources include a history view and others do not (the History button is unavailable or does not display). You can enable the history view by changing the setting in the Infrastructure Settings Manager. To modify the setting, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **End User/System Availability Management**, and locate the **Event Log Report Data Sources History** entry in the **End User/System Availability Management - Data** table. Set the property value by adding the data source names for which you want to enable the History button (separate data source names with commas)—in the Value box. The change takes place after restart. For details, see “Infrastructure Settings” in *Platform Administration*.

Working with Event Details

To display all the data (common and specific) related to an event, you display the event details.

Click the **Event Details** button in the Event Log page to open the Event Details report in a new window.

The Event Details report displays detailed information about the specified event as well as the fields and the field values from the event data. The type of information provided depends on the data source.

The Event Details report can display any of the following fields:

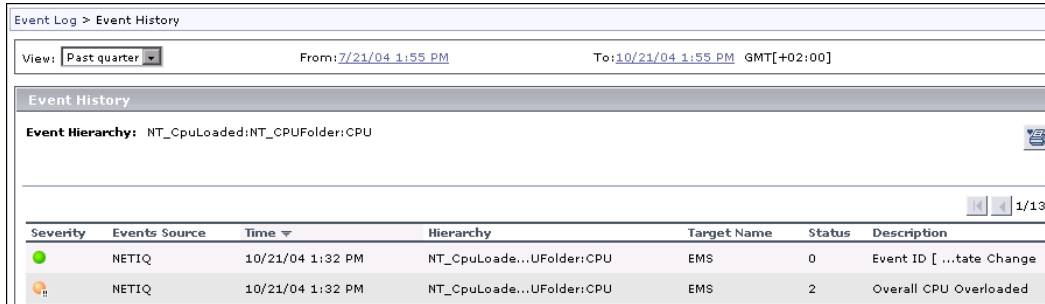
- **Time.** The time of the event.
- **Severity.** The severity of the event.
- **Original Severity.** The original severity of the event.
- **Status.** The event status or type. If the hierarchy is very long, this field displays a shortened string and the tooltip displays the complete status.
- **Event Source.** The application or software from which this event is collected.
- **Logical Group.** The additional logical level of event hierarchy.
- **Hierarchy.** The hierarchy of the event source. It can include the path to where the event occurred in the area, sub area, or instance and/or the event depending on the application or software from which the event is collected.



Depending on the data source, the hierarchy can have two to four branches. If the hierarchy is very long, this field displays the shortened string and the tooltip displays the complete hierarchy.

- **Target Name and IP.** The name or IP address of the host or device that caused this event.
- **Collector host.** The name of the machine that collected the data.
- **Description.** A description of the event.
- **Acknowledged By.** The operator who acknowledged this event.
- **Value.** Any numeric values that are sent with the event.
- **Additional information field (1... 5).** Additional rows (up to 5) that contain additional information for the current event.

Working with Event History

Click the **Event History** button in the Event Log page to open the Event History report in a new window.



Severity	Events Source	Time	Hierarchy	Target Name	Status	Description
	NETIQ	10/21/04 1:32 PM	NT_CpuLoad...UFolder:CPU	EMS	0	Event ID [...tate Change
	NETIQ	10/21/04 1:32 PM	NT_CpuLoad...UFolder:CPU	EMS	2	Overall CPU Overloaded

The Event History report displays detailed information about the specified event for different time periods.

The data displayed provides a historical view of the event:

- ▶ **Event Source.** The application or software from which the event was collected. Event sources can be: HP OVO, Remedy ARs, SitescopeAlert, SitescopeAlertStatusChange, Tivoli TEC, BMC Patrol, CA Unicenter, HP SIM, Compaq Insight Manager, Whatsup, or Compaq Insight Manager, depending on the external systems that sent the events to HP Business Availability Center.
- ▶ **Time.** The time when the event occurred. By default, the data sorted in this column is in descending order.
- ▶ **Hierarchy.** The hierarchy description of the event source. It can include the path to where the event occurred in the area, sub area, or instance and/or the event depending on the application or software from which the event was collected. Depending on the data source, the hierarchy can have two to four branches. If the hierarchy is very long, this field displays the shortened string and the tooltip displays the complete hierarchy.
- ▶ **Target Name.** The name or the IP address of the host or device that caused the event.
- ▶ **Status.** The status or type of the event. If the hierarchy is very long, the value is shortened and the tooltip displays the full hierarchy.

- **Description.** The event description. If the description is very long, the value is shortened and the tooltip displays the full hierarchy.

To view different periods of the event history select the required time frame in the **View** list. This selection has no effect on the time frame selected in the **View** list in the Event Log page.

Note: By default, some data sources include a history view and others do not (the History button is unavailable or does not display). You can enable the history view by changing the setting in the Infrastructure Settings Manager. To modify the setting, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **End User/System Availability Management**, and locate the **Event Log Report Data Sources History** entry in the **End User/System Availability Management - Data** table. Set the property value by adding the data source names for which you want to enable the History button (separate data source names with commas)—in the Value box. The change takes place after restart. For details, see “Infrastructure Settings” in *Platform Administration*.

Part III

General and Administration

7

SiteScope Monitor Tree

This chapter includes the main concepts and reference information for the SiteScope monitor tree.

This chapter includes:

Concepts

- ▶ SiteScope Monitor Tree Overview on page 166
- ▶ SiteScope Monitors and HP Business Availability Center Configuration Items on page 166
- ▶ Copying and Moving SiteScope Objects on page 168
- ▶ Navigating and Performing Actions in the Contents Tab and the Monitor Tree on page 170

Reference

- ▶ Monitor Tree User Interface on page 170

SiteScope Monitor Tree Overview

SiteScope's interface objects are organized into a hierarchy represented by a monitor tree. You use the monitor tree to navigate through containers and elements in SiteScope and drill down to monitor and other configuration settings. For user interface details on the different hierarchy elements, see "Monitor Tree" on page 171.

You can customize your view of the monitor tree to list only those SiteScope elements with which you are working. You can also assign categories to your groups, monitors, reports, and alerts to further refine your selection. For details on this topic, see "Views and Categories Overview" on page 195.

SiteScope enables you to change monitor configurations across multiple monitors, groups, or multiple SiteScopes using Global Replace. For details on the Global Replace user interface, see "Global Search and Replace Wizard" on page 351.

SiteScope Monitors and HP Business Availability Center Configuration Items

If your SiteScope is integrated with HP Business Availability Center, when you create a monitor, that monitor object creates a corresponding (CI) in the Universal configuration management history database. For details on understanding configuration items, see "Configuration Items (CI)" in *Model Management*.

The monitors that populate the CMDB are represented in the CMDB as monitor CIs. Monitor CIs receive data from the SiteScope monitor and use the data to calculate status.

You can also create relationship between a monitor and any existing, logical CI in the CMDB. This relationship enables the monitor to pass KPI status to the CI to which it is attached.

You can create this relationship:

- ▶ using the **Modeling** tab in Universal CMDB Administration. For details, see “Attaching Existing CIs” in *Model Management*.
- ▶ using the **Link Monitor to CI** area while creating a monitor. The **Select CIs** button in this area opens the Select CIs dialog box in which you can select a view in the left pane that includes the CI you want to attach to the monitor. For details on selecting and working with views, see “View Explorer” in *Reference Information*.
- ▶ using the **Monitor Deployment Wizard** to deploy SiteScope monitors onto existing CIs. If a SiteScope monitor already has an attached CI, you can use the Monitor Deployment Wizard to modify the monitors that are reporting status to the attached CI. For details, see “Monitor Deployment Wizard Concepts and Tasks” on page 81.

Note: The Monitor Deployment Wizard is available only to those users accessing SiteScope using System Availability Management Administration in HP Business Availability Center.

You can view and edit the relationship you created in IT Universe Manager in Universal CMDB Administration.

Note: The monitor CI appears in the views as a child object to the original CI only if, in the original CI’s properties, the **Include Related Elements** option is selected. For details, see “Include Related CIs” in *Model Management*.

Copying and Moving SiteScope Objects

You can copy SiteScope objects to different locations in the monitor tree. In addition, you can move a monitor or monitor group and its contents to a template or to a different monitor group.

To enable you to differentiate between objects, object names must be unique within the parent container. For instance, when you copy or move SiteScope objects, you cannot create two monitors within the same group with exactly the same name. If you make a copy of a SiteScope object and it has the same name as an existing object in the container, SiteScope automatically adds a suffix (number) to the end of the object's name. For example, if you create a copy of monitor Mail Flow and paste it in the same monitor group, SiteScope automatically renames it Mail Flow(1).

You can copy or move the following SiteScope objects:

Context Menu Option	Action	Description
Group	Cut/Paste Copy/Paste	<p>Enables you to copy or move a monitor group, including its monitors, alerts, and reports. You can make a copy in the same monitor group, or copy or move it to a different monitor group. You can also copy it to a different template.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ You cannot move or copy a monitor group to its subgroup. ▶ If you move a group that is targeted by an alert or report without also moving the alert or report, the group is removed from the alert or report target. ▶ Baseline thresholds are not copied or moved with a monitor whose thresholds were set using the baseline.

Context Menu Option	Action	Description
Monitor	Cut/Paste Copy/Paste	Enables you to copy or move a monitor, including its alerts and reports. You can make a copy in the same monitor group, or copy or move it to a different monitor group. You can also copy it to a different template. Note: <ul style="list-style-type: none"> ▶ If you move a monitor that is targeted by an alert or report without also moving the alert or report, the monitor is removed from the alert or report target. ▶ Baseline thresholds are not copied or moved with a monitor whose thresholds were set using the baseline.
Template Container	Paste	Enables you to paste a template into the template container.
Template	Copy/Paste	Enables you to copy a template group or template monitor to a template container or template.
Alert	Copy/Paste	Enables you to copy the alert to another location in the monitor tree.
Report	Copy/Paste	Enables you to copy the report to another location in the monitor tree.

For details on copying or moving SiteScope objects, expand the relevant context menu option in “Context Menu Options” on page 176.

Navigating and Performing Actions in the Contents Tab and the Monitor Tree

There are several ways to navigate the monitor tree, perform actions, and edit object properties.

The monitor tree itself enables you to highlight any object within the tree and right-click the object to access a menu of options for that object. For example, if you right-click the SiteScope node, you select from a menu listing only those actions that can be performed on the SiteScope node.

The Contents tab enables you to view all the objects within any of the containers or profiles in the monitor tree, including the SiteScope node itself. When an object that includes child objects is highlighted, the Contents tab lists all of the child objects according to their type.

Additionally, the Contents tab enables you to select actions for each object type. The actions applicable to the highlighted object appear as optional buttons at the top of the Contents page. The actions applicable to the child objects of the highlighted object appear as optional buttons in the area listing the objects of that type.

Monitor Tree User Interface

This section describes:

- Monitor Tree on page 171
- Context Menu Options on page 176
- Contents Tab on page 191

 **Monitor Tree**

Description	The monitor tree of SiteScope represents the organization of systems and services in your network environment. The tree includes containers and objects within your infrastructure.
Important Information	The root node of the tree is the SiteScope container. Only one SiteScope node exists in the monitor tree. You add all other elements to the tree under the SiteScope node.







Monitor Tree View Options








The following elements are included (unlabeled GUI elements are shown in angle brackets>):





Menu Item	Description
Monitor	<p>To filter the objects appearing in the monitor tree by monitor name, type a monitor name and press ENTER.</p> <ul style="list-style-type: none"> ▶ The monitor name is the string entered in the Name box in the Main Settings area during monitor configuration. ▶ Clear the box and press ENTER to clear the filter. ▶ Type a regular expression to widen the filter. <p>The monitor tree displays only those monitors, within their groups, matching the string entered and only those groups containing these monitors.</p> <p>Example: To display only those monitors beginning with the string CPU, type CPU* and press ENTER.</p>
Target	<p>To filter the objects appearing in the monitor tree by the target server, type a server name and press ENTER.</p> <ul style="list-style-type: none"> ▶ The target is the string entered in the Server box in the Main Settings area during monitor configuration. ▶ Clear the box and press ENTER to clear the filter. ▶ Type a regular expression to widen the filter. <p>The monitor tree displays only those monitors, within their groups, whose target server matches the string entered and only those groups containing these monitors.</p>
View window	<p>Select an existing view from the drop-down list. You create views in the Views tab to modify the objects that appear in the monitor tree.</p> <p>For details, see “Defining and Managing View Settings” on page 196.</p>

Monitor Tree Objects

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Represents an individual SiteScope server. Parent: Enterprise node or container. Add to tree by: Importing or adding an empty SiteScope profile.
	Represents a template container. A template container is used to organize configuration deployment templates. Parent: SiteScope. Add to tree by: Creating, or importing with a SiteScope that has template containers defined.
	Represents a solution template container. Parent: SiteScope.
	Represents a template configuration for deploying SiteScope objects. Parent: Template container. Add to tree by: Creating.
	Represents a variable used as placeholder to prompt for input when deploying a template. Parent: Template. Add to tree by: Creating.
	Represents a SiteScope monitor group or subgroup. Parent: SiteScope or SiteScope group. Add to tree by: Creating, or importing with a SiteScope that has groups defined.

GUI Element	Description
	<p>Represents a SiteScope monitor.</p> <p>Parent: SiteScope group or subgroup, template, or solution template.</p> <p>Add to tree by: Creating, or importing with a SiteScope that has monitors configured.</p>
	<p>Preferences representing the collection of SiteScope configuration settings.</p> <p>Parent: SiteScope.</p> <p>Add to tree by: Creating, or importing with a SiteScope that has preferences defined.</p>
	<p>Represents a preference.</p> <p>Parent: Preferences container or preference.</p>
	<p>Represents a remote server preference.</p> <p>Parent: Preferences container, remote server preference, or template.</p> <p>Add to tree by: Creating.</p>
	<p>Represents the collection of available health monitors that are deployed to check proper functioning of SiteScope monitors.</p> <p>Parent: SiteScope.</p> <p>Add to tree by: Automatically added with SiteScope object.</p>
	<p>Represents the collection of alert schemes configured for the SiteScope.</p> <p>Parent: SiteScope.</p> <p>Add to tree by: Automatically added with SiteScope object.</p>
	<p>Represents an alert.</p> <p>Parent: SiteScope, SiteScope group container, a template, or a monitor.</p> <p>Add to tree by: Creating.</p>

GUI Element	Description
	<p>Represents a report.</p> <p>Parent: SiteScope, SiteScope group container, or a monitor.</p> <p>Add to tree by: Creating.</p>
	<p>Represents a tools container. A container used to organize the various tools for configuring the SiteScope.</p> <p>Parent: SiteScope.</p>
	<p>Click the Refresh button to refresh the data in the tree.</p>
	<p>Click the Hide Tree Panel button to hide the monitor tree and expand the right pane.</p>

Context Menu Options

Following are descriptions of the various context menu options that are available for each object in the monitor tree.

SiteScope Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Baselining	<p>Enables you to create a baseline for monitoring variations in response times and performance in the infrastructure for all monitors under SiteScope.</p> <ul style="list-style-type: none"> ▶ Calculate. Enables you to select monitors and specify the relevant time and schedule to be used for calculating the baseline. It also enables you to select and fine-tune the baseline adherence level and define boundaries. ▶ Review & Activate. Displays a summary of calculated monitors and baseline data. It also enables you to save the current monitor configuration, view and retry failed operations, view baseline measurement graphs, and apply the baseline configuration. ▶ Status Report. Displays information about the baseline status for all monitors under SiteScope. <p>For details, see “Setting Status Thresholds Using a Baseline” on page 478.</p>
Expand All	Opens all the subtrees under SiteScope.
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see “Global Search and Replace Wizard” on page 351.

Menu Item (A-Z)	Description
Monitor Deployment Wizard	This menu item is available only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center. Opens the Monitor Deployment Wizard. For details, see “Monitor Deployment Wizard Concepts and Tasks” on page 81.
New Alert	Opens the New Alert window which enables you to define a new alert for SiteScope.
New Group	Opens the New Group window which enables you to define a new SiteScope group.
New Report	Opens the New Report window which enables you to define a new SiteScope report.
New Template Container	Opens the New Template Container window which enables you to define a new template container.
Paste	Pastes the selected SiteScope object (that was previously copied or cut) to the SiteScope node.
Paste from other SiteScope	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Pastes the selected SiteScope object (that was previously copied or cut) from another SiteScope to the SiteScope node.

Template Container Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Delete	Deletes the template container.
Edit	Opens an editing window for the template container, which enables you to edit its settings.
Expand All	Expands the templates container to display all the template objects within the container.

Menu Item (A-Z)	Description
Export	Opens the Export Template window which enables you to export a template file.
Generate XML	Opens the Generate Auto Deployment XML window which enables you to create an XML file to use for automatically deploying the templates in the container.
Import	Opens the Import Template window which enables you to import a template file.
New Template	Opens the New Container window which enables you to define a new template.
New Template Container	Opens the New Template Container window which enables you to define a new template container.
Paste	Pastes a template into the template container.

Solution Templates Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Expand All	Expands the solution templates container to display all the solution templates within the container.

Template Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Copy	Copies a template group, monitor, or alert. You can paste the template group, monitor, or alert to the SiteScope tree.
Delete	Deletes the template.
Edit	Opens an editing window for the template, which enables you to edit its settings.
Expand All	Opens all the subtrees under the template.
New Group	Opens the New Group window, which enables you to define a new template group.
New Remote NT	Opens the New Template window, which enables you to define a new remote NT template.
New Remote Unix	Opens the New Template window, which enables you to define a new remote UNIX template.
New Variable	Opens the New Template Variable window, which enables you to define a new template variable.
Paste	Pastes a template group, monitor, or alert to a template.
Publish Changes	Opens the Publish Template Changes wizard, which enables you to check deployed groups for template compliancy and to update SiteScope objects deployed by templates whenever the template is updated.

Template Variable Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Delete	Deletes the template variable.
Edit	Opens an editing window for the template variable, which enables you to edit its settings.

Template Remote Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Copy	Copies the template remote to a template. Note: You can add only one template remote server to a template. This does not apply to templates created in older versions of SiteScope.
Delete	Deletes the template remote.
Edit	Opens an editing window for the template remote, which enables you to edit its settings.

Template Group Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Copy	Copies the template group and its contents (monitors, alerts, and subgroups) to a template.
Delete	Deletes the template group.
Edit	Opens an editing window for the template group, which enables you to edit its settings.

Menu Item (A-Z)	Description
Expand All	Opens all the subtrees under the template group.
New Alert	Opens the New Template Alert window which enables you to define a new alert for the template group.
New Group	Opens the New Template Group window which enables you to define a new template subgroup.
New Monitor	Opens the New Monitor window which enables you to define a new SiteScope monitor for the template group.
Paste	Pastes the selected template group and its contents (monitors, alerts, and subgroups) to a template.

Template Monitor Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Copy	Copies the template monitor and its contents (alerts) to a template group.
Delete	Deletes the template monitor.
Edit	Opens an editing window for the template monitor, which enables you to edit its settings.
New Alert	Opens the New Template Alert window which enables you to define a new alert for the template monitor.
Paste	Pastes the selected template monitor and its contents (alerts) to a template group.

Template Alert Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Copy	Copies the template alert to a template group.
Delete	Deletes the template alert.
Edit	Opens an editing window for the template alert, which enables you to edit its settings.

Group Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Baselining	<p>Enables you to create a baseline for monitoring variations in response times and performance in the infrastructure for all monitors in the group.</p> <ul style="list-style-type: none"> ▶ Calculate. Enables you to select monitors from the group and specify the relevant time and schedule to be used for calculating the baseline. It also enables you to select and fine-tune the baseline adherence level and define boundaries. ▶ Review & Activate. Displays a summary of calculated monitors and baseline data for the group. It also enables you to save the current monitor configuration, view and retry failed operations, view baseline measurement graphs, and apply the baseline configuration. ▶ Status Report. Displays information about the baseline status for all monitors in the group. <p>For details, see “Setting Status Thresholds Using a Baseline” on page 478.</p>

Menu Item (A-Z)	Description
Copy	<p>Copies the group and its contents (monitors, alerts, and reports) to a monitor group or template.</p> <p>Note: When copying a group that contains monitors with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitors are no longer in baseline mode.</p>
Copy to other SiteScope	<p>This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Copies the group and its contents (monitors, alerts, and reports) from another SiteScope to a monitor group or template in the SiteScope node.</p>
Cut	<p>Moves the group and its contents (monitors, alerts, and reports) or a monitor and its contents (alerts and reports) to a monitor group.</p> <p>Note: When moving a group that contains monitors with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitors are no longer in baseline mode.</p>
Delete	<p>Deletes the group.</p> <p>Note: You cannot delete a group if it has dependent alerts or reports at the container level. To delete a group with dependencies, you must remove the group from Alert Targets and Monitors and Groups to report on in the Main Settings for each dependency, and then delete the group. You can delete groups that have dependencies at the child level.</p>
Edit	<p>Opens an editing window for the group, which enables you to edit its settings.</p>
Expand All	<p>Opens all the subtrees under the group.</p>

Menu Item (A-Z)	Description
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see “Global Search and Replace Wizard” on page 351.
Monitor Deployment Wizard	This menu item is available only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center. Opens the Monitor Deployment Wizard. For details, see “Monitor Deployment Wizard Concepts and Tasks” on page 81.
New Alert	Opens the New Alert window which enables you to define a new alert for the group.
New Group	Opens the New Group window which enables you to define a new SiteScope group.
New Monitor	Opens the New Monitor window which enables you to define a new SiteScope monitor.
New Report	Opens the New Report window which enables you to define a new SiteScope report.
Paste	Pastes the selected group and its contents (monitors, alerts, and reports) or a monitor and its contents (alerts and reports) to the specified monitor group.
Paste from other SiteScope	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Pastes the selected group and its contents (monitors, alerts, and reports) or a monitor and its contents (alerts and reports) from another SiteScope to the specified monitor group.
Run Monitors	Runs any monitors configured in the group, and opens an information window with the results.

Monitor Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Baselining	<p>Enables you to create a baseline for monitoring variations in response times and performance in the infrastructure for the specific monitor.</p> <ul style="list-style-type: none"> ▶ Calculate. Enables you to select the monitor and specify the relevant time and schedule to be used for calculating the baseline. It also enables you to select and fine-tune the baseline adherence level and define boundaries. ▶ Review & Activate. Displays a summary of the calculated monitor's baseline data. It also enables you to save the current monitor configuration, view and retry failed operations, view baseline measurement graphs, and apply the baseline configuration. ▶ Status Report. Displays information about the monitor's baseline status. <p>For details, see “Setting Status Thresholds Using a Baseline” on page 478.</p>
Copy	<p>Copies the monitor and its contents (alerts and reports) to a monitor group or template.</p> <p>Note: When copying a monitor with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitor is no longer in baseline mode.</p>
Copy to other SiteScope	<p>This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Copies the monitor and its contents (alerts and reports) from another SiteScope to a monitor group or template.</p>

Menu Item (A-Z)	Description
Cut	<p>Moves the monitor and its contents (alerts and reports) to a monitor group.</p> <p>Note: When moving a monitor with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitor is no longer in baseline mode.</p>
Delete	<p>Deletes the monitor.</p> <p>Note: You cannot delete a monitor if it has dependent alerts or reports at the container level. To delete a monitor with dependencies, you must remove the monitor from Alert Targets and Monitors and Groups to report on in the Main Settings for each dependency, and then delete the monitor. You can delete monitors that have dependencies at the child level.</p>
Edit	<p>Opens an editing window for the monitor, which labels you to edit its settings.</p>
Global Replace	<p>Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see “Global Search and Replace Wizard” on page 351.</p>
New Alert	<p>Opens the New Alert window which enables you to define a new alert for the monitor.</p>
New Report	<p>Opens the New Report window which enables you to define a new SiteScope report.</p>
Paste	<p>Pastes the selected monitor context object to the specified monitor.</p>
Paste from other SiteScope	<p>This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Pastes the selected monitor context object from another SiteScope to the specified monitor.</p>
Run	<p>Runs the monitor and opens an information window with the results.</p>

Preferences Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets):

Menu Item (A-Z)	Description
Expand All	Opens all the subtrees under the preferences.
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see “Global Search and Replace Wizard” on page 351.

Preference Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets):

Menu Item (A-Z)	Description
<context-sensitive options>	The context menu options for a preference object are specific to the individual preference.

Server Preference Context Menu Options

The following options are available for the Preferences container only. They are not available for individual preferences.

Menu Item (A-Z)	Description
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see “Global Search and Replace Wizard” on page 351.
New Microsoft Windows/UNIX Server	Opens the New Server window which enables you to define a new Microsoft Windows or UNIX server.

SiteScope Health Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Disable Logging	Disables logging on SiteScope Health. For details, see “SiteScope Server Health” on page 365.
Enable Logging	Enables logging on SiteScope Health. For details, see “SiteScope Server Health” on page 365.
Expand All	Opens all the subtrees under SiteScope Health.
New Alert	Opens the New Alert window which enables you to define a new alert for Health.
New Group	Opens the New Group window which enables you to define a new SiteScope group.
New Monitor	Opens the New Monitor window which enables you to define a new SiteScope monitor.
New Report	Opens the New Report window which enables you to define a new SiteScope report.
Paste	Pastes monitors and monitor groups into the Health container.
Run Monitors	Runs the health monitors and opens an information window with the results.

Alert Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Copy	Copies the alert to the selected location in the monitor tree.
Copy to other SiteScope	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Copies the alert from another SiteScope to the selected location in the monitor tree.
Delete	Deletes the alert.
Disable	Disables the alert.
Edit	Opens an editing window for the alert, which enables you to edit its settings.
Enable	Enables the alert.
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see “Global Search and Replace Wizard” on page 351.
Test	Opens the Test Alert page which enables you to test the alert.

Reports Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Copy	Copies the report to the selected location in the monitor tree.
Delete	Deletes the report.
Edit	Opens an editing window for the report, which enables you to edit its settings.
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see “Global Search and Replace Wizard” on page 351.

Tools Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
Expand All	Opens all the subtrees under Tools.

 **Contents Tab**

Description	<p>Displays view panels and tables that enable you to view the current status of monitors, view the detailed content of object containers, and manage configuration settings for monitors, alerts, and reports.</p> <p>To access: Select an object and click the Contents tab in the right pane.</p>
Important Information	<p>The Contents tab enables you to view all the objects within any of the containers or profiles in the monitor tree, including the SiteScope node itself. When an object that includes child objects is highlighted, the Contents tab lists all of the child objects according to their type.</p> <p>Additionally, the Contents tab enables you to select actions for each object type. The actions applicable to the highlighted object appear as optional buttons at the top of the Contents page. The actions applicable to the child objects of the highlighted object appear as optional buttons in the area listing the objects of that type.</p>

The Contents Tab includes the following elements:

GUI Element	Description
Up	Click to go up one level in the monitor tree. This option is not available for SiteScope (the highest level in the tree).
<action buttons>	The Contents tab for each of the objects contains action buttons corresponding to the context menu options in the monitor tree for that object. For details, see the relevant context menu options under “Monitor Tree” on page 171.

The Contents Tab for each object contains areas specific to that object as follows:

Object	Child Objects
SiteScope	Template Containers Groups Preferences Health Alerts Reports Tools
Template Container	Template Containers Templates
Template	Template Groups Template Alerts Template Monitors Template Variables Template UNIX Remote Template NT Remote
Group	Groups Alerts Reports Monitors
Monitor	Alerts Reports

Object	Child Objects
Preferences	General Settings UNIX Server Container Log Preferences E-mail Recipient Container Pager Recipient Container SNMP Trap Container Absolute Schedule Container Infrastructure Settings Preferences Windows Server Container Range Schedule Container Users
Server Preferences	Servers
Health	Groups Alerts Reports Monitors
Tools	The selection of tools available for monitoring.

8

Views and Categories

This chapter includes the main concepts, tasks, and reference information for Views and Categories.

This chapter includes:

Concepts

- Views and Categories Overview on page 195
- Defining and Managing View Settings on page 196
- Working with Categories on page 197

Tasks

- Create and Define a New Category on page 198

Reference

- Views and Categories User Interface on page 200

Views and Categories Overview

When administrating monitor deployment, an extensive monitor tree displaying every object added to it could prove difficult to manage. SiteScope enables you to select which objects in the tree you want to view, based on various filter criteria. You can define multiple views with different filter conditions that can be applied for varying configuration tasks.

For example, you can create a view to display only SiteScope monitors that are monitoring CPU utilization and Disk Space. The result of this filter displays a tree with all CPU and Disk Space monitor types directly under the enterprise node.

You can also assign categories to any object in the monitor tree and use those categories to filter the view. For example, you define a category for all monitors running on a specific operating system.

For details on views, see the next section.

For details on categories, see “Working with Categories” on page 197.

Defining and Managing View Settings

You define and manage view settings by accessing the Views tab at the top of the SiteScope interface.

You can define views:

- ▶ **based on object type only.** For example, you can define a view that includes all CPU monitors, regardless of their properties. In this view, the monitor tree lists all the CPU monitors defined in the SiteScope.
- ▶ **based on object type and the properties configured for the selected object types.** For example, you can define a view that includes all SiteScope monitors with the same host defined, giving you a view of only those monitors monitoring the selected host.
- ▶ **to appear in a flat list.** A flat list lists all objects meeting the view’s selection criteria as child objects to the SiteScope node, regardless of its parent object.
- ▶ **to appear as a hierarchy.** The hierarchy option lists all objects with their respective parent objects even if the parent object does not meet the view’s selection criteria.
- ▶ **to include all child objects of a selected object.** This is done by making your selections recursively.
- ▶ **to represent object properties.** This is done by using regular expressions to represent object properties if basing your selections on an object’s properties.

If you have any views defined, they appear in the drop-down list above the monitor tree in the Monitors tab. You select the view from the list and the monitor tree displays only those objects defined in your view selection.

Working with Categories

You create custom categories for use in filtering the display of the monitor tree for your monitor deployment. You define the categories and their values, and assign these to the different elements in your enterprise.

For example, you define a category called **Priority** with the possible values of **Critical**, **High**, **Medium**, and **Low**. You assign these category values to different elements in the infrastructure. Monitors of Web servers and databases that support 24x7 customer access could be assigned a category value of **Priority: Critical**. While adding a new view setting, you select types in the **Filter by Types** area, and click **Apply Selection**. In the **Filter by Property Values** area, expand the **Category Settings** area, select the **Assigned categories** check box, and select **Priority:Critical** as the value of the object. This filter displays only those elements to which you assigned this category and value.

Create and Define a New Category

This task describes the steps involved in defining a new category and assigning it to one or more elements in the monitor tree.

This task includes the following steps:

- “Create a Category” on page 198
- “Assign Categories to Monitor Tree Elements” on page 198
- “Define a Category for a View Setting” on page 198

1 Create a Category

You use the Categories area of SiteScope to add categories. For details on the user interface, see “Categories Page” on page 203.

2 Assign Categories to Monitor Tree Elements

Before you can use a category as part of a view filter, you must assign the category to one or more elements in the monitor tree. You can assign categories to any item in the tree, including any container, monitor, group, alert, profile, or preference.

You assign categories while adding, importing, or editing objects in the monitor tree. **Category Settings** are included as properties for every type of object in the monitor tree. For details on monitor tree objects in the user interface, see “Monitor Tree” on page 171.

3 Define a Category for a View Setting

Once you have assigned the category to one or more items in the monitor tree, you can use the category as an object for a view filter. For details on filtering a view in the user interface, see “New View/Edit View Page” on page 201.

Example

Create a category indicating the type of operating system on which the monitors are running. The category Operating Systems would have values such as Windows 2000, Windows XP, Solaris, Linux, and so forth.

New Category											
Main Settings											
Name *	Operating Systems										
Value*	<table border="1"> <thead> <tr> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Windows 2000</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Windows XP</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Solaris</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Linux</td> <td></td> </tr> </tbody> </table>	Name	Description	<input type="checkbox"/> Windows 2000		<input type="checkbox"/> Windows XP		<input type="checkbox"/> Solaris		<input type="checkbox"/> Linux	
Name	Description										
<input type="checkbox"/> Windows 2000											
<input type="checkbox"/> Windows XP											
<input type="checkbox"/> Solaris											
<input type="checkbox"/> Linux											

Assign the category to a monitor tree element such as a group by editing it and selecting Operating Systems as an Assigned category under **Category Settings**.

SiteScope Group "Windows m...for doors"	
Main Settings	
Group Name *	Windows monitors for doors
Advanced Settings	
Category Settings	
Assigned categories	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Operating Systems <ul style="list-style-type: none"> <input type="checkbox"/> Linux <input type="checkbox"/> Solaris <input checked="" type="checkbox"/> Windows 2000 <input checked="" type="checkbox"/> Windows XP

Using this new category, you could define a view setting for the monitor tree to display only those monitors running on Windows machines.

Views and Categories User Interface


This section describes:

- Views Page on page 200
- New View/Edit View Page on page 201
- Categories Page on page 203
- New Category/Edit Category Page on page 204

Views Page

Description	Enables you to add and edit views. To access: Click the Views tab in SiteScope.
Important Information	The Views page lists all the views that have been defined for the monitor tree. Two default views, Alerts and Reports, are automatically defined on the page.
Useful Links	“Views and Categories Overview” on page 195 “Defining and Managing View Settings” on page 196

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element (A-Z)	Description
	Click to open the Edit View page which enables you to edit the selected view.
Description	A description of the view.

GUI Element (A-Z)	Description
Name	The name of the view. Syntax exceptions: You cannot use any of the following characters in the view name: , / \ + = % "
New View	Click to open the New View page which enables you to define a new view.

New View/Edit View Page

Description	Enables you to add a new view or edit an existing one. To access: Click the Views tab, and click the New View button or the Edit button from the Views page.
Useful Links	“Views and Categories Overview” on page 195 “Defining and Managing View Settings” on page 196

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click to display additional information about the dialog box elements.
Name	Type a view filter name. This name appears in the list of available views above the monitor tree.
Result Type	Select whether you want your view to appear as a flat list or in a hierarchy.

Filter by Types Area

The Filter by Types area of the New View/Edit View page includes the following elements (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<SiteScope objects>	Select the check box to the left of the object by which you want to filter your view. You can select multiple objects. When you apply your selection, the Filter by Property Values area is updated to accord with the objects you select.
Apply Selection	Click to apply the settings you selected.
Recursive Selection	Select to automatically select all child objects of a selected object. Note: If you have selected this option and want to remove a selected object from the selection, you must clear the selection of the object which you do not want to appear in the view and clear Recursive Selection . If you do not clear Recursive Selection , all objects within that parent object appear in the view even if you have cleared that object from the selection.
Show all properties (Advanced)	Select this option to display in the Filter by Property Values area all properties associated with all the object types selected in this Filter by Types list.
Show shared properties	Select this option to display in the Filter by Property Values area only those properties that are shared by all the object types selected in this Filter by Types list.

Advanced Area

The Advanced area of the New View/Edit View page includes the following elements (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Description	You can expand this area and type a description for the category. This description appears only when editing the category. Note: This field is optional.

Filter by Property Values Area


The Filter by Property Values area of the New View/Edit View page includes the following elements (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<SiteScope object properties>	This area includes the properties specific to the SiteScope objects selected in the Filter by Types area. Type or select a value for each property by which you want to filter.

Categories Page

Description	Enables you to add and edit categories. To access: Click the Categories tab in SiteScope.
Included in Tasks	“Create and Define a New Category” on page 198
Useful Links	“Working with Categories” on page 197



The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click Edit to open the Edit Category page which enables you to edit the selected category.
Description	A description of the category.
Name	The name of the category. Syntax exceptions: You cannot use any of the following characters in the view name: , / \ + = % "
New Category	Click to open the New Category page which enables you to define a new category.

New Category/Edit Category Page

Description	Enables you to add a new category or edit an existing one. To access: Click the Categories tab, and click the New Category button or the Edit button from the Categories page.
Included in Tasks	"Create and Define a New Category" on page 198
Useful Links	"Working with Categories" on page 197

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click to display additional information about the dialog box elements.
	Click to delete a selected value.

GUI Element (A-Z)	Description
Advanced Settings - Description	You can expand the Advanced Settings area and type a description for the category. This description appears only when editing the category. Note: This field is optional.
Name	Type a new category name. This name appears as the display name in the Categories page, and when defining or editing category settings for all objects in the monitor tree.
New Value	Click to add a row for entering a new value for the category.
Value Description	Type an optional description for each value. This description appears only when editing the category.
Value Name	Type a name for the value to be included in the category. Each category must include at least one value. Each value appears as a child object of the category name when defining or editing category settings for all objects in the monitor tree.

9

Preferences

This chapter includes the main concepts, tasks, and reference information for SiteScope monitor preferences.

This chapter includes:

Concepts

- Preferences Overview on page 209
- General Preferences on page 211
- Infrastructure Settings Preferences on page 216
- Integration Preferences on page 216
- Failover Preferences on page 219
- Microsoft Windows Remote Preferences on page 219
- UNIX Remote Preferences on page 220
- Log Preferences on page 221
- E-mail Preferences on page 222
- Pager Preferences on page 222
- SNMP Trap Preferences on page 223
- Absolute Schedule Preferences on page 224
- Range Schedule Preferences on page 225
- User Preferences on page 226
- Credential Preferences on page 229

Tasks

- Configure SiteScope for a Non-English Locale on page 231

- ▶ Configure SiteScope-HP Business Availability Center Integration Preferences on page 234
- ▶ Configure SiteScope to Monitor a Remote Windows Server on page 236
- ▶ Configure Credential Preferences on page 243

Reference

- ▶ Monitors Tested for Internationalization on page 244
- ▶ SiteScope Log Database Table Structure on page 246
- ▶ Password Requirement Parameters on page 247
- ▶ Preferences User Interface on page 247

Troubleshooting and Limitations on page 334

Preferences Overview

SiteScope Preferences enable you to configure specific properties and settings related to most of the administrative tasks within SiteScope.

Note: Only an administrator, or a user granted **Edit Preferences** permissions, can create or make changes to SiteScope Preferences and restart SiteScope from Infrastructure Settings Preferences.

The following table lists Preferences available for SiteScope. The sections that follow contain more information about each Preference.

Preference	Description
General Preferences	Use to perform various post-configuration tasks, such as enter standard and optional SiteScope license keys, control display functions, and set security options. For details, see “General Preferences” on page 211.
Infrastructure Settings Preferences	Use to define the values of global settings that determine how SiteScope runs. For details, see “Infrastructure Settings Preferences” on page 216.
Integration Preferences	Use to configure SiteScope as a data collector for Business Availability Center. For details, see “Integration Preferences” on page 216.
Failover Preferences	Use to indicate a primary SiteScope to be mirrored and set how often the configurations should be mirrored to the SiteScope Failover installation. For details, see “Failover Preferences” on page 219.
Microsoft Windows Remote Preferences	Use to set up connection properties, such as credentials and protocols, so that SiteScope can monitor systems and services running on remote Windows servers. For details, see “Microsoft Windows Remote Preferences” on page 219.

Preference	Description
UNIX Remote Preferences	Use to set up connection properties, such as credentials and protocols, so that SiteScope can monitor systems and services running on remote UNIX servers. For details, see “UNIX Remote Preferences” on page 220.
Log Preferences	Use to controls the accumulation and storage of monitor data logs. For details, see “Log Preferences” on page 221.
E-mail Preferences	Use to define e-mail server settings and profiles for SiteScope e-mails alert and status reports. For details, see “E-mail Preferences” on page 222.
Pager Preferences	Use to configure settings and additional pager profiles that SiteScope uses for sending Pager alerts. For details, see “Pager Preferences” on page 222.
SNMP Trap Preferences	Use to define settings that are used by SiteScope SNMP Trap alerts when sending data to management consoles. For details, see “SNMP Trap Preferences” on page 223.
Absolute Schedule Preferences	Use for customizing the operation of SiteScope monitors and alerts to run only at specific times. For details, see “Absolute Schedule Preferences” on page 224.
Range Schedule Preferences	Use for customizing the operation of SiteScope monitors and alerts to run only during specific time periods. For details, see “Range Schedule Preferences” on page 225.
User Preferences	Use to define and manage user login profiles that control how others access SiteScope. For details, see “User Preferences” on page 226.
Credential Preferences	Use to create and manage credentials for SiteScope resources. For details, see “Credential Preferences” on page 229.

General Preferences

This section includes the following main concepts of SiteScope General Preferences:

- “Working in an Internationalization (I18N) Environment” on page 211
- “Using Default Authentication Credentials” on page 212
- “Suspending Monitor Processes” on page 212
- “Working with SiteScope Configuration Files” on page 212
- “Web Script Monitor Files Directory” on page 213
- “Setting the SiteScope Restart Schedule” on page 213

Working in an Internationalization (I18N) Environment

SiteScope supports working in an internationalization environment. For more information, see the following topics:

- “General Limitations for Using SiteScope in an I18N Environment” on page 213
- “Multi-Lingual User (MLU) Interface Support” on page 214
- “Database Environment Issues” on page 215
- “Monitors Tested for Internationalization” on page 244

Using Default Authentication Credentials

You use this section to enter default authentication credentials that SiteScope uses to log into certain applications and systems. This user name and password are used if the following conditions are met:

- ▶ No other authentication credentials are entered as part of an individual monitor configuration.
- ▶ The target application or system requires authentication credentials. The URL Monitor, URL Sequence Monitor, and Web Service Monitor can use this function.

Suspending Monitor Processes

In large and complex monitoring environments, it is possible that SiteScope can become heavily loaded with a large number of monitors running and the responsiveness may become slow. This may be due to some monitors being configured to monitor too aggressively or systems that are becoming overloaded. If monitoring actions are slowing the performance of SiteScope, it can be useful to temporarily suspend monitoring actions to make configuration changes. You can temporarily suspend monitors to reduce the time required to complete large configuration operations such as a global search and replace operation. The **Suspend Monitors** option provides this function.

Working with SiteScope Configuration Files

SiteScope uses a binary monitor and system configuration data storage for the SiteScope application. This is different than versions of SiteScope earlier than 8.0.0.0 which stored monitor and system configuration data in text files in the `<SiteScope root directory>\groups` folder.

This option is selected by default when SiteScope is installed. You should leave this option selected if you plan to make changes or additions to the **master.config** file or manually edit other files in the groups folder. If this option is not selected, SiteScope ignores changes made to the text configuration files.

Disabling this option may improve SiteScope performance.

Note: If you disable this option and later want to re-enable it, you must select the box, click **OK** to save the change, and then restart SiteScope to complete the change.

Web Script Monitor Files Directory

The Web Script Monitor runs VuGen scripts to monitor performance and content on Web applications. The VuGen scripts used by the monitor can be stored in the default directory for these scripts, **<SiteScope root directory>\templates.webscripts**, or you can define a different directory in General Preferences.

Note: The Web Script monitor is available only to users accessing SiteScope directly and not to users accessing SiteScope by using System Availability Management Administration in HP Business Availability Center.

Setting the SiteScope Restart Schedule

Restarting the SiteScope server is necessary for clearing problems and resetting monitors. You can select a schedule used for restarting SiteScope in the General Preferences page. Selecting a convenient restart schedule helps minimize or avoid gaps in monitoring coverage and data.

For details on configuring these preferences, see “SiteScope General Preferences User Interface” on page 248.

General Limitations for Using SiteScope in an I18N Environment

- Username, password, and URLs must be in English characters.
- Support for internationalization is available only in the new user interface.
- The machine on which SiteScope is installed (SiteScope machine) and the monitored machine must have the same locale. English is the default locale.

- ▶ The SiteScope machine can have a non-English locale in addition to English. For example, the monitored machine supports the German locale while the SiteScope machine supports German and English. For details on setting a non-English locale, see “Configure SiteScope for a Non-English Locale” on page 231.
- ▶ When deploying the Web Script Monitor, script names and transaction names must also be in English characters.
- ▶ Script monitor on Redhat ES4 does not support parameters in any language other than English.
- ▶ SiteScope always uses "en_US" locale for parsing dates retrieved from remote UNIX machines (for example during a File monitor run). If the UNIX machine's default locale is different from en_US, in the definition of the UNIX remote for this machine, the **Initialize Shell Environment** field must contain "LANG=C; export LANG".

Multi-Lingual User (MLU) Interface Support

The SiteScope user interface can be viewed in the following languages in your Web browser:

Language	Language Preference in Web Browser
English	English
Simplified Chinese	Chinese (China) [zh-cn], Chinese (Singapore) [zh-sg]
Korean	Korean [ko]
Japanese	Japanese [ja]

Use the language preference option in your browser to select how to view SiteScope. The language preference chosen affects only the user's local machine and not the SiteScope machine or any other user accessing the same SiteScope. For details on setting the user interface viewing language, see “View SiteScope User Interface in a Specific Language” on page 233.

Note: The language is determined when you log in to SiteScope; changing the language preference in your browser once you have logged in has no affect until you log out and log back in.

Notes and Limitations

- ▶ There is no language pack installation. All translated languages are integrated into SiteScope Multi-lingual User interface (MLU).
- ▶ Data stays in the language it was entered in, even if the language of the Web browser changes. Changing the language of the Web browser on your local machine does not change the language of monitor definitions and configurations.
- ▶ Names of entities included with the SiteScope installation, such as template examples, solution templates, views, and health monitors, are in English only.
- ▶ SiteScope Help can be viewed in Japanese if that is the language that you have selected for the user interface. When you select **Help on this page** or **SiteScope Help**, it is displayed in Japanese. To activate this function, you must install a software patch. Contact HP Software Support (<http://www.hp.com/go/hpsoftwaresupport>) for further information.
- ▶ Other links in the Help drop-down list, such as **Troubleshooting & Knowledge Base**, **HP Software Support**, and **HP Software Web Site**, are also displayed in the user interface language you selected.

Database Environment Issues

- ▶ When you create a new Oracle instance in an Oracle database, you must specify the character set for the instance. All character data, including data in the data dictionary, is stored in the instance's character set.
- ▶ The Database Query Monitor can connect to an Oracle database but the Oracle user names and passwords must contain only English characters.

Infrastructure Settings Preferences

Infrastructure Settings Preferences enable you to view and define global SiteScope settings without having to access the **master.config** file. Infrastructure Settings Preferences are sorted and grouped into the following categories: General Settings, Server Settings, Monitor Settings, Alert Settings, Persistency Settings, Classic UI, Report Settings, and Baseline Settings.

After you edit setting values in Infrastructure Settings Preferences, SiteScope validates that all input data is in the correct format and warns you if restarting SiteScope is required. You can restart SiteScope from the Infrastructure Settings Preferences page.

For details on configuring infrastructure preference values, see “Infrastructure Settings Preferences User Interface” on page 256.

Integration Preferences

This section includes the main concepts related to HP Business Availability Center integration preferences.

- ▶ “Registering SiteScope to an HP Business Availability Center” on page 216
- ▶ “Using SSL for SiteScope-HP Business Availability Center Communication” on page 217
- ▶ “Changing the Gateway Server to Which SiteScope Sends Data” on page 218

Registering SiteScope to an HP Business Availability Center

To enable logging of SiteScope monitor data to Business Availability Center, the SiteScope must be configured as a data collector for Business Availability Center. This involves registering the Business Availability Center in SiteScope, and adding a SiteScope to the System Availability Management Administration page in the Business Availability Center. For details, see “Configure SiteScope-HP Business Availability Center Integration Preferences” on page 234.

If the HP Business Availability Center Server to which you are connecting is on a different machine than the HP Business Availability Center Server that SiteScope reports data, you must provide connection information for both servers under the Main Settings in SiteScope's Integration Preferences, or Distributed Settings in System Availability Management Administration's New SiteScope Page.

Note: Monitors created in SiteScope before registration to Business Availability Center have their logging option set to **Do not report to HP Business Availability Center**. After you configure SiteScope as a data collector reporting to Business Availability Center, the default for new monitors created in SiteScope is to log their monitoring data to Business Availability Center.

To change logging options use either the Business Availability Center logging options on the Integration Preferences page, or edit a specific monitor and select the **Do not report to HP Business Availability Center** option in the **HP BAC Logging** section of the edit monitor page. For details, see "Integration Preferences User Interface" on page 278 and "HP BAC Logging" on page 525.

Using SSL for SiteScope-HP Business Availability Center Communication

You can use Secure Sockets Layer (SSL) to transmit data from SiteScope to the Business Availability Center server. If you have installed a certificate signed by a root Certificate Authority on the Business Availability Center server, no additional setup is required on the SiteScope server. If you are using a self-signed certificate on the HP Business Availability Center server and want to use that certificate for secure communication with SiteScope, you must perform the steps as described in "Use SSL for SiteScope-HP Business Availability Center Communication" on page 235.

Note:

- ▶ You only need to specify these settings if the certificate installed on the Business Availability Center machine is not signed by a root Certificate Authority (CA). For example, if you are using a certificate signed by a Certificate Authority like Verisign, you do not need to change these settings.
 - ▶ You can import the self-signed certificate into the same keystore file used for other SiteScope monitors but that is not required. You can create a separate keystore for the Business Availability Center server certificate.
-

Changing the Gateway Server to Which SiteScope Sends Data

You can change the Gateway Server to which a SiteScope reports its data. Generally, this is only applicable if you are working with an HP Business Availability Center deployment with components installed on more than one server. You make this change by entering the required Gateway Server name or IP address in the **Business Availability Center server machine name/IP address** box in the Integration Preferences page. You must also update the SiteScope settings with the Gateway Server name in System Availability Management Administration.

Note: This function can only be used for changing the Gateway Server for a SiteScope that is already registered with a given HP Business Availability Center installation. It cannot be used to add a new SiteScope, or to connect a SiteScope to a different HP Business Availability Center system.

For information about troubleshooting reporting data to HP Business Availability Center, see “Troubleshooting and Limitations” on page 334.

For details on configuring these preferences, see “Integration Preferences User Interface” on page 278.

Failover Preferences

Note: Failover Preferences are available only to users accessing SiteScope Failover that have a SiteScope Failover license.

When using SiteScope Failover, a special version of SiteScope that includes automated mirroring and failover functionality, you can use Failover Preferences to indicate a primary SiteScope to be mirrored and set how often the configurations should be mirrored to the failover SiteScope installation.

For details on configuring these preferences, see “Failover Preferences User Interface” on page 283.

Microsoft Windows Remote Preferences

SiteScope must be able to establish a connection to the servers you want to monitor. It must also be authenticated as a user having permissions to access the Windows performance registry on the remote machine. Microsoft Windows Remote Preferences options are used to set up the connection properties, such as credentials and protocols, so that SiteScope can monitor systems and services running in remote environments. Multiple monitors can use the same connection profile. For details on enabling SiteScope to monitor data on remote Windows servers, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.

For information about troubleshooting and limitations of SiteScope monitoring of remote Windows NT and Windows 2000 servers, see “Troubleshooting and Limitations” on page 334.

For details on configuring these preferences in the user interface, see “Microsoft Windows Remote Preferences User Interface” on page 285.

UNIX Remote Preferences

SiteScope must be able to establish a connection to the servers you want to monitor. It must also be authenticated as a remote user with permissions to run command line tools on the remote machine as a remote user. UNIX Remote Preferences options are used to set up the connection properties, such as credentials and protocols, so that SiteScope can monitor systems and services running in remote UNIX environments. Multiple monitors can use the same connection profile. To enable SiteScope to monitor data on remote UNIX servers, you must perform the following:

- ▶ Define an individual remote UNIX server connection profile for each server
- ▶ Create or modify an account on the remote server that corresponds with the connection method and permissions you intend to grant to SiteScope as a "remote user" logging onto that server
- ▶ Configure the remote server in UNIX Remote Preferences and test the connection to validate credentials and connectivity

After you define a remote UNIX connection profile, you can create monitors to watch the resources and performance counters for that server. Multiple monitors can use the same connection profile. Click the Server list on the New Monitor page to display a list of the remote servers you have defined. You can then select the server that you want to monitor.

Note: You can use SiteScope UNIX operating system adapters to extend SiteScope to connect to, and remotely monitor versions of UNIX that are not supported by default. For details, see “UNIX Operating System Adapters” on page 1529.

For information about troubleshooting and limitations of SiteScope monitoring of remote UNIX servers, see “Troubleshooting and Limitations” on page 334.

For details on configuring these preferences, see “UNIX Remote Preferences User Interface” on page 291.

Log Preferences

Log Preferences enable you to select how much monitor data is accumulated and maintained on the SiteScope server. It also configures SiteScope to export monitor data to an external database.

By default, SiteScope saves monitor results, alert data, error data, and other readings returned by monitors into log files. For monitor data results, a date-coded log file is created for each 24-hour period of monitoring. This data is stored as tab delimited text. SiteScope uses the log files to create management reports on system availability and performance over time.

Storing data logs can become a problem over time. However, you can limit how much log information SiteScope saves to the local file system by setting the number of days to maintain log files or by setting a maximum data log file size. You can also send monitoring data to an external database application. This helps reduce the data storage capacity required on the SiteScope server and makes the monitoring data available to other reporting tools.

Note: To create SiteScope Management Reports the monitoring log information for the desired time period of the report must be available on the SiteScope server file system. For details on creating management reports, see “Management Report” on page 1473.

For details on configuring these preferences, see “Log Preferences User Interface” on page 301.

E-mail Preferences

The E-mail Preferences container includes two view panels; the Properties panel and the Contents panel.

The E-mail Preferences Properties panel is used to configure the settings SiteScope needs to communicate with an external e-mail server. These are the default settings that SiteScope uses to send alerts as e-mail messages.

The E-mail Preferences Contents panel is used to define custom E-Mail Recipient profiles to send e-mail alert messages to recipients other than the one defined in the Properties panel. The E-mail Recipient profile can then be associated with one or more E-mail alerts by editing the applicable alert definition.

For details on configuring these preferences, see “E-mail Preferences User Interface” on page 304.

Pager Preferences

Pager Preferences includes two view panels; the Properties panel and the Contents panel.

The Pager Preferences Properties panel is used to configure the settings SiteScope needs to communicate with an external electronic paging service. These are the default settings that SiteScope uses to send alerts to an electronic pager.

The Pager Preferences Contents panel is used to define custom Pager Recipient profiles other than the one defined in the Properties panel. The Pager Recipient profile can then be associate with one or more Pager alerts by editing the applicable alert definition.

The preferred pager connection option is to connect directly to a **modem at your pager service**. When a modem-to-modem connection is used, SiteScope is able to verify that the message was sent successfully and can receive messages describing any communication problem. The other connection options generally send messages to automated voice response systems using touch tone dialing. The touch tone dialing method is limited to numeric messages and SiteScope cannot confirm that your paging service correctly received the message.

For details on configuring these preferences, see “Pager Preferences User Interface” on page 309.

SNMP Trap Preferences

The SNMP Trap Preferences container includes two view panels; the Properties panel and the Contents panel.

The SNMP Trap Preferences Properties panel is used to configure the settings SiteScope needs to communicate with an external SNMP host or management console. These are the default SNMP parameters for use with SNMP Trap alerts.

The SNMP Trap Preferences Contents panel is used to define custom SNMP Trap profiles or templates to send traps to hosts other than the one defined in the Properties panel. The SNMP Trap profile can then be associated with one or more SNMP Trap alerts by editing the applicable alert definition.

For details on configuring these preferences, see “SNMP Trap Preferences User Interface” on page 316.

Absolute Schedule Preferences

SiteScope monitors, alerts, and reports are enabled 24 hours a day, 7 days a week, 365 days a year by default. This means that as long as a monitor is enabled, it is run according to the update frequency specified in the individual monitor configuration. For example, if a monitor is configured to run every 30 seconds, SiteScope attempts to run the monitor every 30 seconds throughout the day. If SiteScope detects an error condition, any associated alert is triggered as well, regardless of the time of day.

In some situations, it is useful to enable certain SiteScope actions to correspond with a single event or a particular time of day. For example, you may want to use this type of scheduling for monitors, such as the Link Checking monitor, which you want to run only once a day at a time when the server generally has a lighter load.

Absolute Scheduling lets you set specific times that a monitor is run on a weekly basis. Absolute schedules are reset at the end of the week and repeated each week. Absolute Schedule Preferences triggers a monitor to run only once at each time specified in the schedule.

Absolute Schedule Preferences are inactive until they are explicitly associated with a monitor instance. Use the Advanced Settings section of a monitor configuration page to associate Absolute Schedule Preferences with a monitor.

Note: Absolute Schedule Preferences are associated to alerts indirectly by way of the monitors associated with the alert. Any alerts associated with the monitors disabled by Absolute Schedule Preferences are effectively unavailable for the period during which those monitors are disabled. However, if an alert is associated with other monitors that are not controlled by the same schedule, that alert is still triggered if the other monitors report an error condition.

For details on configuring these preferences, see “Absolute Schedule Preferences User Interface” on page 319.

Range Schedule Preferences

SiteScope monitors, alerts, and reports are enabled 24 hours a day, 7 days a week, 365 days a year by default. This means that as long as a monitor is enabled, it is run according to the update frequency specified in the individual monitor configuration. For example, if a monitor is configured to run every 30 seconds, SiteScope attempts to run the monitor every 30 seconds throughout the day. If SiteScope detects an error condition, any alert associated with the monitor is triggered as well, regardless of the time of day.

In some situations, it is useful to enable and disable certain SiteScope actions based on the schedules of the individuals or groups responsible for the servers and systems being monitored. You use Range Schedule Preferences to instruct SiteScope to enable or disable monitors according to time periods that you define.

You can use Range Scheduling to specify a time range during which SiteScope either enables or disables particular monitors. If you specify an enabled time range for a new monitor (using the Advanced Options on the Add monitor page), SiteScope only runs the monitor during that range. For example, if you create a range of 8AM- 9PM, Monday through Friday, any monitors that have that range schedule associated with them are run only during those times.

A common use of range scheduling is to set up different pager alerts associated with monitors running at times that coincide with work shifts when different administrators are on call. The schedule helps prevent pager alerts being sent to individuals at an inappropriate time of day relative to the work schedule of that individual.

Range Schedule Preferences are inactive until they are explicitly associated with a monitor instance. You use the Advanced Settings section of a monitor configuration page to associate Range Schedule Preferences with a monitor.

Note: Range Schedule Preference are associated to alerts indirectly by way of the monitors associated with the alert. Any alerts associated with the monitors disabled by Range Schedule Preference are effectively unavailable for the period during which those monitors are disabled. However, if an alert is associated with other monitors that are not controlled by the same schedule, that alert is still triggered if the other monitors report an error condition.

For details on configuring these preferences, see “Range Schedule Preferences User Interface” on page 321.

User Preferences

Note: User Preferences are available only to users accessing SiteScope directly and not to users accessing SiteScope using System Availability Management Administration in HP Business Availability Center.

You manage SiteScope user accounts from the Users Preferences page. This page enables you to administer the users that are allowed access to SiteScope.

As a client-server based architecture, a single SiteScope user profile can be accessed by multiple users simultaneously. You can define multiple SiteScope user accounts that provide different view and edit permissions for different audiences. For example, you can create a user profile that allows users to view monitor status and reports but does not enable the users to add or edit monitor configurations or alerts.

A user profile limits access to SiteScope to those users that enter a correct user name and password. Optionally, user authentication can be handled by submitting a query to a LDAP database. For more restrictive access control to SiteScope, see “SiteScope General Preferences User Interface” on page 248 for options on how to restrict access to SiteScope to certain IP addresses only.

A user profile has two main components:

- ▶ User authentication information and access permission
- ▶ Action permissions

Configure these settings for each user profile in the applicable User Profile container.

User Types

SiteScope provides the following user types:

- ▶ **Administrator.** SiteScope provides a single administrator by default. An administrator can view and change anything in SiteScope. It has other special properties as well, such as being allowed to create other users and to change their profiles on the Users Preferences form. The administrator account cannot be disabled or deleted.
- ▶ **Power user (super user).** A power user has all the permissions of an administrator except that it cannot delete itself or the administrator. Both an administrator and a power user can create a power user. There may exist any number of power users. For details about enabling this user type, see “Preference Settings” on page 330.
- ▶ **Regular User.** A regular user cannot create, delete, or edit other users. It has all the permissions defined for it by the administrator or power user.

Note:

- ▶ The administrator account is the default account used when accessing SiteScope. This means that anyone requesting the server address and port number where SiteScope is running is, by default, logged in on the administrator account. To restrict access to this account and its privileges, you must edit the administrator account profile to include a user login name and login password. SiteScope then displays a login dialog before SiteScope can be accessed.
 - ▶ You can create a named user account that does not require a user login name and password. You do this by creating a new user profile by providing a **Title**, but leaving the **Login Name** and **Password** boxes blank. With this configuration, users accessing SiteScope are presented with an authentication dialogue. They may be authenticated as this named user by leaving the **Login Name** and **Password** boxes blank and clicking the **Log In** button.
 - ▶ You should restrict the permissions on this type of account to avoid unauthorized changes to your SiteScope configuration.
-

Changing a User's Password

You can change a user's password by clicking the **Change Password** link in the SiteScope Login window, and entering the user's user name, current password, and a new password in the Change Password dialog box.

If the new password does not comply with password configuration rules, an error message is displayed and the password is not changed. For password configuration rules, see "Password Requirement Parameters" on page 247.

For details on configuring these preferences, see "User Preferences User Interface" on page 324.

Credential Preferences

Credential Preferences provides centralized credential management for SiteScope resources. It enables you to input user names and passwords for SiteScope monitors, templates, and remote hosts once, and then have SiteScope automatically supply that information when you configure those resources.

Using Credential Preferences enables you to:

- Create and manage your credentials. You can add, modify, and delete credentials from one central location.
- Update credentials. If credentials for a resource expire or need to be updated, the credential profile can be updated and the changes are applied to all usages of the resource within SiteScope. This saves having to find and manually update all usages of the resource in SiteScope.
- Keep user credentials secure. All passwords stored in Credential Preferences are encrypted. Only an administrator, or a user granted **Edit Preferences** permissions, can make changes to the credentials.
- Search and replace by credential properties, and replace credentials with other credentials using Global Search and Replace.
- Copy monitors in SiteScope with their credential settings. You can also copy monitors to other SiteScopes when there is more than one SiteScope connected to Business Availability Center (only available through System Availability Management Administration). If a credential profile does not exist in the SiteScope to which the monitor is copied, the credential profile is created in that SiteScope.

This section includes:

- “Monitoring Credential Profiles” on page 230
- “Supported Monitors” on page 230
- “Notes” on page 231

Monitoring Credential Profiles

If user credentials expire or change, the monitors using these credentials will fail and be in **Error** status. To avoid this situation, you can create a monitor for each credential profile that checks the authentication, and makes all monitors of the monitor type dependent on the test monitor. For example, you can create an IPMI monitor, `IPMI_test_credentials`, and manually configure the server login and password. When you configure your IPMI monitors, in Advanced Settings, enter `IPMI_test_credentials` in the **Depends on** box and select Available as the **Depends Condition**. If the `IPMI_test_credentials` monitor becomes unavailable for any reason, the IPMI monitors are automatically disabled.

Supported Monitors

You can use Credential Preferences to store credentials for the following monitors:

Monitor Category	Monitor
Application	<ul style="list-style-type: none"> ▶ SAP CCMS ▶ SAP CCMS Alert ▶ SAP Java Web Application Server ▶ SAP Performance ▶ SAP Work Processes ▶ Siebel Application Server ▶ WebSphere Application Server
Database	<ul style="list-style-type: none"> ▶ Database Counter ▶ DB2 8.x ▶ Oracle Database
Server	<ul style="list-style-type: none"> ▶ IPMI
Web Transaction	<ul style="list-style-type: none"> ▶ URL ▶ URL Content ▶ URL List

Notes

- ▶ Copying credential settings to other SiteScopes is not supported when copying monitors to older versions of SiteScope.
- ▶ You cannot delete a credential profile if it is referenced by a monitor or a remote host. You must remove the credential profile from each dependency before you can delete the credential profile.
- ▶ If a credential that is used in a template remote host or template monitor has been deleted, you must add the missing credential to Credential Preferences or manually enter credentials for the resource in the template object before deploying the template.

For details on how to configure Credential Preferences, see “Configure Credential Preferences” on page 243.

For details on the user interface, see “Credential Preferences User Interface” on page 332.

Configure SiteScope for a Non-English Locale

This task describes the steps involved in configuring SiteScope for a non-English locale.

This task includes the following steps:

- ▶ “Change the Locale Version Setting” on page 232
- ▶ “Set New Locale Time and Data Settings” on page 232
- ▶ “View SiteScope User Interface in a Specific Language” on page 232
- ▶ “Results” on page 232

1 Change the Locale Version Setting

In the monitor tree, select **Preferences > General Preferences**, and click **Edit**. In the Main Settings view, select **International Version**, and click **OK**. Restart SiteScope. This enables SiteScope to work with multiple character sets.

2 Set New Locale Time and Data Settings

You can set a new locale time and data settings for SiteScope.

- a** Open `<SiteScope root directory>\groups\master.config` in a text editor.
- b** Find the entry `_localeCountry=`, and assign it an uppercase 2-character ISO-3166 country code. For example: `_localeCountry=US`. A list of country codes is available at http://www.chemie.fu-berlin.de/diverse/doc/ISO_3166.html.
- c** Find the entry `_localeLanguage=`, and assign it a lowercase 2-character ISO-639 language code. For example: `_localeLanguage=en`. A list of language codes is available at <http://www.ics.uci.edu/pub/ietf/http/related/iso639.txt>.
- d** Save the file and restart SiteScope.

3 View SiteScope User Interface in a Specific Language

Select a language preference for viewing the SiteScope user interface. For details on how to perform this task, see “View SiteScope User Interface in a Specific Language” on page 233.

4 Results

SiteScope is configured to work with multiple foreign character sets, the time and data settings are displayed in a locale-specific format, and the user interface is displayed in a foreign language.

View SiteScope User Interface in a Specific Language

This task describes how to select a language preference for viewing the SiteScope user interface.

Note: For a list of supported languages, see “Multi-Lingual User (MLU) Interface Support” on page 214.

To view SiteScope user interface in a specific language:

- 1** Install the required language’s fonts on your local machine if they have not yet been installed. If you choose a language in your Web browser whose fonts have not been installed, the SiteScope user interface uses the default language of your local machine.

For example, the default language on your local machine is English and the Web browser is configured to use Japanese. If Japanese fonts are not installed on the local machine, the SiteScope user interface is displayed in English.

- 2** If you use Internet Explorer, configure the Web browser on your local machine to select the language in which you want to view the SiteScope user interface. For details, see <http://support.microsoft.com/kb/306872/en-us>. Go to step 4.
- 3** If you use FireFox, configure the Web browser on your local machine as follows:
 - a** Select **Tools > Options > Advanced**. Click **Edit Languages**. The Language dialog box opens.
 - b** Highlight the language in which you want to view SiteScope.
If the language you want is not listed in the dialog box, expand the **Select language to add...** list, select the language, and click **Add**.
 - c** Click **Move Up** to move the selected language to the first row.
 - d** Click **OK** to save the settings. Click **OK** to close the Language dialog box.
- 4** Click **LOGOUT** at the top of the SiteScope window. SiteScope refreshes and the user interface is displayed in the selected language.

Configure SiteScope-HP Business Availability Center Integration Preferences

This task describes the steps involved in configuring SiteScope as a data collector for Business Availability Center.

This task includes the following steps:

- ▶ “Register SiteScope to an HP Business Availability Center” on page 234
- ▶ “Specify Connection Parameters to HP Business Availability Center Servers” on page 234
- ▶ “Configure SSL for SiteScope-HP Business Availability Center Communication” on page 235

1 Register SiteScope to an HP Business Availability Center

- a** In SiteScope, register the Business Availability Center to the SiteScope in the Main Settings on the Integration Preferences page. For details on the user interface, see “Integration Preferences User Interface” on page 278.
- b** In Business Availability Center, add a SiteScope to the System Availability Management Administration page. For details on the user interface, see “New SiteScope Page” on page 65.

2 Specify Connection Parameters to HP Business Availability Center Servers

Complete the other connection options in the Integration Preferences page. For details on the user interface, see “Integration Preferences User Interface” on page 278.

3 Configure SSL for SiteScope-HP Business Availability Center Communication

If you are using a self-signed certificate on the HP Business Availability Center server and want to use that certificate for secure communication with SiteScope, you must import the certificate from the Business Availability Center server to the keystore on the SiteScope server and add three entries to the **master.config** file on the SiteScope server. For details on this topic, see “Use SSL for SiteScope-HP Business Availability Center Communication” on page 235.

Use SSL for SiteScope-HP Business Availability Center Communication

This task describes the steps involved in enabling secure communication between SiteScope and HP Business Availability Center using a self-signed certificate.

To use a self-signed certificate on the HP Business Availability Center server for secure communication with SiteScope:

- 1 Obtain a copy of the self-signed certificate from the Business Availability Center server saved in a DER-encoded binary X.509 format. Normally, the certificate file has an extension of *.cer.
- 2 Import the certificate into a keystore on the SiteScope server using the procedures described in “Configuring SiteScope to Use SSL” in the *HP SiteScope Deployment Guide* PDF.

Note: It is not necessary to create the certificate request file, because you already have a certificate.

- 3 Edit the **master.config** file in the `<SiteScope_root_directory>\groups` using a text editor. Add the following three entries with the data indicated:

```
_sslTrustedCertKeyStoreFile=<path>\<filename>  
_sslTrustedCertKeyStorePassword=<keystorepassword>  
_sslAcceptAllUntrustedCerts=<boolean>
```

For example, the entries added to the **master.config** file may be as follows:

```
_sslTrustedCertKeyStoreFile=c:\keystores\topaz.keystore  
_sslTrustedCertKeyStorePassword=sUp3rS3cr3tP@ssw0RD  
_sslAcceptAllUntrustedCerts=false
```

- 4 Save the changes to the file.
- 5 Restart the SiteScope server.

Configure SiteScope to Monitor a Remote Windows Server

This task describes the steps involved in configuring SiteScope to monitor data on remote Windows servers.

This task includes the following steps:

- ▶ “Enable SiteScope to Monitor Data on Remote Windows Servers” on page 237
- ▶ “Configure User Permissions for Remote Monitoring” on page 237
- ▶ “Configure and Test the Settings for the Windows Remote Server” on page 237
- ▶ “Results” on page 238

1 Enable SiteScope to Monitor Data on Remote Windows Servers

To enable SiteScope to monitor data on remote Windows servers, you must perform one of the following steps:

- ▶ Define an individual remote Windows server connection profile for each server. For details on how to perform this task, see “Define Remote Windows Server Connection Profiles” on page 239.
- ▶ Set domain access privileges to permit SiteScope to access remote servers. For details on how to perform this task, see “Set Domain Privileges for SiteScope Monitoring” on page 239.

2 Configure User Permissions for Remote Monitoring

Configure the user permissions to access the remote machine according to the operating system on the SiteScope machine. For details on how to perform this task, see “Configure User Permissions for Remote Monitoring” on page 241.

3 Configure and Test the Settings for the Windows Remote Server

Configure the remote Windows server in Microsoft Windows Remote Preferences. For details on the user interface, see “Microsoft Windows Remote Preferences” on page 219.

After defining the Microsoft Windows Remote Preferences definition for SiteScope, click the **Test** link for the applicable server in the list of Microsoft Windows Remote Preferences servers to test the connection.

Note:

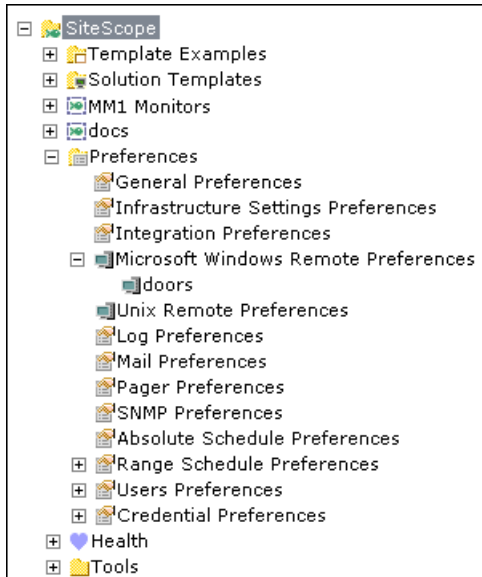
- ▶ If an "unable to connect to remote machine" error message opens when trying to view remote counters, refer to the Microsoft Knowledge Base (<http://support.microsoft.com/kb/300702/>).
 - ▶ Testing SSH connectivity to a remote Windows server using the Plink connection method for key-based Authentication returns a success message even if the test fails.
-

4 Results

The remote Windows server is added to the list of remote Windows servers in the Microsoft Windows Remote Preferences container. You can then create monitors to watch the resources and performance counters for that server.

Tip: When deploying a monitor, select **Display only configured servers to display** and then click **Get Servers** to display only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences.

Example



Define Remote Windows Server Connection Profiles

Monitoring remote Windows server data requires authenticated access to the remote server. A Windows server connection profile provides the necessary address and login credentials for SiteScope to log in to a remote server and to access the Windows performance registry on that remote machine. To use this method, either:

- ▶ Log on to the remote server as a user with administrator privileges.
- ▶ Create or modify a user account on the remote server that corresponds with the connection method and login permissions used in the SiteScope connection profile for that server.

Set Domain Privileges for SiteScope Monitoring

SiteScope for Windows automatically generates a list of servers visible in the local domain. These servers are listed in the Servers list for monitor types where a server must be specified. SiteScope running on Windows may be able to use this list to monitor remote Windows servers without having to create individual connection profiles for each server.

You can set domain privileges using any of the following methods:

- ▶ **Set the SiteScope service to run as a user in the Domain Admin group.**
By default, SiteScope is installed to run as a Local System account. You can set the SiteScope service to log on as a user with domain administration privileges. This gives SiteScope access privileges to monitor server data within the domain. For details on how to change the SiteScope account user, see “Change the User Account of the SiteScope Service” on page 240.
- ▶ **Add the server where SiteScope is running to the Domain Admin group in ActiveDirectory (for Windows 2000 or later).**

With this option, the SiteScope service is set to log on as a Local System account, but the machine where SiteScope is running is added to a group having domain administration privileges.

- ▶ **Edit the registry access permissions for all machines in the domain to allow non-admin access.**

This option requires changes to the registry on each remote machine that you want to monitor. This means that while the list of servers in the domain includes all machines in the domain, only those remote machines whose registry has been modified can be monitored without use of a connection profile.

Change the User Account of the SiteScope Service

This task describes the steps involved in changing the user account of the SiteScope service.

To change the user account of the SiteScope service:

- 1** Select **Start > Programs > Administrative Tools > Services**, and select **SiteScope** from the list of services. The SiteScope Properties dialog box opens.
- 2** Click the **Log On** tab, and in the **Log on as** area, enter an account that can access the remote servers.
- 3** Click **OK** to save your settings and close the SiteScope Properties dialog box.
- 4** Right-click **SiteScope**. Click **Stop** to stop the SiteScope service.
- 5** Click **Start**. The SiteScope service now uses the new account.

Configure User Permissions for Remote Monitoring

For SiteScope to collect performance measurements on a remote machine, SiteScope must have permission to access the remote machine. This task describes how to configure user permissions according to the operating system on the SiteScope machine.

Note:

- ▶ Microsoft Best Practice recommends giving permissions to groups instead of to users.
 - ▶ Back up the registry before making any registry changes.
-

To configure Windows XP and Windows 2003:

- 1** On the SiteScope machine, select **Start > Run**. In the Open text box, enter **Regedt32.exe**. The Registry Editor dialog box opens.
- 2** In the **HKEY_LOCAL_MACHINE** window, select **SOFTWARE > Microsoft > Windows NT > CurrentVersion > Perflib**.
- 3** Click **Security** in the Registry Editor tool bar and select **Permissions**. The Permissions for Perflib dialog box opens.
- 4** In the Name pane, highlight the user SiteScope uses to access the remote machine. In the Permissions pane, select the **Allow** check box for **Read**. Click **OK** to save the configuration and close the Permissions for Perflib dialog box.
- 5** In the **HKEY_LOCAL_MACHINE** window, select **SYSTEM > CurrentControlSet > Control > SecurePipeServers > winreg**. Click **Security** in the Registry Editor tool bar and select **Permissions**. The Permissions for Winreg dialog box opens.

- 6 In the Name pane, highlight the user that SiteScope uses to access the remote machine. In the Permissions pane, select the **Allow** check box for **Read**. Click **OK** to save the configuration and close the Permissions for Perflib dialog box.
- 7 In the Registry Editor tool bar, click **Registry** and select **Exit** to save the configuration and exit.
- 8 Restart the SiteScope machine.

Note: For information about enabling non-administrative users to monitor performance on a remote machine, refer to the Microsoft Knowledge Base (<http://support.microsoft.com/kb/q164018/>).

To configure Windows 2000:

- 1 On the SiteScope machine, select **Start > Programs > Administrative Tools > Computer Management**. The Computer Management dialog box opens.
- 2 In the System Tools tree, expand the **Local Users and Groups** tree and select **Groups**. All groups on the machine are listed in the right-hand pane.
- 3 In the right-hand pane, select the **Administrators** group. The Administrators Properties dialog box opens.
- 4 If the user that SiteScope uses to access the remote machine is listed in the Members pane, go to step 5. If the user is not listed, click **Add**. The Select Users or Groups dialog box opens.
 - a Enter the user in the text box.
 - b Click **OK** to save the configuration and close the Select Users or Groups dialog box.
- 5 Click **OK** to save the configuration and close the Administrators Properties dialog box.
- 6 In the Computer Management dialog box, click **File** in the tool bar and select **Exit**.
- 7 Restart SiteScope on the SiteScope machine.

Configure Credential Preferences

This task describes the steps involved in configuring and managing credentials for SiteScope objects that require user authentication.

This task includes the following steps:

- “Prerequisites” on page 243
- “Create a Credential Profile” on page 243
- “Configure SiteScope Resources Using Credential Profiles” on page 243
- “Update Credential Profiles” on page 244
- “Results” on page 238

1 Prerequisites

To create or make changes to the credentials, you must be an administrator in SiteScope, or a user granted **Edit Preferences** permissions.

2 Create a Credential Profile

Configure a credential profile in Credential Preferences for each SiteScope monitor, template, and remote host that requires user authentication. For details on the user interface, see “Credential Preferences User Interface” on page 332.

For a list of supported monitors, see “Supported Monitors” on page 230.

3 Configure SiteScope Resources Using Credential Profiles

When you configure a SiteScope resource that has a credential profile, select the profile in the **Credentials** box in the resource’s Main Settings area.

- For details on the user interface when configuring a monitor, see the Main Settings for the specific monitor.
- For details on the user interface when configuring a remote server, see “Microsoft Windows Remote Preferences User Interface” on page 285, and “UNIX Remote Preferences User Interface” on page 291.

4 Update Credential Profiles

If credentials for a resource change, you can update the credential profile without having to find all usages of the resource and update each resource separately in SiteScope. To change a profile, select the profile in Credential Preferences, click **Edit**, and make the necessary changes. For details on the user interface, see “Credential Preferences User Interface” on page 332.

5 Results

SiteScope authenticates the login and password for the resource using the credentials supplied in Credential Preferences.

Monitors Tested for Internationalization

The following monitors have been tested for internationalization.

Windows Operating System

- CPU Monitor
- Database Counter Monitor
- Database Query Monitor
- Disk Space Monitor
- IIS Server Monitor
- Link Check Monitor
- Log File Memory Monitor
- Microsoft SQL Server Monitor
- Microsoft Windows Event Log Monitor
- Microsoft Windows Performance Counter Monitor
- Microsoft Windows Resources Monitor
- Oracle 9i Application Server Monitor
- Oracle 10g Application Server Monitor

- Ping Monitor
- Script Monitor
- Service Monitor
- SNMP Monitor
- SNMP Trap Monitor
- UDDI Monitor
- URL Monitor
- URL Content Monitor
- URL List Monitor
- URL Sequence Monitor
- Web Script Monitor

UNIX Operating System

- CPU Monitor
- Database Query Monitor
- Disk Space Monitor
- Log File Monitor
- Port Monitor
- Script Monitor
- Service Monitor
- UNIX Resources Monitor
- URL Monitor
- URL Content Monitor
- URL Sequence Monitor

SiteScope Log Database Table Structure

When database login is enabled, monitor data is contained in a single table called **SiteScopeLog**. The first nine fields of each database record are the same for all monitors. The next ten fields contain different measurements depending on the kind of monitor supplying the data. All the fields in the table use the VARCHAR(255) data type. A description of the fields in the log database record are shown in the table below along with their default field names:

Field Name	Example Data	Description
datex	1999-01-20 11:54:54	The first field contains the date that the monitor ran.
serverName	demo.sitescope.com	The second field contains the name of the server where SiteScope is running.
class	URLMonitor	The third field contains the type of the monitor.
sample	23	The fourth field contains the sample number of this monitor.
category	good	The fifth field contains the category name of the monitor.
groupName	URLs	The sixth field contains the group name of the monitor.
monitorName	Home Page	The seventh field contains the name of the monitor.
status	1.01 seconds	The eighth field contains the status of the monitor.
monitorID	10	The ninth field contains the ID of the monitor.
value1, value2, ... value10	(variable)	The tenth through nineteenth fields contain the monitor specific data as described in the Log Columns page. The first variable field (value1) corresponds to the value listed as column 7 in the log files.

The SQL statement that is used for database logging can be changed by editing the parameter `_logJdbcInsertSiteScopeLog=` in the `<SiteScope root directory>\groups\master.config` file. A stored procedure can be called by replacing the insert statement with a call statement. For example, `call logit(?,?,?)` would call the stored procedure named `logit` passing it the first three parameters.

Password Requirement Parameters

You can configure password requirements by setting the following parameters in `<SiteScope root directory>\groups\master.config`:

Parameter	Description
<code>_adminMinimumLength = x</code>	The password length must be at least x characters.
<code>_adminRequireAlpha = (1,0)</code>	<ul style="list-style-type: none"> ▶ 0. Password does not require an alphabetic character. ▶ 1. Password must contain an alphabetic character.
<code>_adminRequireNumber = (1,0)</code>	<ul style="list-style-type: none"> ▶ 0. Password does not require a numeric character. ▶ 1. Password must contain a numeric character.
<code>_adminRequirePunctuation = (1,0)</code>	<ul style="list-style-type: none"> ▶ 0. Password does not require punctuation. ▶ 1. Password must contain punctuation.

Preferences User Interface

This section describes:

- ▶ SiteScope General Preferences User Interface on page 248
- ▶ Infrastructure Settings Preferences User Interface on page 256
- ▶ Integration Preferences User Interface on page 278

- ▶ Failover Preferences User Interface on page 283
- ▶ Microsoft Windows Remote Preferences User Interface on page 285
- ▶ UNIX Remote Preferences User Interface on page 291
- ▶ Log Preferences User Interface on page 301
- ▶ E-mail Preferences User Interface on page 304
- ▶ Pager Preferences User Interface on page 309
- ▶ SNMP Trap Preferences User Interface on page 316
- ▶ Absolute Schedule Preferences User Interface on page 319
- ▶ Range Schedule Preferences User Interface on page 321
- ▶ User Preferences User Interface on page 324
- ▶ Credential Preferences User Interface on page 332

SiteScope General Preferences User Interface

Description	Use to enter and view licensing information, and other general display functions, optional functions, and access options for SiteScope. To access: Expand Preferences in the monitor tree and click General Preferences .
Important Information	Only an administrator in SiteScope, or a user granted Edit Preferences permissions, can create or make changes to SiteScope Preferences.
Included in Tasks	“Configure SiteScope for a Non-English Locale” on page 231
Useful Links	“General Preferences” on page 211

The SiteScope General Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
License Number	Enter SiteScope license number to register SiteScope monitors. This number is issued when purchasing a set of monitors. A license must be purchased if intending to use SiteScope beyond the trial period.
Option Licenses	If you have purchased licensing for optional SiteScope monitoring capabilities, enter the license number. Generally, this license key has the same syntax as the SiteScope license. If you have purchased multiple license keys, enter each key separated with a comma.
Options Enabled	Displays information about the license as entered in the License Number and Option Licenses boxes. This includes the total number of monitor points permitted by the license and how many points have been used, plus a label for any optional monitor license keys entered.
Locale-Specific Date and Time	Select to have SiteScope display dates and times in a format that is applicable to a certain locale, country, or culture. To use a different locale setting, modify the SiteScope configuration file to include the codes for the desired locale and select this option in the General Preferences Settings. Default value: United States format

GUI Element	Description
International Version	<p>Select to enable international character sets. When this option is selected, SiteScope honors all character encoding. Use this option to instruct SiteScope to simultaneously handle character encoding from multiple sources and operating systems (for example, foreign language Web pages).</p> <p>If not selected, only the default character set of the operation system where SiteScope is installed is supported. The exceptions are all the URL monitor types, the Log File Monitor, and the File Monitor. These monitor types support multiple character encoding regardless of the International Version option setting.</p>
Number of backups per file	<p>Enter the number of SiteScope configuration file backups to be kept. This function helps preserve important monitor, alert, and general SiteScope configuration information. This number represents the number of backups per file that is maintained. SiteScope uses a naming convention of filename.bak.1, filename.bak.2, filename.bak.#, where 1 is the latest backup file.</p> <p>Example: You can backup files containing general SiteScope configuration information in <code><SiteScope root directory>\groups</code>.</p>
Default Authentication Username	<p>Enter the default user name to be used for authentication with remote systems. Both <code><username></code> and <code><DOMAIN>\<username></code> are valid formats. SiteScope uses this user name unless a different user name is entered explicitly as part of the monitor configuration.</p>
Default Authentication Password	<p>Enter the default password to be used for authentication with remote systems. SiteScope uses this password for the monitor types listed above unless a different password is entered explicitly as part of the monitor configuration.</p>

GUI Element	Description
Preemptive Authorization	<p>Select an option used for authenticating the default user credentials when SiteScope requests the target URL.</p> <ul style="list-style-type: none"> ▶ Authenticate first request. Sends the username and password on the first request SiteScope makes for the target server. ▶ Authenticate if requested. Sends the username and password on the second request if the server requests a username and password.
Suspend All Monitors	<p>Select to temporarily suspend the execution of all monitors. Use to make configuration changes across your monitoring infrastructure. To reactivate monitoring, clear the option.</p> <p>Note: This option disables all monitors currently defined for this SiteScope installation. If setting Suspend Monitors and later clearing this option to re-enable the monitors, the individual monitors that were set as disabled prior to the Suspend Monitors action, retain their original disabled state.</p> <p>Using this option may affect reports. Monitors that would have run during the time that monitoring was suspended may display blanks for that period in reports.</p> <p>Warning: There is currently no visual indication in the interface that SiteScope is in a suspended monitor state. When the Suspend Monitors option is enabled, the following message is displayed: SiteScope is in Suspended mode; no monitors are currently running.</p>
Enable Configuration Files	<p>This option enables the use of the master and monitor group configuration files for SiteScope. When enabled, SiteScope periodically checks for changes to any files in the SiteScope\groups directory and updates the binary configuration data accordingly.</p>

GUI Element	Description
VuGen scripts path route	<p>Enter a directory to store the zip files of VuGen scripts for use by the Web Script Monitor. The files in the directory you enter here appear in the list of available scripts when configuring the Web Script Monitor. If you do not enter a value here, the files in the default directory <SiteScope root directory>\templates.webscripts appear when configuring the monitor.</p> <p>For details on working with the monitor, see “Web Script Monitor Overview” on page 984.</p>
SiteScope restart schedule	<p>Select the schedule used for restarting SiteScope. You can define schedules in Absolute Schedule Preferences. For details, see “Absolute Schedule Preferences User Interface” on page 319.</p> <p>Note: SiteScope must be restarted at least once every 24 hours. Any Absolute Schedule that contains an interval of more than 24 hours between schedule times is not displayed in the restart schedule list.</p> <p>Default value: Every 24 hours after start</p>

SSH Preferences

Description	Use to configure preferences for securely accessing a remote computer. To access: Expand Preferences in the monitor tree and click General Preferences . Click SSH Preferences .
Useful Links	“General Preferences” on page 211

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
SSH V2 Connect Timeout	Enter the total number of seconds SiteScope should wait for a successful reply. When the time is exceeded, the connection is automatically closed. Default value: 30
SSH V2 Hello Timeout	Enter the handshake timeout (in seconds). Default value: 30
SSH V2 Key Exchange Timeout	Enter the total number of seconds SiteScope should wait for SSH key exchange. Default value: 30
SSH V2 Authentication Phase Timeout	Enter the total number of seconds SiteScope should wait for SSH authentication. Default value: 60

Dashboard Monitor History View Options

Description	You configure Monitor History to view monitor history on all monitors and monitor groups. To access: Expand Preferences in the monitor tree and click General Preferences . Click Dashboard Monitor History View Options .
Important Information	In the Dashboard layout, you can then use a filter to further limit the monitors displayed to those that meet selected criteria. Your preferences are saved with the Dashboard filter settings. For details, see “Dashboard Filter Overview” on page 415.
Useful Links	“Customize SiteScope Dashboard” on page 419

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Enable Monitor History View	Select to enable or disable Monitor History. Default value: Disabled
Display Time Period	Select the time frame for displaying past runs.
Monitor Run Status	Select the required run status.
Maximum Number of Runs to Display	Enter the number of rows of data to keep in memory.

JDBC Global Options

Description	<p>Use to apply global JDBC options to the following resources that connect to the database:</p> <ul style="list-style-type: none"> ▶ SiteScope database logger ▶ Database tools (Database Connection, Database Information) ▶ Database alerts ▶ Database monitors (Oracle database, Database Counter, Database Query, DB2 8.x, Technology Database Integration) <p>To access: Expand Preferences in the monitor tree and click General Preferences. Click JDBC Global Options.</p>
Useful Links	“General Preferences” on page 211

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Connection Timeout	<p>The amount of time, in seconds/minutes/hours/days, to wait for a new SQL connection to be made. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored.</p> <p>Default value: 1 minute</p>
Driver Trace Log File	<p>Used to create a driver trace log file for troubleshooting database drivers. This box is empty by default, and it is recommended that you use it only for troubleshooting.</p> <p>To create the log file, enter the full path or UNC name of the driver trace file (for example, e:\mydir\myfile.log).</p> <p>Note: The target log file can contain login information, table names and queries.</p>

Infrastructure Settings Preferences User Interface

Description	Enables you to define the values of settings that determine how SiteScope runs. To access: Expand Preferences in the monitor tree and click Infrastructure Settings Preferences .
Important Information	<ul style="list-style-type: none"> ▶ Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences and restart SiteScope from Infrastructure Settings Preferences. ▶ Some settings are displayed without user-friendly text labels, and are listed only by their corresponding property name from the master.config file.
Useful Links	“Infrastructure Settings Preferences” on page 216

The Infrastructure Settings Preferences includes the following elements:

General Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
NT SSH Timeout	The number of seconds to wait for an SSH connection to remote Windows servers before timing out. Default value: No value Property name: _NTSSHTimeout
Allow Unix to NT	Allows using remote Windows servers if SiteScope is running on UNIX. Note: You must restart SiteScope if you change this setting. Property name: _allowUnixToNT

GUI Element	Description
Recursive 'depends on'	<p>Allows recursion in the monitor Depends On box. This means that subgroups become disabled when the parent group is disabled because of a dependency. By default, only the immediate group impacted by the dependency is disabled.</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_dependsOnRecursive</code></p>
Disable quotes for cmd.exe	<p>Avoids wrapping parameters in quotes when running cmd.exe for various tasks.</p> <p>Property name: <code>_disableDoubleQuotesInTemplates</code></p>
Disable host DNS resolution	<p>Disables DNS resolution for host names and IPs sent to BAC through SiteScope and EMS topology channel. Should be used only if all host names extracted from EMS events are irresolvable on the SiteScope-side.</p> <p>Property name: <code>_disableHostDNSResolution</code></p>
DNS name tags	<p>A comma-separated list of values considered by DNS-related functionality as the DNS "name" tag.</p> <p>Property name: <code>_dnsNameTags</code></p>
DNS server tags	<p>A comma-separated list of values considered by DNS-related functionality as the DNS "server" tag.</p> <p>Property name: <code>_dnsServerTags</code></p>
Perfex timeout	<p>The number of seconds for perfex to attempt to make a connection or to attempt to run a monitor before timing out.</p> <p>Default value: 120</p> <p>Property name: <code>_perfexTimeout</code></p>

GUI Element	Description
Process pool kill timeout	<p>The number of milliseconds to wait before SiteScope kills a non-responsive process. This is to avoid killing processes on every timeout.</p> <p>Default value: 60000</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_processPoolKillTimeout</code></p>
Maximum processes per pool	<p>The maximum number of processes allowed per process pool.</p> <p>Default value: 200</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_processPoolMaxPerPool</code></p>
Accept untrusted SSL certificates	<p>Allows SiteScope to accept any untrusted certificate when SSL is used. Otherwise, only certificates specified in the keystore file or that have a trust chain leading to a registered CA certificate are accepted.</p> <p>Property name: <code>_sslAcceptAllUntrustedCerts</code></p>
Maximum idle threads per pool	<p>The maximum number of idle threads allowed per thread pool.</p> <p>Default value: 100</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_threadPoolMaxIdle</code></p>
Time zone offset	<p>Manually sets the time zone offset, in hours, from Greenwich Mean Time (GMT). You can enter both positive and negative, integer and non-integer values.</p> <p>Default value: -999 (no offset)</p> <p>Example: In Eastern US (EST), the time zone offset is GMT -5.</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_timeZoneOffset</code></p>

GUI Element	Description
Traceroute command	<p>(For Unix) Specify the path to the traceroute command to override the default for the platform.</p> <p>Default value: No value</p> <p>Property name: <code>_tracerouteCommand</code></p>
Number of open port tries	<p>The maximum number of attempts to open a reserved port in the 811-1024 range for rlogin and rsh remote access methods.</p> <p>Default value: 25</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_localPortRetryCount</code></p>
E-mail character set	<p>The character set for the E-mail alert.</p> <p>Property name: <code>_mailCharSet</code></p>
E-mail subject character set	<p>The e-mail subject character set for the E-mail alert.</p> <p>Property name: <code>_mailSubjectCharSet</code></p>
Monitor delay between refresh	<p>The amount of time, in milliseconds, to wait before running a monitor after it has already been run since startup.</p> <p>Default value: 1000</p> <p>Property name: <code>_monitorDelayBetweenRefresh</code></p>
SiteScope sleep delay	<p>The amount of time, in milliseconds, of the sleep interval in the main thread.</p> <p>Default value: 180</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_monitorProcessCheckDelay</code></p>
Don't check default thresholds	<p>SiteScope checks monitor results against user selected thresholds only and not against the default SiteScope monitor thresholds.</p> <p>Property name: <code>_noCheckDefaultThresholds</code></p>

GUI Element	Description
Numeric values format	<p>The format of numeric values when converting to string representation.</p> <p>Default value: #.##</p> <p>Property name: _noScientificNotation</p> <p>Tip: For more detailed information on numeric values format, refer to the HP Software Self-solve knowledge base (http://h20230.www2.hp.com/selfsolve/document/KM305059). To enter the knowledge base, you must log in with your HP Passport ID.</p>
Log only enabled monitors	<p>SiteScope does not log runs for disabled monitors in the daily log files.</p> <p>Property name: _onlyLogEnabledMonitors</p>
Sleep interval on error	<p>The amount of time, in milliseconds, to wait before rerunning a monitor using the Verify Error option.</p> <p>Default value: 5000</p> <p>Property name: _verifySleepDuration</p>
Auto Deployment Check Frequency	<p>The time interval in seconds that the auto template deployment xml files in the persistency\autodeployment directory are deployed. For details on the feature, see “Auto Template Deployment” on page 1253.</p> <p>Default value: 120</p> <p>Property name: _autoDeploymentCheckFrequency</p>

Server Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Kill processes	Allows SiteScope to kill its child processes when the SiteScope process is stopped. Property name: <code>_killProcesses</code>
Shutdown on monitor skips	SiteScope shuts down with an error if a monitor exceeds its maximum allowed skip count. Property name: <code>_shutdownOnSkips</code>
Host name override	Allows overriding of the SiteScope host name for Business Availability Center. Default value: Not selected Property name: <code>_sisHostNameOverride</code>
Startup script	Runs this script whenever SiteScope starts up, regardless of the platform or procedure used to start SiteScope. (Empty=none) Default value: No value Property name: <code>_startupScript</code>
Maximum monitor processes	The maximum number of monitor processes in the process pool. Default value: 100 Note: You must restart SiteScope if you change this setting. Property name: <code>_maxMonitorProcesses</code>
Maximum monitor running	The maximum number of running monitor processes in the queue. Default value: 400 Note: You must restart SiteScope if you change this setting. Property name: <code>_maxMonitorsRunning</code>

GUI Element	Description
Maximum monitor skips	<p>The maximum number of consecutive monitor skips allowed before a monitor is disabled or SiteScope is shut down.</p> <p>Default value: 10</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_maxMonitorSkips</code></p>
SiteScope shutdown timeout	<p>The amount of time, in seconds, that SiteScope should wait to shutdown before timing out.</p> <p>Default value: 60</p> <p>Property name: <code>_shutdownTimeout</code></p>

Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
MS Media Player 9 account blocked	<p>Select this option and add the account directory path to the MS Media Player 9 account directory box if your Media Player account stops working with a 17999 error.</p> <p>Property name: <code>_MediaPlayer9AccountBlocked</code></p>
MS Media Player 9 account directory	<p>Enter the Media Player account directory if you get a 17999 error for the Media Player monitor.</p> <p>Default value: No value</p> <p>Example: <code>C:\Documents and Settings\<user>\Local Settings\Application Data\Microsoft\Windows Media\9.0</user></code></p> <p>Property name: <code>_MediaPlayer9AccountBlockedDir</code></p>
Maximum NT Counter monitor counters	<p>The maximum number of counters allowed for each instance of a Microsoft Windows Performance Counter monitor.</p> <p>Default value: 8</p> <p>Property name: <code>_NTCounterMonitorMaxCounters</code></p>

GUI Element	Description
Keep Astra log files	Allows the Astra monitor to keep Astra log files. Property name: <code>_astraKeepLogFiles</code>
Maximum BMC counters	The maximum number of BMC Patrol counters the monitor is allowed to retrieve. Default value: 50 Property name: <code>_browsableBMCCContentMaxCounters</code>
Browsable EXE timeout	The maximum amount of time, in milliseconds, to wait for retrieving counter information and for running the monitor. This setting only applies to executable-based browsable monitors, such as SAP, Sybase, and DB2 monitors. Default value: 45000 Property name: <code>_browsableExeTimeout</code>
CPU error at 100%	The CPU monitor switches to the default error status when CPU utilization reaches 100% on the target machine. Property name: <code>_cpuEnableErrorAt100</code>
CPU maximum units	The maximum number of CPU units supported by the CPU monitor. Default value: 16 Property name: <code>_cpuMaxProcessors</code>
DB maximum columns	The maximum number of columns processed by DB monitors. Default value: 10 Property name: <code>_databaseMaxColumns</code>
DB maximum rows	The maximum number of rows processed by DB monitors. Default value: 1 Property name: <code>_databaseMaxRows</code>

GUI Element	Description
DB maximum value length	<p>The maximum length, in characters, of the data processed by DB monitors.</p> <p>Default value: 200</p> <p>Property name: <code>_databaseMaxSummary</code></p>
Default precision	<p>The default precision for floating-point values processed by some monitors.</p> <p>Default value: 0 (disabled)</p> <p>Property name: <code>_defaultPrecision</code></p>
Dialup options	<p>Options for dialup.exe when running it from the Microsoft Windows Dial-up monitor. Set to <code>-silent</code> to have the modem dial silently. Set to <code>-debug</code> to enable dialup debugging.</p> <p>Default value: No value</p> <p>Property name: <code>_dialupOptions</code></p>
Empty last line reading	<p>Includes the last empty line in the Script monitor output.</p> <p>Property name: <code>_enable_script_monitor_non_empty_last_line_reading</code></p>
Event log messages to save	<p>The number of Microsoft Windows Event Log descriptions to save when saving diagnostic text for alerts.</p> <p>Default value: 10</p> <p>Property name: <code>_eventLogMessagesToSave</code></p>
Exclusive monitor timeout	<p>The maximum amount of time, in seconds, that exclusive monitors must wait for other monitors to finish before running. The only monitor affected by this is the Microsoft Windows Dial-up monitor.</p> <p>Default value: 120</p> <p>Property name: <code>_exclusiveMonitorTimeout</code></p>
FTP content match maximum size	<p>The maximum size of the buffer used to match FTP content.</p> <p>Default value: 50000</p> <p>Property name: <code>_ftpContentMatchMax</code></p>

GUI Element	Description
FTP download limit	<p>The maximum number of bytes downloaded from each file to match.</p> <p>Default value: -1 (no limit)</p> <p>Property name: <code>_ftpDownloadLimit</code></p>
FTP max threads	<p>The maximum number of simultaneous FTP worker threads allowed.</p> <p>Default value: 1</p> <p>Property name: <code>_ftpMaxThreads</code></p>
Initial monitor delay	<p>The time, in seconds, over which to randomly schedule monitor updates after a SiteScope restart.</p> <p>When changing a monitor's frequency so that its next run occurs immediately (for example, if a monitor has not run in 5 minutes, and you change the frequency to less than 5 minutes), SiteScope randomly schedules the next run during the specified period.</p> <p>Default value: 600</p> <p>Property name: <code>_initialMonitorDelay</code></p>
WebService monitor: maximum read length	<p>The maximum amount of data, in bytes, to read from the log file for the Web Server monitor.</p> <p>Default value: 50000</p> <p>Property name: <code>_maxAmountToRead</code></p>
Network Bandwidth monitor sanity check	<p>Performs a sanity check on the Network Bandwidth monitor.</p> <p>Property name: <code>_performNetworkBandwidthSanityCheck</code></p>
SNMP Trap encoding	<p>SNMP Trap encoding for the SNMP Trap monitor. Empty=ISO8859-1.</p> <p>Default value: ISO8859-1</p> <p>Property name: <code>_snmpTrapEncoding</code></p>

GUI Element	Description
HTTP content match display limit	<p>The maximum number of bytes to display for URL monitor content match.</p> <p>Default value: 150</p> <p>Property name: <code>_urlContentMatchDisplayMax</code></p>
HTTP content match limit	<p>The maximum number of bytes to check for URL monitor content match.</p> <p>Default value: 50000</p> <p>Property name: <code>_urlContentMatchMax</code></p>
SNMP Trap monitor log limit	<p>The maximum number of lines to look through SNMP Trap log for the SNMP Trap monitor. This box is filled only if Run Alerts is set to Once, after all SNMP Traps have been checked in the SNMP Trap monitor page.</p> <p>Note: Setting a high limit may increase the size of the <code>SiteScope.log</code> or <code>RunMonitor.log</code>.</p> <p>Default value: 1000</p> <p>Property name: <code>_SNMPTrapMonitorDetailsMax</code></p>
Maximum browsable counters to be selected	<p>The maximum number of browsable counters that can be selected from the browsable tree.</p> <p>Default value: 100</p> <p>Property name: <code>_browsableContentMaxCounters</code></p>
Enable JDBC logging	<p>Enables JDBC search results logging for the Link Check monitor.</p> <p>Property name: <code>_linkMonitorJdbcEnabled</code></p>
Error tokens for Script monitor	<p>List of keywords that should be handled as signs of failure during server output parsing.</p> <p>Default value: not found, Not Found, denied, Denied, cannot execute such file or directory</p> <p>Property name: <code>_scriptMonitorErrorMsgs</code></p>

GUI Element	Description
Additional list of keywords	<p>Additional list of keywords that should be handled as signs of failure during server output parsing.</p> <p>Default value: Failed to .* Error code:</p> <p>Property name: _scriptMonitorErrorMsgs2</p>
Script monitor output limit	<p>The number of lines to save from Script output after launching the Script monitor.</p> <p>Default value: 25</p> <p>Property name: _scriptMonitorLinesToSave</p>
Script monitor replacement strings	<p>Stores a list of space-separated strings which are parameter tags in the remote script. When the Script monitor is run, it replaces parameters tags from the script command with actual parameter values from monitor preferences.</p> <p>Default value: \$ %</p> <p>Property name: _scriptMonitorReplacementChars</p> <p>Example: If the script command is test \$ %, replacement chars are \$ %, and parameters are Param1 Param2, the the monitor runs the following command: test Param1 Param2.</p>
Run script through perfex tool	<p>Runs the script through the perfex tool.</p> <p>Property name: _scriptRunThroughPerfex</p>
SNMP monitors maximum number	<p>The maximum number of SNMP monitors that can run at any given time.</p> <p>Default value: 10</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: _snmpMonitorMaximum</p>
Mail Attachment Content Support Base64	<p>Supports mail attachment content-transfer-encoding with base64 for the Mail monitor.</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: _mailAttachmentBase64Support</p>

Alert Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Maximum sound alert length	The maximum length of time, in milliseconds, of the Sound Alert sound. Default value: No value Property name: <code>_AudioSleepTime</code>
Pager delay	The delay between pager signals when using a Pager Alert. Default value: 5 Property name: <code>_delayBetweenPages</code>
Maximum script alert processes	The maximum number of Script Alert processes that are allowed to run simultaneously. Default value: 25 Property name: <code>_maxScriptAlertProcesses</code>
Alert attempt delay	The number of seconds to wait between each attempt to send a Post Alert. Default value: 120 Property name: <code>_postAttemptDelay</code>
Maximum runs for Post action	The maximum number of attempts to send a Post Alert. Default value: 4 Property name: <code>_postAttempts</code>

GUI Element	Description
Maximum alert threads	The maximum number of alert threads in the pool. Default value: 100 Property name: <code>_threadPoolAlertMaxThreads</code>
Simultaneously running DNS monitors	The maximum number of DNS monitors that can run simultaneously. This is relevant only when using the roundTripTime counter. The NSLookup operation can load the operating system and affect the values. Default value: 0 (0 means that the number of simultaneous DNS monitors is unlimited) Note: You must restart SiteScope if you change this setting. Property name: <code>_maxDnsMonitorsRunning</code>

Persistency Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Maximum persistence history size	The maximum size of persistence history in bytes. Default value: 20000 Note: You must restart SiteScope if you change this setting. Property name: <code>_PersistencyMaxHistorySize</code>
Maximum persistence history items	The maximum number of history items kept in persistence. Default value: 1000 Property name: <code>_PersistencyMaxHistoryItems</code>

GUI Element	Description
<p>Maximum changes per persistency delta file</p>	<p>The maximum number of persistency changes kept in each persistency delta file.</p> <p>Default value: 51</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: _PersistencyMaxChangesInDeltaFile</p>
<p>Maximum temp directory size</p>	<p>The maximum size, in kilobytes, of the temp directory.</p> <p>Default value: 10000</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: _tempDirMaxSize</p>

Classic UI Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
No "change password" link	Disables the Change Password link on the login page of the SiteScope Classic user interface. Property name: <code>_disableLoginChangePassword</code>
Disable the Classic UI	Disables the SiteScope Classic user interface. Note: You must restart SiteScope if you change this setting. Property name: <code>_disableOldUI</code>
Group page refresh rate	The number of seconds before refreshing a group page in the SiteScope Classic user interface. Default value: 60 Property name: <code>_groupRefreshRate</code>
Lock web server address	SiteScope does not map the Web server address to available IP addresses. SiteScope locks the Web server address entry on the Preferences page in the SiteScope Classic user interface from reverting to "localhost" after it is changed to an IP address or computer name. Property name: <code>_lockWebserverAddress</code>
Progress Page refresh rate	The number of seconds before refreshing the Progress page in the SiteScope Classic user interface. Default value: 20 Property name: <code>_progressRefreshRate</code>

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Include alert.log.old into report	Includes the alert.log.old file in the Alert Report. Property name: <code>_includeAlertLogOld</code>
Maximum errors in the History report	The maximum number of errors shown in the monitor history report. Default value: 100 Property name: <code>_maxReportErrors</code>
Maximum warnings in the History report	The maximum number of warnings shown in the monitor history report. Default value: 100 Property name: <code>_maxReportWarnings</code>

Baseline Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Activation thread priority	<p>The priority assigned to the activation thread. The priority, if specified, must be between 1-10 inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baselines are activated. It is recommended to keep priority as low as possible, so as not to interfere with SiteScope online functionality.</p> <p>Default value: 1 (low priority)</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_baseliningActivationThreadPriority</code></p>
Calculation thread priority	<p>The priority assigned to the calculation thread. The priority, if specified, must be between 1-10 inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baselining calculations take to complete. It is recommended to keep priority as low as possible, so as not to interfere with SiteScope online functionality.</p> <p>Default value: 1 (low priority)</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_baseliningCalculationThreadPriority</code></p>

GUI Element	Description
Parsing thread priority	<p>The priority assigned to the parsing thread. The priority, if specified, must be between 1-10 inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baselining calculations take to complete. It is recommended to keep priority as low as possible, so as not to interfere with SiteScope online functionality.</p> <p>Default value: 1 (low priority)</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_baseliningParsingThreadPriority</code></p>
Failed parsings handler thread priority	<p>The priority assigned to the failed parsing thread handler. The priority, if specified, must be between 1-10 inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baselining calculations take to complete. It is recommended to keep priority as low as possible, so as not to interfere with SiteScope online functionality.</p> <p>Default value: 1 (low priority)</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_baseliningFailedParsingHandlerThreadPriority</code></p>
Number of days to include in calculation	<p>The number of days of historical data that are included in baselining calculations. The higher the number, the more precise the baselining result, but the calculation takes more time and uses more disk space. Data that is older than this value is not included in the calculation. For more details on the calculation model, see “How SiteScope Calculates Thresholds” on page 486.</p> <p>Default value: 30</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_baseliningDaysToIncludeInCalculation</code></p>

GUI Element	Description
Include today's data in calculation	<p>Specifies whether to include the current day's data in the baseline calculation.</p> <p>Default value: Selected</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_baseliningCalculationIncludesToday</code></p>
Parsing chunk size	<p>Specifies the number of monitors that are handled simultaneously by the log file parser. The higher the number, the faster the baselining calculation, but more file handlers are used.</p> <p>Default value: 100</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_baseliningParsingChunkSize</code></p>
Offset for calculating Error Boundary	<p>Specifies the offset value to use for calculating the error boundary. The baseline threshold is multiplied by this value when:</p> <ul style="list-style-type: none"> ▶ The Automatically create Error Threshold Boundary if no error thresholds are defined option is selected (see below), or ▶ The current most extreme error threshold is less extreme than the calculated baseline threshold. <p>Default value: 0.3</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_baseliningUpperBoundOffset</code></p>

GUI Element	Description
Automatically create an Error Boundary if no error thresholds are defined	<p>Automatically creates a baseline threshold using the error boundary offset value when no error thresholds have been defined for a monitor.</p> <p>Default value: Selected</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: _baseliningAutomateUpperBoundCreation</p>
Maximum number of percentile ranges	<p>Limits the number of percentile ranges displayed in the Percentile Ranges Mapping Table.</p> <p>Default value: 8</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: _baseliningMaxNumberOfPercentilesRanges</p>
Percentile of discarded samples	<p>The percentile of the most extreme samples (considered "noise" measurement samples) that are not included in the baseline calculation.</p> <p>Default value: 2.0</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: _baseliningNoiseMarginPercentile</p>
Minimum number of samples required for baselining	<p>The minimum number of samples required for SiteScope to calculate the baseline.</p> <p>Default value: 2016 (the number of samples produced for a monitor running over a two week period, where the monitor runs every 10 minutes)</p> <p>Minimum value: 1 (if you enter a value of less than 1, the default value is used instead).</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: _baseliningMinimumNumberOfSamples</p>

GUI Element	Description
<p>Minimum number of days required for baselining</p>	<p>The minimum number of days that the monitors must have run for SiteScope to calculate the baseline.</p> <p>Default value: 14</p> <p>Minimum value: 1 (if you enter a value of less than 1, the default value is used instead).</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_baseliningMinimumNumberOfDays</code></p>
<p>Interval for saving accumulated baseline data to disk</p>	<p>The interval, in minutes, used by SiteScope to save baseline data accumulated in the memory to the disk. A shorter interval reduces the memory consumption, but increases the vulnerability to failures and reduces performance.</p> <p>Default value: 5</p> <p>Note: You must restart SiteScope if you change this setting.</p> <p>Property name: <code>_baseliningSaveAccumulatedDataIntervalMinutes</code></p>

Integration Preferences User Interface

Description	<p>Use to configure SiteScope as a data collector for HP Business Availability Center. If SiteScope has been configured as a data collector for HP Operations Manager, you can also view and modify some of the integration settings.</p> <p>To access: Expand Preferences in the monitor tree and click Integration Preferences.</p>
Important Information	<p>Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences.</p>
Included in Tasks	<p>“Configure SiteScope-HP Business Availability Center Integration Preferences” on page 234</p>
Useful Links	<p>“Integration Preferences” on page 216</p> <p>“Troubleshooting and Limitations” on page 334</p>

The Integration Preferences include the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Business Availability Center/Operations Manager machine name/IP address	Enter the machine name or IP address of the Business Availability Center server to which you want this SiteScope to connect. If SiteScope has been configured as a data collector for HP Operations Manager, displays the name or IP address of the Operations Manager server to which SiteScope connects. Note: This is a required field.
SiteScope agent machine location (BAC integration only)	Enter the location of the SiteScope server that you are connecting to Business Availability Center. You can specify any value that helps you identify the location of this specific SiteScope server. Note: This is a required field.
Business Availability Center/Operations Manager user name	Enter the username of a Business Availability Center/Operations Manager administrator-level user.
Business Availability Center/Operations Manager user password	Enter the password for the specified user.
Disable all logging to Business Availability Center (BAC integration only)	Select to stop SiteScope from sending data to Business Availability Center. This also disables all topology reporting. Clear the check box to enable logging again.

Web Server Security Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Authentication username	If the Business Availability Center/Operations Manager server is configured to use basic authentication, enter the username to access the server.
Authentication password	If the Business Availability Center/Operations Manager server is configured to use basic authentication, enter the password to access the server.
Use SSL (HTTPS protocol)	Select this option if the Business Availability Center/Operations Manager server is configured to use the HTTPS protocol.

Proxy Server Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Address	Enter the proxy server address if applicable.
Username	Enter the username for the proxy server.
Password	Enter the password for the specified server.

Topology Reporting Settings (BAC Integration only)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Topology resynchronization time interval	<p>The number of days for SiteScope to synchronize topology data with Business Availability Center.</p> <p>The topology information SiteScope reports to Business Availability Center is synchronized when SiteScope restarts after this time interval has been reached. SiteScope restarts by default every 24 hours.</p> <p>Default value: 7 (days)</p> <p>Note: All topologies created by SiteScope and stored in CMDB are subjected to the aging process. To prevent aging, see “Aging of CIs in CMDB” on page 48.</p>
Default topology probe domain	<p>Enter the default domain of the SiteScope topology probe.</p> <p>Note: You must restart SiteScope if you change this setting.</p>
Topology receiver port	<p>Enter the topology receiver port used in Business Availability Center.</p> <p>Default value: 8080</p> <p>Note: You must restart SiteScope if you change this setting.</p>
Topology receiver SSL port	<p>Enter the topology receiver SSL port used in Business Availability Center.</p> <p>Default value: 443</p> <p>Note: You must restart SiteScope if you change this setting.</p>

BAC/OM Preferences Available Operations

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Re-synchronize (BAC integration only)	Forces SiteScope to resend all its configuration data to Business Availability Center. This data consists of all the group and monitor definitions. Re-synchronize also forces SiteScope to resend all topology data to Business Availability Center.
Hard Re-synchronize (BAC integration only)	Forces SiteScope to resend all its configuration data and topology data to Business Availability Center. For configuration data, it also deletes the existing monitor and group data from Business Availability Center for this SiteScope profile.
Reset	<p>This deletes all the Business Availability Center/Operations Manager-related settings from the SiteScope server and all SiteScope configurations are deleted from Business Availability Center/Operations Manager. This also sends a message to the applicable Business Availability Center/Operations Manager server to release the SiteScope agent from the corresponding profile.</p> <p>Note: If you choose to reset the current settings, you have to create or use a different profile to reconnect SiteScope with Business Availability Center/Operations Manager. Business Availability Center/Operations Manager does not enable you to select a previously used connection profile.</p>

Failover Preferences User Interface

Description	<p>SiteScope Failover is a special version of SiteScope that includes automated mirroring and failover functionality. It enables you to implement failover capability for infrastructure monitoring by provisioning for backups, redundant, and failover mechanisms. Use the Failover Preferences to indicate a primary SiteScope to be mirrored and set how often the configurations should be mirrored to the failover SiteScope installation.</p> <p>To access: Expand Preferences in the monitor tree and click Failover Preferences.</p>
Important Information	<ul style="list-style-type: none"> ▶ Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences. ▶ The Failover Preferences are available only to users accessing SiteScope High Availability that have a SiteScope Failover License. ▶ SiteScope Failover restarts itself after each mirroring operation.
Useful Links	“Failover Preferences” on page 219

The Failover Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Host	Enter the name or IP address of the server that you want this SiteScope Failover server to mirror configurations from.
Port	Enter the SiteScope port of the server that you want this SiteScope Failover server to mirror configurations from (for example, 8888).

GUI Element	Description
Use SSL	When this box is checked, the mirror server contacts the primary SiteScope server by using HTTPS.
Admin login	The login name used to access the administrator login account for the primary SiteScope instance. If no administrator login has been configured on the target machine, leave this box blank.
Admin password	The password used to access the administrator login account for the primary SiteScope instance. If no SiteScope administrator login has been configured on the primary SiteScope, leave this box blank.
Mirror every (hours)	The schedule for synchronizing (mirroring) configuration data to the failover SiteScope from the primary SiteScope. This is used to make sure that the SiteScope Failover configuration reflects updates and changes to the monitoring configuration on the primary SiteScope server. Values for this box should be between 1 to 23 hours. Enter values as whole numbers. Default value: 4 hours
Last mirror time	The time and date of the most recent mirroring operation.
Next scheduled mirror time	The time and date of the next scheduled mirroring operation.
Mirror Configuration Now	Click to mirror the primary SiteScope configuration data now.

Microsoft Windows Remote Preferences User Interface

Description	<p>SiteScope on Windows can monitor systems and services running on remote Windows servers for a large number of statistics without the installation of agent software on each server. This includes monitoring server resources such as CPU, Disk Space, Memory, and Windows-specific performance counter data. Select the servers to display when configuring monitors. SiteScope creates a new remote connection profile for each server address in the list.</p> <p>To access: Expand Preferences in the monitor tree and click Microsoft Windows Remote Preferences.</p>
Important Information	<ul style="list-style-type: none"> ▶ Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences. ▶ When configuring particular monitor types, you can display only those servers that have been configured in Remote Preferences by selecting the Display only configured servers option. ▶ You cannot delete a remote server from the list of Microsoft Windows Remote Preferences servers if the server is referenced by a monitor. Select a different server in the Servers box of the Main Settings for each monitor that references the remote server, and then delete the remote server from the preferences list.
Included in Tasks	<p>“Configure SiteScope to Monitor a Remote Windows Server” on page 236</p>
Useful Links	<p>“Microsoft Windows Remote Preferences” on page 219</p> <p>“Troubleshooting and Limitations” on page 334</p>

The Microsoft Windows Remote Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Host	<p>Enter the real IP address or UNC name of the monitored Windows server (virtual IP addresses are not supported). An IP host name also works if the SiteScope server is able to translate this common name into an IP address by using a hosts file, DNS, or WINS/DNS integration.</p> <p>To use the same login credentials to configure multiple servers at the same time, enter the server names or addresses separated by a comma (","), semi-colon (";"), or a space.</p> <p>Example: If using NetBIOS to connect to other servers in an NT domain, enter a comma-separated string of server addresses such as: \\server1,\\server2,\\server3,\\server4.</p> <p>Note: In the list of Microsoft Windows Remote Preferences servers, use the Test button to test connectivity after the profiles have been added. Alternatively, right-click the profile in the monitor tree, and click Test.</p>
Credentials	<p>To have SiteScope automatically supply the login and password for the remote Windows host, select a credential profile from the list of Credential Preferences. If you are creating a new template remote, you must enter the name of the credential profile.</p> <p>Note: If you select or enter a credential profile, you do not need to enter a login and password. A credential profile takes priority over login and password entries.</p>

GUI Element	Description
Login	<p>Enter the login for the remote server. If the server is within the same domain as the SiteScope machine, include the domain name in front of the user login name. For example: <DOMAIN>\<username>. If using a local machine login account for machines within or outside the domain, include the machine name in front of the user login name. For example: <machinename>\<username>.</p> <p>Note: If a credential profile is selected in the Credentials box, the credential profile login is used instead of the login in this box.</p>
Password	<p>Enter the password for the remote server or the passphrase for the SSH key file. When using SSH authentication with public/private key based authentication, enter the passphrase for the identity file here.</p> <p>Note: If a credential profile is selected in the Credentials box, the credential profile password is used instead of the password in this box.</p>
Name	<p>Enter a name by which to identify this remote machine. This name appears in the Server list of monitors that can use this connection profile.</p>
Trace	<p>Select to trace messages to and from the subject server, recorded to the SiteScope RunMonitor.log file.</p>

GUI Element	Description
Method	<p>SiteScope uses one of two connection types for monitoring Windows server resources. From the drop-down list select:</p> <ul style="list-style-type: none"> ▶ NetBIOS. The default server-to-server communication protocol for Microsoft Windows NT and 2000 networks. ▶ SSH. Secure Shell, a more secured communication protocol that can be installed on Microsoft Windows NT/2000 based networks. This connection method normally requires installing SSH libraries on each server to be connected. For more information see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1541.
Remote Machine Encoding	<p>Enter the encoding for the remote server, if the remote server is running an operating system version that uses a different character encoding than the server on which SiteScope is running. This enables SiteScope to display encoded content correctly.</p> <p>Default value: Cp1252 encoding</p> <p>Other encodings: Cp1251, Cp1256, Shift_JIS, EUC_JP</p>

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
SSH Connection Method	<p>Select the client to use for this connection from the list. The currently supported clients are:</p> <ul style="list-style-type: none"> ▶ Internal Java Libraries. Connect using the Java SSH client integrated with SiteScope. ▶ Plink/External SSH. Connect using an external SSH client. On Windows, SiteScope includes Plink.
SSH Port Number	<p>Enter the port on which the remote SSH server is listening.</p>

GUI Element	Description
Disable Connection Caching	Select to turn off connection caching for this remote. By default, SiteScope caches open connections.
Connection Limit	<p>Enter the number of open connections that SiteScope allows for this remote. If there are many monitors configured to use this connection, set the number of open connections high enough to relieve a potential bottleneck.</p> <p>Note: This setting does not effect running tests for a remote server. Tests always create a new connection.</p>
SSH Authentication Method	<p>Select the authentication method to use for SSH connections from the drop-down list. The currently supported methods are:</p> <ul style="list-style-type: none"> ▶ Password. Authenticate using a password. ▶ Key File. Authenticate using public/private key authentication. When this option is selected SiteScope uses the private key in the file <code><SiteScope root directory>\groups\identity</code> to authenticate. The corresponding public key must be listed in the <code>authorized_keys</code> file on the remote host. For information about SSH requirements, see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1541.
Key File for SSH connections	<p>Select the file that contains the private key for this connection. The default key file is <code><SiteScope root directory>\groups\identity</code>. This setting applies only when the authentication method is Key File.</p>
SSH Version 2 Only	<p>Check this option to force SiteScope to use SSH protocol version 2 only. This option applies only when using the integrated Java Client. For information about configuring an external SSH client to use SSH2 protocol, see “External SSH Client Overview” on page 1566.</p>
SSH Keep Alive Mechanism	<p>Check this option to engage a keep alive mechanism for SSH version 2 sessions. This option applies only when using the integrated Java Client.</p>

GUI Element	Description
Custom Commandline	<p>Enter a custom command line for a remote server using the External Client. Use this option when passing specific commands to the external client to run. Valid substitution variable are:</p> <ul style="list-style-type: none"> ➤ \$user\$. This translates the username entered into the remote server. ➤ \$password\$. This translates the password entered into the remote server. ➤ \$host\$. This translates the host name entered into the remote server.
Description	<p>Add a text description for the remote Windows server. This text appears only when editing the remote's properties. You can include HTML tags such as the
, <HR>, and tags to control display format and style.</p> <p>Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> ➤ Tags: script, object, param, frame, iframe. ➤ Any tag that contains an attribute starting with on is declined. For example, onhover. ➤ Any attribute with javascript as its value.

Category Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Assigned categories	<p>Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see "Create and Define a New Category" on page 198.</p>

UNIX Remote Preferences User Interface

Description	<p>SiteScope can monitor systems and services running on remote UNIX servers for certain statistics (such as CPU, Disk Space, Memory, and Processes) without the installation of agent software on each server. Select the servers to display when configuring UNIX monitors. SiteScope creates a new remote connection profile for each server address in the list.</p> <p>To access: Expand Preferences in the monitor tree and click UNIX Remote Preferences.</p>
Important Information	<ul style="list-style-type: none"> ▶ Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences. ▶ You cannot delete a remote server from the list of UNIX Remote Preferences servers if the server is referenced by a monitor. Select a different server in the Servers box of the Main Settings for each monitor that references the remote server, and then delete the remote server from the preferences list.
Useful Links	<p>“UNIX Remote Preferences” on page 220</p>

The UNIX Remote Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Host	<p>Enter the real IP address or host name of the monitored server (virtual IP addresses are not supported). If using the HTTP method of monitoring, enter the full URL of the CGI script (for example: <code>http://demo.thiscompany.com/cgi-bin/run.sh</code>). To use the same login credentials to configure multiple servers at the same time, enter the server names or addresses separated by a comma (","), semi-colon (";"), or a space.</p> <p>Example: If using NetBIOS to connect to other servers, enter a comma-separated string of server addresses such as: <code>serveraddress1,serveraddress2,serveraddress3,serveraddress4</code></p> <p>When completing the other required entries on the form, SiteScope creates a new remote connection profile for each server address in the list.</p> <p>Note: To test connectivity after the host is added, click Test in the table listing the UNIX Servers. This tests only the connection to the server. Click Detailed Test to run a test that displays the result of running commands on the remote host. This enables checking the permissions for the defined user.</p>
Credentials	<p>To have SiteScope automatically supply the login and password for the remote UNIX host, select a credential profile from the list of Credential Preferences. If you are creating a new template UNIX remote, you must enter the name of the credential profile.</p> <p>Note: If you select or enter a credential profile, you do not need to enter a login and password. A credential profile takes priority over login and password entries.</p>

GUI Element	Description
Login	<p>Enter the login for the remote server.</p> <p>Note: If a credential profile is selected in the Credentials box, the credential profile login is used instead of the login in this box.</p>
Password	<p>Enter the password for the remote server or the passphrase for the SSH key file. When using SSH authentication with public/private key based authentication, enter the passphrase for the identity file.</p> <p>Note: If a credential profile is selected in the Credentials box, the credential profile password is used instead of the password in this box.</p>
Name	<p>Enter a name by which the remote machine should be known in SiteScope. This name appears in the list of the servers for monitors that can connect to remote servers.</p>
Trace	<p>Select to trace messages to and from the remote server in the RunMonitor.log file.</p>
OS	<p>The operating system that is running on a remote server. This is required so that the correct information can be obtained from that server. Select an operating system from the list.</p> <p>For servers running versions of UNIX which are not included in the list, see “UNIX Operating System Adapters” on page 1529.</p>

GUI Element	Description
Method	<p>The currently supported methods are:</p> <ul style="list-style-type: none"> ▶ HTTP. Connect to an HTTP server on the remote server and run the command using a CGI. For this method the Login and Password are optional and are used for authorizing SiteScope to log on to the remote machine if required. ▶ Rlogin. Log in to the remote server using the Rlogin protocol. ▶ SSH. Log in to the remote server using the SSH protocol. This may require additional software and setup depending on the version of UNIX. ▶ Telnet. Log in to the remote server using Telnet. <p>For information about the connection methods, see “Connection Methods for Remote UNIX” on page 299.</p>
Prompt	<p>This is the prompt output when the remote system is ready to handle a command.</p> <p>Default value: #</p>
Login Prompt	<p>This is the prompt output when the system is waiting for the login to be entered.</p> <p>Default value: login:</p>
Password Prompt	<p>This is the prompt output when the system is waiting for the password to be entered.</p> <p>Default value: password:</p>
Secondary Prompt	<p>Enter the secondary prompts if the telnet connection to the remote server causes the remote server to prompt for more information about the connection. Separate multiple prompt string by commas (,).</p> <p>Example: For Telnet connections to some remote servers, the remote server may ask what terminal type should be emulated for the connection. In this case, enter Terminal type? as the secondary prompt. The response to the secondary prompt is entered in the Secondary Response box below.</p>

GUI Element	Description
Secondary Response	Enter the responses to any secondary prompts required to establish connections with this remote server. Separate multiple responses with commas (,).
Initialize Shell Environment	<p>Enter any shell commands to be run at the beginning of the session. Separate multiple commands with a semicolon (;). This option specifies shell commands to be run on the remote machine directly after a Telnet or SSH session has been initiated. These commands can be used to customize the shell for each SiteScope remote. Some examples include:</p> <ul style="list-style-type: none"> ▶ The remote shell may not have the correct path set for SiteScope scripts to run. The following command adds the directory <code>/usr/local/bin</code> into the <code>PATH</code> of the current shell on the remote machine: <code>export PATH=\$PATH:/usr/local/sbin</code> ▶ The remote shell may not be initializing the pseudo terminal correctly. Enter the following command to increase the terminal width to 1024 characters: <code>stty cols 1024;\${SHELL}</code> <p>Note: Commands after a shell invocation are not run.</p> <ul style="list-style-type: none"> ▶ There have been cases where the remote Telnet Server does not echo back the command line properly. This may cause strange behavior for monitors that rely on this behavior. Enter the following command to force the remote terminal to echo: <code>stty echo</code> ▶ Certain UNIX shells have been known to behave erratically with SiteScope. This includes <code>bash</code>, <code>ksh</code>, and <code>csh</code>. Enter the following command to change the shell to <code>sh</code> for the SiteScope connection: <code>/bin/sh</code>
Remote Machine Encoding	<p>Enter the encoding for the remote server if the remote server is running an operating system version that uses a different character encoding than the server on which SiteScope is running. This enables SiteScope to display encoded content correctly.</p> <p>Default value: Cp1252 encoding</p> <p>Other encodings: Cp1251, Cp1256, Shift_JIS, EUC_JP</p>

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
SSH Connection Method	<p>Select the client to use for this connection from the list. The currently supported clients are:</p> <ul style="list-style-type: none"> ▶ Internal Java Libraries. Connect using the Java SSH client integrated with SiteScope. ▶ Plink/External SSH. Connect using an external SSH client. On Microsoft Windows, SiteScope includes Plink. On Solaris or Linux SiteScope uses an installed client such as OpenSSH.
SSH Port Number	Enter the port on which the remote SSH server is listening.
Disable Connection Caching	<p>Select to turn off connection caching for this remote.</p> <p>Default value: Not selected (SiteScope caches open connections)</p>
Connection Limit	<p>Enter the number of open connections that SiteScope allows for this remote. If there are many monitors configured to use this connection, set the number of open connections high enough to relieve a potential bottleneck.</p> <p>Note: This setting does not effect running tests for a remote server. Tests always create a new connection.</p>

GUI Element	Description
SSH Authentication Method	<p>Select the authentication method to use for SSH connections from the list. The currently supported methods are:</p> <ul style="list-style-type: none"> ▶ Password. Authenticate using a password. ▶ Key File. Authenticate using public/private key authentication. When this option is selected, SiteScope uses the private key in the file <SiteScope root directory>\groups\identity to authenticate. The corresponding public key must be listed in the authorized_keys file on the remote host. For information about SSH requirements, see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1541.
Key File for SSH connections	<p>Select the file that contains the private key for this connection. The default key file is SiteScope\groups\identity. This setting applies only when the authentication method is Key File.</p>
SSH Version 2 Only	<p>Check this option to force SiteScope to use SSH protocol version 2 only. This option applies only when using the integrated Java Client. For information about configuring an external SSH client to use SSH2 protocol, see “External SSH Client Overview” on page 1566.</p>
SSK Keep Alive Mechanism	<p>Check this option to engage a keep alive mechanism for SSH version 2 sessions. This option applies only when using the integrated Java Client.</p>

GUI Element	Description
Custom Commandline	<p>Enter a custom command line for a remote server using the External Client. Use this option when passing specific commands to the external client to be run. Valid substitution variable are:</p> <ul style="list-style-type: none"> ➤ \$root\$. This translates the SiteScope directory. ➤ \$user\$. This translates the username entered into the remote server. ➤ \$password\$. This translates the password entered into the remote server. ➤ \$host\$. This translates the host name entered into the remote server.
Description	<p>Add a text description for the remote UNIX server. This text appears only when editing the remote's properties. You can include HTML tags such as the
, <HR>, and tags to control display format and style.</p> <p>Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> ➤ Tags: script, object, param, frame, iframe. ➤ Any tag that contains an attribute starting with on is declined. For example, onhover. ➤ Any attribute with javascript as its value.

Category Settings

The following elements are included:

GUI Element	Description
Assigned categories	<p>Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see "Create and Define a New Category" on page 198.</p>

Connection Methods for Remote UNIX

This table includes information on the methods for connecting SiteScope to remote UNIX servers.

Connection Method	Description
<p>HTTP</p>	<p>There are some cases where it may be useful to use a Common Gateway Interface program over HTTP to access performance data or application data from a UNIX server. Two simple CGI scripts are included with SiteScope to enable access over HTTP:</p> <ul style="list-style-type: none"> ▶ <code><SiteScope root directory>\conf\examples\remote.pl</code> ▶ <code><SiteScope root directory>\conf\examples\remote.sh</code> <p>The remote.pl CGI is a Perl (version 4 and above) script that runs a command on the server; the remote.sh script does the same, except as a UNIX sh script. CGI commands are passed in using the <code>COMMAND</code> CGI variable. If you are using the CGI connection method and you want to use remote actions, remember that the permissions for both the directory containing the CGI script and the <code>/script</code> directory must enable the Web server (probably running as a user with few permissions) to run in those directories. Additionally, the scripts must have execute permission.</p> <p>If you want to use a CGI script that puts more restrictive limits on the commands that can be run, you can use a different CGI script. All that matters is that the CGI returns the output of the command passed in using the <code>COMMAND</code> variable. For greater security, it is recommended to set up your Web server to require a login/password authorization to run the script. Also, if you have a secure Web server on that server, you can set up the script to run using the Secure Sockets Layer (SSL used in HTTPS requests), so that the request and output is encrypted.</p>
<p>rlogin</p>	<p>You can set up your remote servers to require a password for rlogin, or to enable access without a password (like "rsh"). SiteScope supports either case.</p>

Connection Method	Description
SSH	<p>For Solaris, using the SSH access method requires that an SSH client is installed on the SiteScope machine and the SSH server installed on the servers you are monitoring. The path to the SSH client on the machine where SiteScope is running should be <code>/usr/local/bin/ssh</code> or <code>/usr/bin/ssh</code>. For information about SSH requirements, see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1541.</p> <p>For Microsoft Windows NT or 2000, an SSH client is included in the package. For debugging, the Microsoft Windows SSH client can be run from the command line, replacing the values for the username, host name, and password:</p> <pre>\SiteScope\tools\plink.exe -ssh myUser@myServer.myCompany.com -pw myPassword</pre> <p>Using SSH requires that digital certificates be installed on each of the servers to which you are connecting.</p>
telnet	<p>Telnet is a popular method for connecting to remote UNIX servers. You can set up your remote servers to require a password for telnet, or to enable access without a password (like "rsh"). SiteScope handles either case.</p>

Log Preferences User Interface

Description	<p>Effective system availability monitoring requires that monitoring data be recorded and stored for a required interval of time. SiteScope Log Preferences controls the accumulation and storage of monitor data.</p> <p>To access: Expand Preferences in the monitor tree and click Log Preferences.</p>
Important Information	<p>Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences.</p>
Useful Links	<p>“Log Preferences” on page 221</p> <p>“SiteScope Log Database Table Structure” on page 246</p> <p>“Troubleshooting and Limitations” on page 334</p>

The Log Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Daily Logs To Keep	<p>Enter the number of days of monitoring data to keep. Once a day, SiteScope deletes any logs older than the specified number of days.</p> <p>Default value: 40</p> <p>Note: Keeping monitor data logs for long periods can cause a data storage problem for the SiteScope server depending on the total number of monitors configured and how often the monitors run per day. You should monitor the size of the log files in the <code><SiteScope root directory>\logs</code> directory to estimate the data accumulation rate and adjust the Daily Logs To Keep setting or server resources as necessary.</p>

GUI Element	Description
Maximum Size of Logs	<p>Enter the maximum size allowed for all monitoring logs. Once a day, SiteScope checks the total size of all monitoring logs and removes any old logs that are over the maximum size.</p> <p>Default value: No value</p> <p>Note: By default, this setting is blank and not used as it can result in the loss of monitor report data.</p>
Database Connection URL	<p>To enable Database logging, enter a URL to a Database Connection. The easiest way to create a database connection is to use ODBC to create a named connection to a database.</p> <p>Example: First use the ODBC control panel to create a connection called SiteScopeLog. Then, enter jdbc:odbc:SiteScopeLog in this box as the connection URL.</p> <p>Note for using Windows Authentication: If you want to access the database using Windows authentication, enter jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>;AuthenticationMethod=type2 as the connection URL, and com.mercury.jdbc.sqlserver.SQLServerDriver as your database driver. Leave the Database User Name and Database Password boxes empty, since the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.</p>
Database Driver	<p>Specify the database driver SiteScope should use to connect to the database. The driver should be a JDBC driver. To have SiteScope use another driver the driver must also be installed in the <SiteScope root directory>\WEB-INF\lib directory and the path and filename must be entered in this box.</p> <p>Default value: sun.jdbc.odbc.JdbcOdbcDriver</p>

GUI Element	Description
Database Username	Enter the username used to log in to the database. If using Microsoft SQL server, leave this blank and choose NT Authentication when setting up the ODBC connection. With NT Authentication, SiteScope connects using the login account of the SiteScope service.
Database Password	Enter a password used to login to the database. If using Microsoft SQL server, leave this blank and choose NT Authentication when creating the ODBC connection. With NT Authentication, SiteScope connects using the login account of the SiteScope service.
Backup Database Connection URL	<p>(Optional) Enter a URL to a backup database. Use this option to provide failover of SiteScope database logging if the primary database becomes unavailable.</p> <p>Note: The same database table definition, database driver, user name, and password are applied to both database connections.</p> <p>After saving changes to the Database preferences, stop and restart the SiteScope service for the changes take effect.</p>

E-mail Preferences User Interface

Description	E-mail is the default media for sending event alerts when a problem has been detected by SiteScope (in addition to the visual icons and status messages displayed in the SiteScope interface). Use the E-mail Preferences to indicate the SMTP mail server, recipient addresses, and other settings that SiteScope should use when sending e-mail alerts and other SiteScope messages. To access: Expand Preferences in the monitor tree and click Mail Preferences .
Important Information	Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences.
Useful Links	“E-mail Preferences” on page 222 “E-mail Recipient Profile Settings” on page 307

The E-mail Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
E-Mail Server Domain Name	Enter the domain name of the SMTP mail server that SiteScope should use when sending e-mail messages. Example: mail.thiscompany.com If you are unsure of your mail server's domain name, check with your Systems Administrator.
Administrator E-mail Address	Enter the e-mail address to which SiteScope should send status messages. Example: sysadmin@thiscompany.com

GUI Element	Description
Daily Status	Select this option to have SiteScope send a brief daily status message to the administrator's e-mail address. This e-mail is scheduled to be generated at 7:07 AM every day. The subject of e-mail sent includes: "SiteScope daily status". The e-mail content includes the number of active monitors and groups, along with a URL link to the applicable SiteScope main page plus the version number of SiteScope installation.
SiteScope Starts/Restarts	Select this option to have SiteScope send a brief message each time that SiteScope restarts. Normally, SiteScope automatically restarts itself once a day. Other restarts may be an indication of a monitor run problem. For more information, see "SiteScope Server Health" on page 365.
From E-mail Address	Enter the e-mail address used as the From Address for mail generated by SiteScope. Specifying an e-mail address may make it easier to browse and sort e-mail sent by SiteScope. If nothing is entered, the From E-mail Address stays the same as the address where the mail is sent from. Example: sitescope@mycompany.com Note: If the mail server being used required NTLM authentication (see below), the e-mail address entered here must be a valid e-mail address.
Backup Mail Server Domain Name	Enter the domain name of the SMTP mail server that SiteScope should use whenever the primary mail server cannot be reached. If unsure of backup mail server's domain name, check with the Systems Administrator. Example: gateway.mycompany.com.
Login	Enter the username required by the SMTP server in this box. This user name is used for both the primary and backup mail servers. Note: You must restart SiteScope if you change this setting.

GUI Element	Description
Password	<p>If the SMTP server you want SiteScope to use requires authentication, enter the password for username entered in the Login box. This password is used for both the primary and backup mail servers.</p> <p>Note: You must restart SiteScope if you change this setting.</p>
NTLM Authentication	<p>Select an NTLM authentication option from the drop-down list:</p> <ul style="list-style-type: none"> ▶ None. Select if the mail server does not require NTLM authentication. ▶ NTLMv1. Select if the mail server requires authentication using NTLM version 1. ▶ NTLMv2. Select if the mail server requires authentication using NTLM version <p>Note: You must restart SiteScope if you change this setting.</p>
Timeout	<p>Enter an optional length of time (in seconds) to wait for a response from the SMTP server. If a response from the primary mail server is not received within the timeout period, SiteScope switches to use the backup mail server.</p> <p>Default value: No value</p>

E-mail Recipient Profile Settings

Description	The E-mail Recipients page lists E-mail Recipient profiles that you use with SiteScope E-mail Alerts. Create and use the E-mail Recipient profiles for sending SiteScope e-mail alerts to individuals or groups other than the SiteScope Administrator e-mail entered on the E-mail Properties. To access: Expand Preferences in the monitor tree and click Mail Preferences . Click New E-Mail Recipient .
Important Information	You cannot delete an E-mail recipient profile if it is referenced by an alert action. You must change the recipient in the alert before you can delete the profile.
Useful Links	“E-mail Preferences” on page 222 “E-mail Preferences User Interface” on page 304

The E-mail Recipient Profile includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	Enter a text description for the E-mail Recipient Profile definition. The name is used to identify the E-mail Recipient Profile definition in the product display.
E-mail To	The e-mail addresses to which you want to send the alert. Example: test@mycompany.com You can enter multiple e-mail addresses by separating the e-mail addresses with commas. Example: test@mycompany.com, sysadmin@thiscompany.com
Disabled	Stops e-mail alerts from being sent to these e-mail addresses. Use this option to temporarily disable a particular e-mail without editing every alert that contains this e-mail setting.

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Template	Select a template from the drop-down list to define the e-mail alert settings. Once a setting is defined, a single alert is sent to people and pagers. Use the ShortMail template for pagers.
Schedule	Use this option to specify when e-mail settings should be enabled. You may select a more restricted schedule from the names schedules in the drop-down menu. Default value: every day, all day
Description	Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the , <HR>, and tags to control display format and style. Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content: <ul style="list-style-type: none"> ➤ Tags: script, object, param, frame, iframe. ➤ Any tag that contains an attribute starting with on is declined. For example, onhover. ➤ Any attribute with javascript as its value.

Category Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see “Create and Define a New Category” on page 198.

Pager Preferences User Interface

Description	<p>Pager Preferences configures settings and additional pager profiles that SiteScope uses for sending Pager alerts.</p> <ul style="list-style-type: none"> ▶ Sends an automated notification to system administrators who may not have immediate access to e-mail. ▶ Sends alert escalation or notifies support personnel who may be away from the office. <p>To access: Expand Preferences in the monitor tree and click Pager Preferences.</p>
Important Information	Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences.
Useful Links	<p>“Pager Preferences” on page 222</p> <p>“Pager Recipient Profiles” on page 313</p>

The Pager Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Modem Port	<p>Select the communications port that the modem is connected to on the SiteScope server. For SiteScope on Solaris or Linux, enter the path and device name for the modem. On Microsoft Windows NT/2000 platforms, SiteScope uses COM port numbers for both RS-232C type serial ports as well as for USB modem ports.</p> <p>If you are using a USB type modem, select the COM port associated with the USB port to have SiteScope use the USB modem. To find the COM port number for the USB modem, use the Settings > Network and Dial-up Connections menu. Right-click the desired modem, and then click Properties. The properties should show the COM port number that is associated to the modem.</p>

GUI Element	Description
Connection Speed	Select the modem speed used for connections to the paging service from the drop-down list. Default value: 1200 baud
Pager Connection Options	Select an option for sending a message to your paging service: <ul style="list-style-type: none"> ▶ Modem-to-Modem Connection (preferred). Select if you have an alphanumeric pager and use an alphanumeric paging service. ▶ Dial and Enter Message. Select to dial a direct phone number to send a page. ▶ Dial, Enter Command, and Enter Message. Select if you have a direct number, but need to enter a command before sending a page. ▶ Custom Modem Connection. Select if your paging company does not use any of the previous connection choices. <p>For the information required for the selected option, see the table below.</p>

Pager Connection Options

Enter the information required for the selected Pager Connection option:

GUI Element	Description
Modem number	Enter the phone number to use for sending alphanumeric pages to the paging service modem.
Modem pin number	Enter the last seven digits of the PIN number for your alphanumeric pager. If you use an alphanumeric paging service, you must enter the phone number to use for sending alphanumeric pages to the paging service modem. This number is provided by your paging service. The paging service sometimes refers to this as the TAP/IXO number.

GUI Element	Description
Phone number	<p>Enter the phone number exactly as you would dial it from your telephone, including other numbers you may need, such as a number to get an outside line. You can use dashes to make the number easier to read. Use commas to separate the portions of the phone number. Each comma causes the modem script to pause for a few seconds before dialing the rest of the number.</p> <p>Example: If you are dialing your pager from your office, and you have to dial 9 to get an outside line, enter: 9, 555-6789.</p>
Send page command	<p>Enter the page command exactly as you would dial it from your touch tone telephone.</p>
Custom Modem command.	<p>Enter the entire modem command including the phone number to dial, any additional digits, and \$message. SiteScope replaces \$message with the message you specified for each alert.</p> <p>Example: If the number for the pager company is 123-4567, your pager PIN is 333-3333, and your pager company requires that you follow each command with the # key, the command might look like this: ATDT 123-4567,,333-3333#,, \$message#</p> <p>Note: For SiteScope running on UNIX, enter the device path for your modem in the Modem Path box. To see a list of devices using Solaris, use the <code>ls /dev/term/*</code> command.</p>

Pager Recipient Profiles

Description	<p>The Pager Recipients Contents view lists Pager Recipient profiles that can be used with SiteScope Pager Alerts. This view lists the name of all the currently defined Pager settings or profiles. Create and use different Pager Recipient profiles for sending SiteScope Pager alerts to individuals or groups other than the one defined in the Pager Recipient Properties.</p> <p>To access: Expand Preferences in the monitor tree and click Pager Preferences. Click New Pager Recipient.</p>
Important Information	<p>You cannot delete a Pager Recipient profile if it is referenced by an alert action. You must change the recipient in the alert before you can delete the profile.</p>
Useful Links	<p>“Pager Preferences” on page 222</p> <p>“Pager Preferences User Interface” on page 309</p>

The Pager Recipient Profiles includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	<p>Enter the text name string assigned to the setting profile when you create a new pager recipient.</p>
Connection Speed	<p>Select the modem speed used for connections to the paging service from the drop-down menu list.</p> <p>Default value: 1200 baud</p>

GUI Element	Description
Pager Connection Options	<p>There are four options for sending a message to your paging service:</p> <ul style="list-style-type: none"> ➤ Modem-to-Modem Connection (preferred) ➤ Dial and Enter Message ➤ Dial, Enter Command, and Enter Message ➤ Custom Modem Connection <p>The preferred option is to connect directly to a modem at your pager service. When a modem-to-modem connection is used, SiteScope is able to verify that the message was sent successfully and can receive messages describing any communication problem. The other connection options generally send messages to automated voice response systems using touch tone dialing. The touch tone dialing method is limited to numeric messages and SiteScope cannot confirm that your paging service correctly received the message.</p> <p>For information about the different options, see “Pager Preferences” on page 222.</p>
Disabled	Select to temporarily disable a particular pager without editing every alert that contains this persons pager.

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Schedule	Specifies when pager settings should be enabled. A more restricted schedule can be selected from the drop-down list. Default value: every day, all day
Description	Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the , <HR>, and tags to control display format and style. Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content: <ul style="list-style-type: none"> ▶ Tags: script, object, param, frame, iframe. ▶ Any tag that contains an attribute starting with on is declined. For example, onhover. ▶ Any attribute with javascript as its value.

Category Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see “Create and Define a New Category” on page 198.

SNMP Trap Preferences User Interface

Description	Used to define settings that are used by SiteScope SNMP Trap alerts when sending data to management consoles. SiteScope uses the SiteScope SNMP Trap Alert type to integrate with SNMP-based network management systems. To access: Expand Preferences in the monitor tree and click SNMP Preferences .
Important Information	<ul style="list-style-type: none"> ▶ Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences. ▶ You cannot delete an SNMP Trap profile if it is referenced by an alert action. You must change the SNMP Trap in the alert before you can delete the SNMP Trap profile.
Useful Links	“SNMP Trap Preferences” on page 223

The SNMP Trap Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	Enter the text name string assigned to the setting profile when creating a new SNMP recipient.
Send to Host	Enter the domain name or IP address of the machine that receives all SNMP trap messages. This machine must be running an SNMP console to receive the trap message. Examples: snmp.mydomain.com or 206.168.191.20.
SNMP Port	The SNMP port to which the trap is sent.

GUI Element	Description
SNMP Community	<p>The default SNMP community name used for sending traps. The community string must match the community string used by the SNMP management console.</p> <p>Default value: public</p>
SNMP Trap ID	<p>The type of trap to send. There are several predefined ID types for common conditions.</p> <ul style="list-style-type: none"> ▶ Select a generic SNMP type from the Generic SNMP Trap ID drop-down list. ▶ To use an enterprise specific SNMP ID type, enter the number of the specific trap type in the Enterprise-Specific SNMP Trap ID box.
SNMP Trap Version	<p>Select the default SNMP protocol version number to use. SNMP v1 and v2c are currently supported.</p>
SNMP Object ID	<p>This identifies to the console the object that sent the message.</p> <ul style="list-style-type: none"> ▶ Select one of the predefined objects from the Preconfigured SNMP Object IDs drop-down list. ▶ To use another object ID, enter the other object ID in the Other SNMP Object ID box.

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Description	<p>Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the
, <HR>, and tags to control display format and style.</p> <p>Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> ▶ Tags: script, object, param, frame, iframe. ▶ Any tag that contains an attribute starting with on is declined. For example, onhover. ▶ Any attribute with javascript as its value.

Category Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Assigned categories	<p>Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see “Create and Define a New Category” on page 198.</p>

Absolute Schedule Preferences User Interface

Description	Used for customizing the operation of SiteScope monitors and alerts to run only at specific times. To access: Expand Preferences in the monitor tree and click Absolute Schedule Preferences .
Important Information	<ul style="list-style-type: none"> ▶ Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences. ▶ You cannot delete an Absolute Schedule profile if it is referenced by an alert action, report, monitor, or monitor threshold. You must remove the profile from each dependency before you can delete the profile.
Useful Links	"Absolute Schedule Preferences" on page 224

The Absolute Schedule includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	Enter a name for the Absolute Schedule. The name is used to identify the Absolute Schedule in the product display.
Days of the Week	Enter the time or times that the monitor needs to run in the boxes next to the day of the week. Time values for absolute schedules must be limited to the 24-hour period of a standard day for each day. To enter multiple times for a single day, separate the times by a comma (,). Example: 01,02:30,23:30 runs the monitor at 1:00 AM, 2:30 AM, and 11:30 PM

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Description	<p>Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the
, <HR>, and tags to control display format and style.</p> <p>Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> ▶ Tags: script, object, param, frame, iframe. ▶ Any tag that contains an attribute starting with on is declined. For example, onhover. ▶ Any attribute with javascript as its value.

Category Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Assigned categories	<p>Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see “Create and Define a New Category” on page 198.</p>

Range Schedule Preferences User Interface

Description	Used for customizing the operation of SiteScope monitors and alerts to run only during specific time periods. To access: Expand Preferences in the monitor tree and click Range Schedule Preferences .
Important Information	<ul style="list-style-type: none"> ▶ Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences. ▶ You cannot delete a Range Schedule profile if it is referenced by an alert action, report, monitor, or monitor threshold. You must remove the profile from each dependency before you can delete the profile.
Useful Links	"Range Schedule Preferences" on page 225

The Range Schedule Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	Enter a name for the Range Schedule.
Days of the Week	<p>In the boxes next to the day of the week, select Enabled or Disabled and enter the time or times the monitor needs to run. Time values for range schedules must be limited to the 24-hour period of a standard day for each day.</p> <p>Example: To disable monitors from 6:00 PM on Thursday evening until 8:00 AM the following morning, enter a From value of 18 to 24 for Thursday and then enter from 0 to 8 for Friday. If you enter a From value of 18 and a To value of 8 on the Thursday schedule, the schedule becomes invalid.</p> <p>To enter multiple times for a single day, separate the times by a comma (.). For example, to disable from 2-3AM and 7-8AM, enter 2:00,3:00 to 7:00,8:00.</p> <p>Default value: Enabled (no time values specified). See the table below for more information.</p>

Days of the Week

Enable Setting (Enable / Disable)	Time Range (From /To)	Schedule Effect
Enable	From and To time values specified	Monitors are enabled to run only during the From and To time range.
Enable	(no time values specified)	Monitors are enabled to run during all hours of the applicable day. This is the default setting for 24-hour operation.

Enable Setting (Enable / Disable)	Time Range (From /To)	Schedule Effect
Disable	From and To time values specified	Monitors are enabled to run during all hours of the applicable day, except during the From and To time range.
Disable	(no time values specified)	Monitors are disabled during all hours of the applicable day.

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Description	<p>Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the
, <HR>, and tags to control display format and style.</p> <p>Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> ▶ Tags: script, object, param, frame, iframe. ▶ Any tag that contains an attribute starting with on is declined. For example, onhover. ▶ Any attribute with javascript as its value.

Category Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see “Create and Define a New Category” on page 198.

User Preferences User Interface

Description	The data provided by SiteScope can be made available to multiple users without granting full administrative privileges to all users. This page allows you to create multiple user accounts that provide different view and edit permissions for different audiences. To access: Expand Preferences in the monitor tree and click Users Preferences .
Important Information	Only an administrator in SiteScope, or a user granted Edit Preferences permissions can create or make changes to SiteScope Preferences.
Useful Links	“User Preferences” on page 226

The User Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Login Name	<p>Enter the SiteScope login name to access SiteScope using this profile.</p> <p>Alternatively, users can log into SiteScope using LDAP authentication by entering a value in the LDAP boxes below.</p> <p>Allowed characters: Latin alphanumeric.</p> <p>Note: Entering characters other than the allowed characters does not cause an error when creating the user profile. However, the user cannot log in to SiteScope using that login name.</p>
Password	<p>Enter the SiteScope login password for this user.</p> <p>If using LDAP for user authentication, there is no need to enter a password here. Users enter their LDAP password in the SiteScope login dialog box when they log in to their user account.</p> <p>For information about password requirements, see “Changing a User’s Password” on page 228.</p> <p>All SiteScope passwords are encrypted using 3DES (also known as TDES or Triple Data Encryption Algorithm). Although the TDES key is stored in SiteScope, it cannot be modified. For more information, refer to “Hardening the SiteScope Platform” in the <i>HP SiteScope Deployment Guide</i> PDF.</p>
Confirm Password	<p>Re-enter the password entered in the Password box. This is used when creating a new user profile or changing the password of an existing user profile.</p>

GUI Element	Description
LDAP Service Provider	<p>To access the SiteScope service using a centralized LDAP authentication rather than the SiteScope specific password, enter the URL of the applicable LDAP server. This way, password authentication for access to SiteScope can be performed by LDAP.</p> <p>Example: ldap://ldap.mydomain.com:389.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ Users still need to have a SiteScope login name defined. ▶ Users can use LDAP to access SiteScope, but they must have a user login and security principal assigned to them on the LDAP server.
LDAP Security Principal	<p>When using LDAP authentication to access the SiteScope service, enter the Security Principal for this user.</p> <p>Example: uid=testuser,ou=TEST,o=this-company.com</p> <p>Note: Users may be defined with special characters on the LDAP server. However, SiteScope does not support users that contain the following characters in their user name: equal ("="), semi-colon (";"), inverted commas ("").</p>
Title	<p>(Optional) Enter a title for this User profile. The title is displayed in the list of users. If you do not enter a title, the Login Name value is used as the Title.</p>
Allowed Groups	<p>Use the expandable menu tree to select the monitor groups that can be accessed by this user profile. Select the groups the user is allowed to access. Select the box next to individual groups or subgroups to enable access to that group. To restrict user access to fewer groups, clear the check box for the SiteScope node and then select the individual groups below the SiteScope node to which you want to enable access.</p> <p>Default value: The SiteScope node is checked to enable access to all groups.</p>

GUI Element	Description
Login Disabled	Select to disable access to SiteScope with this username and password. Clear the check box to enable access using the user profile.

Enable Editing/Deleting User Preferences

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Enable edit users	Enables the user to edit or delete user preferences for all other users, except the SiteScope administrator user.

Group Actions

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Edit Groups	Enables the user to add new groups, rename, copy, or delete existing monitor groups.
Refresh Groups	Enables the user to refresh or force all the monitors within a group to run regardless of their schedule.
Disable Groups	Enables the user to disable groups.

Monitor Actions

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Edit Monitors	Enables the user to add new monitors, edit existing monitor configurations, or delete monitors.
Refresh Monitors	Enables the user to refresh or force individual monitors to run regardless of their schedule.
Acknowledge Monitors	Enables the user to use the Acknowledge function to comment on monitor status on the group detail page.
Disable Monitors	Enables the user to disable monitors within a group.
Use Monitor Tools	Enables the user to use the Diagnostic Tools form for certain monitor types. When a diagnostic tool is available for a monitor type, a hyperlink is presented in the More column for that monitor in the group detail page. Diagnostic tools may expose sensitive system information.

Alert Actions

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
View Alerts List	Enables the user to view the list of currently configured alert definitions on the Alert List page.
Edit Alerts	Enables the user to add a new alert, edit, or delete existing alerts.
Test Alerts	Enables the user to test an existing alert definition.

GUI Element	Description
Disable Alerts Indefinitely	Enables the user to disable or enable one or more alerts indefinitely.
Disable Alerts Temporarily	Enables the user to disable or enable one or more alerts temporarily.
Create Adhoc Alert Reports	Enables the user to create adhoc or quick alert reports using the Alert Report link below the Alert Definitions table.

Report Actions

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Generate Reports	Enables the user to create a scheduled report manually.
Edit Reports	Enables the user to add new report definitions, and edit or delete existing report definitions.
Create Adhoc Reports	Enables the user to use the Quick Report action on the Management Reports page to create ad hoc reports.
Disable Reports	Enables the user to disable or enable the generation of existing reports.
View Monitor History Report	Enables the user to view the recent history report for a monitor.

Preference Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Edit Preferences	Enables the user to use any of the forms available on the Preferences submenu to add or edit SiteScope settings for e-mail alerts and other SiteScope messages, logging, integration, connectivity to remote servers, and so forth.
Test Preferences	Enables the user to test any preference setting that is testable. This is usually a setting for communicating with an external service such as e-mail, modem, SNMP, or other external application.

View Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
View View	Enables the user to view the Views page to see a list of defined views.
Edit View	Enables the user to add, edit, or delete views and view settings.

Categories Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
View Category	Enables the user to view the Categories page to see a list of defined categories.
Edit Category	Enables the user to add, edit, or delete categories and category settings.

Templates Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
View Templates	Enables the user to view templates that exist in the monitor tree.
Edit Templates	Enables the user to add, edit, deploy, and delete templates.

Other Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Use Tools	Enables the user to view and use the tools in the Tools container.
Use Browse and Summary	Enables the user to use the Browse Monitor form and the Monitor Summary Report.
View Progress	Enables the user to view the progress page showing monitors that are running and SiteScope monitoring load.
View Logs	Enables the user to view the raw data reported by SiteScope monitors, sent by alerts, and other SiteScope logs.

Dashboard Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Edit Favorites	Enables the user to add or delete items in the favorite views list in the Dashboard view.

Credential Preferences User Interface

Description	Provides centralized credential management for SiteScope resources. This enables you to add, update, and delete credentials that are used in configuring SiteScope monitors, templates, and remote hosts. To access: Expand Preferences in the monitor tree and click Credential Preferences .
Important Information	<ul style="list-style-type: none"> ▶ You cannot delete a credential profile if it is referenced by a monitor. You must remove the profile from each dependency before you can delete the profile. ▶ Only an administrator, or a user granted Edit Preferences permissions, can create or make changes to the credentials.
Included in Tasks	"Configure Credential Preferences" on page 243
Useful Links	"Credential Preferences" on page 229

The Credential Preferences includes the following elements:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Name	Enter a descriptive name for the credential profile. Maximum length: 50 characters Note: You cannot use the following characters in the credential profile name: < > ' "
Domain	(Optional) Enter the domain for the credential. During the connection, the domain is added to the login in the format: <domain>\<login>.
Login	Enter the user name to access the resource using this credential profile.

GUI Element	Description
Password	Enter the password to access the resource using this credential profile. All SiteScope passwords are encrypted using 3DES (also known as TDES or Triple Data Encryption Algorithm). For more information, refer to “Hardening the SiteScope Platform” in the <i>HP SiteScope Deployment Guide</i> PDF.
Confirm Password	Re-enter the password entered in the Password box. This is used when creating a new credential or changing the password of an existing credential.

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Description	Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the , <HR>, and tags to control display format and style. Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content: <ul style="list-style-type: none"> ▶ Tags: script, object, param, frame, iframe. ▶ Any tag that contains an attribute starting with on is declined. For example, onhover. ▶ Any attribute with javascript as its value.

Category Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see “Create and Define a New Category” on page 198.

Troubleshooting and Limitations

This section contains troubleshooting and limitations for issues relating to SiteScope preferences.

- ▶ “Remote Servers” on page 335
- ▶ “Reporting Data to Business Availability Center” on page 340
- ▶ “Database Logging Connections” on page 341

Remote Servers

Troubleshooting SiteScope Monitoring of Remote Windows NT and Windows 2000 Servers

The following is additional information relating to setting up and troubleshooting SiteScope monitoring of remote Windows NT and Windows 2000 servers.

- ▶ Connect to the remote machine using PERFMON. If a connection cannot be made using this tool, there is likely a problem involving the user access permissions granted to the SiteScope account on the remote server. SiteScope requires certain administrative permissions to be able to monitor server statistics.
- ▶ For security reasons, SiteScope may not be allowed to use the permissions of a full administrator account. SiteScope can be granted restricted monitoring access by editing certain Windows Registry Keys. For information about restricting access to the registry from a remote machine, refer to the Microsoft Knowledge Base (<http://support.microsoft.com/kb/q153183/>).
- ▶ When you need to monitor a server which is a stand-alone server or not part of a domain already visible to the SiteScope server, try entering the machine name followed by a slash and then the login name in the **Login** box. For example, loneserver\sitescope.
- ▶ Some problems have been found when trying to monitor Windows 2000 servers from SiteScope running on Windows NT4. In many cases, the problem involves incompatibility of the DLL's used by the operating system to communicate between the servers.

Note:

- ▶ For additional information on how to secure performance data in Windows 2000, Windows NT, and Windows XP, refer to the Microsoft Knowledge Base (<http://support.microsoft.com/kb/q146906/>).
 - ▶ For information about troubleshooting performance monitor counter problems for Windows 2000 and Windows NT, refer to the Microsoft Knowledge Base (<http://support.microsoft.com/kb/152513/>).
-

Troubleshooting Microsoft Windows Event Log Access on Remote Windows Servers

Problem:

When viewing Remote Windows event logs or getting alerts relating to monitoring a remote Windows machine, the following message is displayed:

```
The description for Event ID ( XXXX ) in Source ( XXXX ) could not be found. It contains the following insertion string(s):  
The operation has completed successfully.
```

Cause:

When you view the event log on a computer from a remote computer, if the required registry keys (and referenced files) are not present on the remote computer, SiteScope is unable to format the data; hence it displays the data in a generic format.

Resolution:

The required registry entries and DLL files must be copied to the remote computer on which the event viewer application is being run.

To get the remote registry entries and DLL files onto the local SiteScope machine:

- 1 Locate on the remote machine which event you are not getting properly in SiteScope by finding the entry in the Event Viewer. Write down the information for the source, event id, and description. For example:

```
Source: MExchangeSA, Event ID: 5008, Description: The message tracking log file C:\exchsrvr\tracking.log\20020723.log was deleted.
```

- 2 Open the registry setting **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application** and click the source (for example, MExchangeSA).
- 3 Click **EventMessageFile** and write down the data for where that DLL is located (for example, C:\EXCHSRVR\bin\madmsg.dll).

- 4 Locate the DLL on the remote and copy it to the SiteScope machine. You can perform the copy in one of two ways:
 - ▶ Use the **Initlog.exe** utility, in the BackOffice Resource Kit, Second Edition, to copy the required registry entries from the Exchange Server computer to the remote computer. This utility can also copy the required DLL files if you are logged on to Windows NT with an account that has Administrator privilege on the Exchange Server computer (see Microsoft Article Q184719).
 - ▶ Use FTP, mail, and so forth, to get the file to your local drive.
- 5 SiteScope uses the data from the **EventMessageFile** field in step 3 to determine where to find the DLL on the local machine. You must create the same folder structure as in this step and place the file in that directory. Alternatively, you can change the directory structure to say `c:\Windows\System32` (SiteScope looks in the ADMIN\$ by default on the remote machine), and place the DLL in that folder, but you must have this structure and the DLL on both machines. If you do this, you must update the registry in step 3 to reflect the directory in which the DLL is located.

Troubleshooting Remote Windows Connections Using Perfex

Use the following steps to view that data is being returned when SiteScope is trying to access the remote registry:

- 1 Open a command window on the SiteScope server.
- 2 Change the directory to `<SiteScope root directory>\tools`.
- 3 Enter the following in a command line:

```
perfex \\MACHINE -u username -p password -d -elast "Application"
```

This command gives you the number of entries in your Application log. For example:

```
Connected to \\ex-srv as int-ss Next Record: 2369
```

- 4 You should list only the last 10 or 12 events to find the one you are looking for. For this example, the command is:

```
perfx \\MACHINE -u username -p password -d -elog "Application" 2355 | more
```

- 5 Look through each entry until you find the one you need. Note the Record id for easier searching next time when using the command in Step 3.
- 6 This output tells you what data SiteScope is receiving. In the example given, the following is an example of the data that typically would be returned:

```
Type: Information
Time: 02:00:24 08/01/102
Source: MExchangeMTA
ID: 298
Category: 1
Record: 2342
Machine: EX-SRV
FILE=C:\EXCHSRVR\res\mtamsg.dll
REMOTE FILE=
String 835050d is: MTA
Next String 835054d is: OPERATOR
Next String 83505dd is: 34
Next String 835060d is: 0
Next String 835062d is:
File: C:\EXCHSRVR\res\mtamsg.dll
Remote Path:
calling FormatMessage()
Formatted Message 142 bytes long
Raw message is: The most current routing information has been loaded by the MTA,
and a text copy was saved in the fileGWART0.MTA. [MTA OPERATOR 34 0] (12)
Message: The most current routing information has been loaded by the MTA, and a text
copy was saved in the file GWART0.MTA.[MTA OPERATOR 34 0] (12)
```

The file path is where the remote file is being found. If you copy the DLL to the WINDOWS\SYSTEM, the file and remote file path like this:

```
Type: Information
Time: 03:15:00 08/01/102
Source: MSExchangeIS Public
ID: 1221
Category: 6
Record: 2350
Machine: EX-SRV
FILE=C:\WINNT\SYSTEM32\mdbmsg.dll
REMOTE FILE=\\ex-srv\ADMIN$\SYSTEM32\mdbmsg.dll
String 835054d is: 0
Next String 835056d is:
File: C:\WINNT\SYSTEM32\mdbmsg.dll
Remote Path: \\ex-srv\ADMIN$\SYSTEM32\mdbmsg.dll
LOADING LIB REMOTE: \\ex-srv\ADMIN$\SYSTEM32\mdbmsg.dllcalling
FormatMessage()Formatted Message 89 bytes long
Raw message is: The database has 0 megabytes of free spaceafter online
defragmentation has terminated.Message: The database has 0 megabytes of free
space afteronline defragmentation has terminated.
```

Troubleshooting Remote UNIX Servers Not Configured For an English Locale

Problem:

The File Monitor and Directory Monitor may fail when using UNIX remote servers that are not configured by default for an English locale or language.

Resolution:

Add "LANG=C; export LANG" to the **Initialize Shell Environment** property of the problematic UNIX remote server.

Reporting Data to Business Availability Center

Due to the complexity of some monitoring deployments and network communications, there may be some time when SiteScope is temporarily unable to communicate with the Business Availability Center server. SiteScope Health monitoring includes several monitors for watching connectivity and data transfers to the Business Availability Center server.

If SiteScope is unable to connect to the HP Business Availability Center Server, SiteScope continues to record and store monitor data files locally. Once the number of data files exceeds a specified threshold, SiteScope saves the data files in a cache folder with the syntax `<SiteScope_root>\cache\persistent\topaz\data<index>.old`.

Note: By default, the threshold number of data files is set to 1,000 files. You can change this setting by modifying the `_topazMaxPersistenceDirSize` property in the `master.config` file.

After the connection between SiteScope and the Agent Server is restored, you must manually copy the files from these folders to the `<SiteScope root directory>\cache\persistent\topaz\data` folder. It is recommended that you only copy these files when the data folder is empty to avoid overloading the system with large amounts of data to upload. When the number of `data.old` folders exceeds a specified threshold, by default 10 folders, the oldest folders are deleted.

Note: You can configure the number of `data.old` folders to keep by modifying the `_topazMaxOldDirs` property in the `master.config` file.

Database Logging Connections

When Database logging is active and working correctly, you should see a table called **SiteScopeLog** in your database and a record added to the table every time a monitor runs. The data is sent to the database as a single table in a flat-file format.

If the **SiteScopeLog** table is not created or is empty, check the `<SiteScope root directory>\logs\RunMonitor.log` and `<SiteScope root directory>\logs\Error.log` files for log messages starting with "jdbc" or "odbc". When Database logging is working correctly, you should see a set of messages in **RunMonitor.log** that looks like this:

```
jdbc log, reconnect seconds=600
jdbc log, loading, driver=sun.jdbc.odbc.JdbcOdbcDriver
jdbc log, connecting, url=jdbc:odbc:SiteScopeLog,
jdbc log, logged in
jdbc log, checking log table
jdbc log, created log table
jdbc log, prepare insert, 19, INSERT INTO SiteScopeLog...
jdbc log, connected
```

If these entries do not appear in the log file there is a problem with the database interface or configuration of the database connection. You should also check the Database Connection URL you entered. This parameter is case sensitive. Check the spelling and letter case of the connection URL and be sure there are no leading or trailing spaces present in the text box.

You can also check the HP Software Self-solve knowledge base (<http://h20230.www2.hp.com/selfsolve/documents>) for other information relating to database logging. To enter the knowledge base, you must log in with your HP Passport ID.

10

Global Search and Replace

This chapter includes the main concepts, tasks, and reference information for the Global Search and Replace Wizard.

This chapter includes:

Concepts

- ▶ Global Search and Replace Overview on page 343

Tasks

- ▶ Perform a Global Search and Replace on page 345

Reference

- ▶ Global Search and Replace User Interface on page 350

Global Search and Replace Overview

The Global Search and Replace Wizard enables you to make changes to monitor, alert, alert action, group, preferences, and report properties. You can select an object based on object type and globally replace any of the properties of the selected object across your SiteScope or across multiple SiteScopes when working in System Availability Management Administration.

For example, when upgrading HP Business Availability Center, use the Global Search and Replace Wizard to configure all the SiteScopes reporting data to Business Availability Center report to the upgraded version.

Advanced Filter

Use the Advanced Filter option to further refine your selected object for the search operation. You can select specific properties and select or enter values pertaining to your object. This enables you to limit the selected objects but not the value to replace. When performing the replace operation, only the value to replace is replaced and only on those objects that match the properties selected in the Advanced Filter page. For example, select all monitors with frequency set to 5 minutes and replace the monitor dependency setting for all of those monitors, or select only those monitors monitoring a specific server and replace the threshold settings for only those monitor instances matching the value of the server entered in the Advanced Filter.

Find and Replace

Use this method of replacement to search for specific settings and property values and replace only those objects with the entered setting or value. You can search a string, value, or regular expression pattern and replace only that string. Replacements are made only if the filter criteria matches. For example, search for all monitors whose name value includes a server name that is no longer in use. Replace the string representing the old server with a new string representing the updated server.

Threshold Settings

When replacing threshold settings for monitors, by default you replace only those settings that share all of the following:

- ▶ have the same condition (**Error if**, **Warning if**, or **Good if**)
- ▶ are configured for the same schedule
- ▶ use the same operator type (< <=, > >=, ==, !=, contains, !contains).

Note: < (less than) and <= (less than and equal to) are considered the same operator type as are > (greater than) and >= (greater than and equal to).

You also have the option to override all the existing threshold settings that have the same condition (**Error if**, **Warning if**, or **Good if**) regardless of the operator used and the schedule configured. The option is called **Override Category** and appears in the Choose Changes page of the wizard under the **Threshold Settings** area if you selected **Monitor** in the Select Type page of the wizard.

For example, you want to change the **Error if** threshold settings for all CPU monitors to greater than 85%. In the wizard, you select **Monitor** in the Select Type page, **CPU** in the Select Subtype page, and expand the **Threshold Settings** area in the Choose Changes page.

If you select the **Override Category** option when selecting greater than 85% as the **New Error if** status condition, all the existing **Error if** settings for all CPU monitors are overwritten and changed to greater than 85% when you complete the wizard.

If you leave the option cleared, the greater than 85% **Error if** setting you select in the wizard replaces only those **Error if** settings that use the < (greater than) and <= (greater than and equal to) operators and were configured for the same schedule for all CPU monitors.

For details on setting thresholds, see “Setting Status Thresholds” on page 476.

Perform a Global Search and Replace

This task describes how to perform a global search and replace for objects, using the Global Search and Replace Wizard.

This task includes the following steps:

- “Begin Running the Global Search and Replace Wizard” on page 346
- “Select Object Type” on page 346
- “Search and Replace Objects” on page 347
- “Check Affected Objects” on page 350
- “Review Replaced Objects” on page 350

1 Begin Running the Global Search and Replace Wizard

When you are accessing SiteScope from Business Availability Center, in System Availability Management Administration, select **Admin > System Availability Management** and click the **Global Search and Replace** button.

When you are accessing SiteScope standalone, right-click the group, preferences, alert, or monitor in the monitor tree to which you want to perform the global replace, and select **Global Replace** from the menu.

For details on the user interface, see “Global Search and Replace Wizard” on page 351.

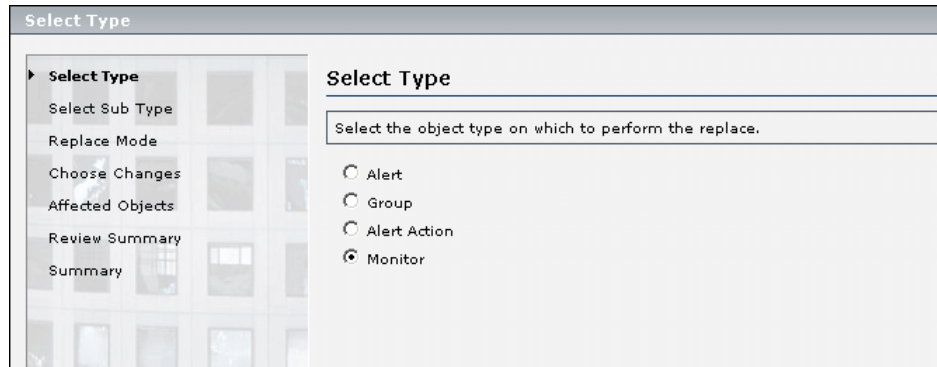
2 Select Object Type

In the **Select Type** and **Select Subtype** page, select the object and, if relevant, the subtype upon which you want to make a replacement. For details on the user interface, see “Select Type Page” on page 352 and see “Select Subtype Page” on page 353.

Example

You want to change the threshold boundaries for all CPU monitors.

You select **Monitor** as the object type



You select **CPU** as the specific monitor type.

The screenshot shows a web interface window titled "Select Sub Type". On the left is a sidebar with a tree view containing the following items: "Select Type", "Select Sub Type" (which is expanded), "Replace Mode", "Choose Changes", "Affected Objects", "Review Summary", and "Summary". The main content area is titled "Select Subtype" and contains a text box with the instruction "Select the type of SiteScope Monitor on which to perform the replace." Below the text box, there is a list of options with checkboxes. The "CPU" option is checked.

3 Search and Replace Objects

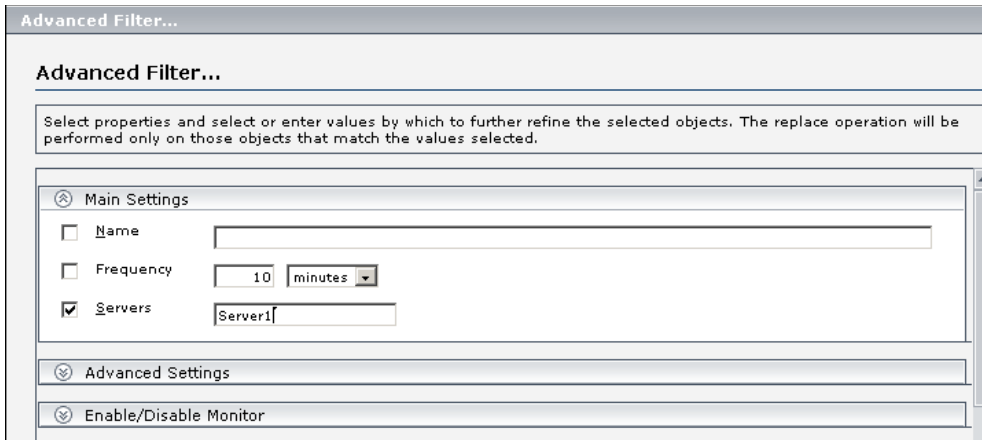
In the **Replace Mode** page, select the type of replacement. Select **Replace** to globally replace the object or select **Find and Replace** to replace specific instances of the object. Optionally, you can open the Advanced Filter dialog box to filter by the object properties. Here you select onto which objects to perform the replace operation. In the **Choose Changes** page, you select what properties or values to replace.

For details on the user interface, see “Replace Mode Page” on page 354 and see “Choose Changes Page” on page 356.

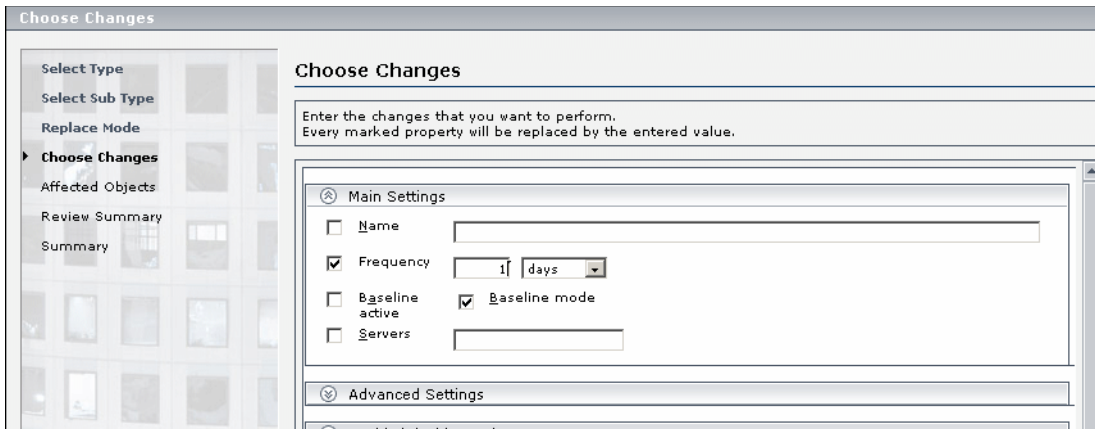
Example

You want to reduce the frequency of how often a monitor runs on a specific server in your company.

You filter your selection in the Advanced Filter page to include only those monitors monitoring the specified server.



In the Choose Changes page, you then enter a new frequency of once a day, to monitor the specified server.



Example

You set up your alert action to send alert messages to specified e-mail addresses. However, one of the e-mail addresses you configured to receive the alerts has changed and you want to send alert messages to the new e-mail address. You want to update only the e-mail address that has changed.

After selecting **Alert Action** as the object type, you select **Find and Replace** in the Replace Mode page.

Replace Mode

Select Type
Select Sub Type
► **Replace Mode**
Choose Changes
Affected Objects
Review Summary
Summary

Replace Mode

Select the replace mode. Choose Replace if you want to replace a field with a new value. Choose Find and Replace to search for a string with a field and replace it with a new value.

Replace
 Find And Replace

In the Choose Changes page, you enter the old e-mail address in the **Find** field and the new e-mail address in the **and Replace with** field.

Choose Changes

Select Type
Select Sub Type
Replace Mode
► **Choose Changes**
Affected Objects
Review Summary
Summary

Choose Changes

Enter the changes that you want to perform. Every marked property will be replaced by the entered value.

Find : @yahoo and Replace with : @hotmail

⊕ Main Settings
 Action Name

4 Check Affected Objects

In the **Affected Objects** page, view the affected objects and, if necessary, clear or select objects for the replacement operation. For details on the user interface, see “Affected Objects Page” on page 359.

5 Review Replaced Objects

In the **Review Summary** page, review the results of the replacement operation and click **Finish** to complete the wizard. You can view a summary of the changes in the **Summary** page to see which changes were implemented successfully and in which errors occurred.

For details on the user interface, see “Review Summary Page” on page 360 and see “Summary Page” on page 362.

Global Search and Replace User Interface

This section describes:

- Global Search and Replace Wizard on page 351
- Select SiteScope Page on page 352
- Select Type Page on page 352
- Select Subtype Page on page 353
- Replace Mode Page on page 354
- Choose Changes Page on page 356
- Affected Objects Page on page 359
- Review Summary Page on page 360
- Summary Page on page 362

Global Search and Replace Wizard

Description	<p>Global Search and Replace enables you to make changes to monitor, alert, group, preferences, alert action, and report properties. These changes can be made across an entire SiteScope infrastructure when working in SiteScope standalone or across several SiteScopes when working in System Availability Management Administration.</p> <p>To access:</p> <p>In SiteScope standalone, right-click the group, preferences, alert, or monitor in the monitor tree to which you want to perform the global replace, and select Global Replace from the menu.</p> <p>In System Availability Management Administration, select Admin > System Availability Management and click the Global Search and Replace button.</p>
Included in Tasks	“Perform a Global Search and Replace” on page 345
Wizard Map	<p>The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.</p>

Select SiteScope Page

Description	Use the Select SiteScope Page to select the SiteScope on which to make replacements.
Important Information	Only SiteScopes running version 9.0 and higher and whose connection status allows configuration changes from System Availability Management are listed. You must select at least one SiteScope.
Wizard Map	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.

Select Type Page

Description	Use the Select Type page to select the object type on which you want to make replacements.
Important Information	Only those types of objects available for the node you selected are listed.
Wizard Map	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Alert Alert Action Group Monitor Preferences Report	<p>You can select only one object type for each replace operation. Only those objects appear that exist in the SiteScope.</p> <p>When performing Global Search and Replace from System Availability Management Administration, group, monitor, alert, alert action, and preferences appear only if they exist on at least one SiteScope selected in the previous page.</p>


Select Subtype Page

Description	Use the Select Subtype page to select the properties of the object type on which you want to make replacements.
Important Information	<p>This page opens only if you selected Alert Action, Monitor, or Preferences as the object type in the Select Type Page of the wizard.</p> <p>If you selected the object type Group or Report, this page does not open.</p>
Wizard Map	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.

Replace Mode Page

Description	Use the Replace Mode page to select the type of replacement: global replacement or replacement based on filter criteria.
Wizard Map	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	<p>Optionally, click to open the Advanced Filter dialog box if you want to further refine your selections. You can select objects based on their specific settings and not only based on object type.</p> <p>The Advanced Filter page opens with setting areas pertinent to the object you selected. For details about these settings, refer to the selected object's settings page.</p> <p>Examples:</p> <ul style="list-style-type: none"> ▶ Select all alerts that have a defined category of critical and replace any setting for those alerts. ▶ Select all groups with a dependency set to a specific monitor or group and replace any setting for those groups. <p>Note: Using the Advanced Filter option merely refines your selection for the replace and does not determine what to replace.</p>
<p>Find and Replace</p>	<p>Select to search the target objects for properties that match a string or regular expression and replace only the matching pattern with the replacement value.</p> <p>This method of replacement includes a search for specific settings and property values and replaces only those objects with the entered setting or value. You can select only a partial value and replace only that string.</p> <p>Example: Search for all monitors whose name value includes a server name that is no longer in use. Replace the string representing the old server with a new string representing the updated server.</p> <p>Note: Use this setting to determine the selection and the value to replace. It differs from the Advanced Filter option which is a way to limit the selected objects but not the value to replace.</p>
<p>Replace</p>	<p>Globally replaces all matching objects with the new string or value.</p>

Choose Changes Page

<p>Description</p>	<p>Use the Choose Changes page to select what to replace for the global replace.</p> <p>The wizard displays only the settings and properties that may be changed for the object type selected in the previous pages.</p> <p>The filter criteria is built from your selections in the Type, Subtype, and Advanced Filter pages.</p>
<p>Important Information</p>	<p>The subtype’s properties may be displayed differently than how they are displayed when editing a monitor, alert, preference, and so forth in SiteScope.</p> <p>Examples: Mail Preferences is a text box in Global Search and Replace utility rather than a drop-down list, and the Depends On property is not displayed in the Global Search and Replace utility.</p> <p>Note for users of SiteScope within System Availability Management Administration:</p> <ul style="list-style-type: none"> ▶ If you select SiteScope as the object type, properties of all selected subtypes of the selected SiteScopes are included in this page. ▶ If the SiteScopes selected for the replace operation are not all the same version, the subtypes of the SiteScopes may have different properties.
<p>Wizard Map</p>	<p>The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Settings area>	<p>This area includes the settings for the object you selected. For details about these settings, refer to the selected object's settings page.</p> <ul style="list-style-type: none"> ▶ If you selected Find and Replace in the Replace Mode page, you must select only the setting in the settings area. Type the value to replace in the Find/Replace with boxes. ▶ If you selected Replace in the Replace Mode page, you must select the setting and the value to replace in the settings area. <p>Note: If you selected Monitor in the Select Type page:</p> <ul style="list-style-type: none"> ▶ The Topology Settings appear only if your selection includes only one monitor type. You cannot use the Global Search and Replace wizard to replace topology settings for multiple monitor types. Note that topology settings are available for Integration monitors and monitors that support reporting topologies to Business Availability Center. For details, see “Reporting Discovered Topologies to HP Business Availability Center” on page 50. ▶ In the Threshold Settings area, the Override Category option appears. When selected, this option enables you to override the threshold settings of the same threshold condition (Error if, Warning if, or Good if) for the selected monitor instances with the settings you enter here for the replace operation. If this option is cleared, the settings you enter here replace only those settings with the same operator type (< <=, > >=, !=, ==, contains, !contains) and the same configured schedule for the monitor instances. Any other settings for the same condition but with a different operator type or a different schedule remain. For details on this option and an example, see “Threshold Settings” on page 344.

GUI Element	Description
<p>Find Replace With</p>	<p>If you chose the Find and Replace option in the Replace Mode page, the text boxes Find and Replace With are added to the top of this page.</p> <ul style="list-style-type: none"> ➤ In the Find box, type the search string, value, or regular expression pattern for the setting or property you want to replace. ➤ In the Replace With box, type the string or value to which you want all matching patterns to be changed. <p>Note: If you select Frequency in Main Settings drop-down list, the values you type in the Find and Replace With text boxes must be in seconds. For example, you want to find monitors with a frequency of 10 minutes and change the frequency to 20 minutes. In the Find text box, type 600 and in the Replace With text box type 1200.</p> <p>If no objects are found that meet the filter criteria, an error message appears. Reselect your filter criteria.</p>

 **Affected Objects Page**

Description	<p>Use the Affected Objects page to view the objects that you selected to change. The page displays the selected objects in tree format.</p> <p>You can clear or select objects in the Affected Objects tree for the replacement operation.</p> <ul style="list-style-type: none"> ▶ If you selected Find and Replace in the Replace Mode page, replacements are made only if the filter criteria are matched. ▶ If you selected Replace, replacements are made in all selected objects.
Important Information	<p>The objects displayed depend on whether the user has change permissions on those objects.</p> <ul style="list-style-type: none"> ▶ When in System Availability Management Administration, the permissions are set in Business Availability Center's Permissions Management (Admin > Platform > Users and Permissions). ▶ When in SiteScope standalone, the permissions are set in Preferences > User Preferences.
Wizard Map	<p>The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets):


GUI Element	Description
<Affected Objects tree>	<p>The Affected Objects tree includes all objects that are matched against the various filter criteria selected in the previous pages of the wizard.</p> <p>Select or clear objects as required for the replace operation.</p> <p>Note: When using Global Replace from System Availability Management Administration, a tree is displayed for each SiteScope selected.</p>

Review Summary Page

Description	<p>Use the Review Summary page to preview the objects on which the replacement operation is performed. The number of objects affected by the global replacement is given above the table listing the replacements.</p> <p>When working with multiple SiteScopes in System Availability Management Administration, a table is displayed for each SiteScope and the name of the SiteScope appears above the table.</p>
--------------------	--

Important Information	<p>The number of objects that are affected by the global replacement is displayed above the table.</p> <p>Each table column can be sorted in ascending or descending order by right-clicking the column title. An up or down arrow indicates the sort order.</p> <p>Once you click Finish in this page, you cannot undo the replacement operation.</p>
Wizard Map	<p>The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.</p>


The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element	Description
	<p>Change the sort order in the columns by clicking the up and down arrow in the column title.</p> <p>Default: The Monitor Full Name column is in alphabetical order, from top to bottom.</p>
Monitor Full Name	<p>The name format is <group name>/<monitor name>.</p>
Property	<p>The box name that you marked in the Choose Changes page that changes as a result of the replace operation.</p>
Previous Value	<p>The current value that changes as a result of the replace operation.</p>
New Value	<p>The new value that you entered in the Choose Changes page.</p>

Summary Page

Description	<p>The Summary page reports the changes that were implemented successfully and those in which errors occurred. The page displays the changes in table format.</p> <p>When working with multiple SiteScopes in System Availability Management Administration, a table is displayed for each SiteScope and the name of the SiteScope appears at the top of the table.</p>
Important Information	<p>The number of objects affected by the global replacement is given above the table.</p> <p>Each table column can be sorted in ascending or descending order by right-clicking the column title. An up or down arrow indicates the sort order.</p> <p>There is no way to undo changes made by the replace operation.</p>
Wizard Map	<p>The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Change the sort order in the columns by clicking the up and down arrow in the column title.</p> <p>Default: The Monitor Full Name column is in alphabetical order, from top to bottom.</p>
Monitor Full Name	The name format is <group name>/<monitor name>.
Property	The box name that you marked in the Choose Changes page that changed as a result of the replace operation.

GUI Element	Description
Previous Value	The value that was replaced in the global replace operation.
New Value	The new value that resulted from the global replace operation.
	Click to open a printer-friendly version of the results. This version can then be printed, sent via email, converted into a format for editing, such as Microsoft Word, and saved.
OK	Closes the wizard. You return to System Availability Management Administration in Business Availability Center or SiteScope Dashboard in standalone.

11

SiteScope Server Health

This chapter includes the main concepts, tasks, and reference information for monitoring SiteScope server health.

This chapter includes:

Concepts

- ▶ SiteScope Health Overview on page 366
- ▶ SiteScope Health Group on page 366
- ▶ BAC Integration Statistics Monitor on page 367
- ▶ SiteScope Log Events Monitor on page 368
- ▶ SiteScope Monitor Load Monitor on page 370
- ▶ SiteScope Server Health Monitor on page 370
- ▶ Using Log Files on page 371
- ▶ Using the Audit Log on page 372
- ▶ Using the SiteScope Progress Report on page 373

Tasks

- ▶ Analyze SiteScope Health Monitor Data on page 376
- ▶ Configure the Audit Log on page 382

Reference

- ▶ SiteScope Log File Columns on page 383
- ▶ Audit Log Entries on page 384
- ▶ SiteScope Health User Interface on page 394

Troubleshooting and Limitations on page 409

SiteScope Health Overview

SiteScope Health is a specially designed group of monitors that display information about SiteScope's the performance and availability SiteScope itself. Health monitors retrieve data about SiteScope's resource usage, key processes, monitor load, server parameters, and the integrity of key configuration files.

By default, the daily monitor logs record the SiteScope Health monitoring data and let you can create reports on SiteScope's performance and operational health. These log files are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions. For example, SiteScope's audit log contains configuration changes performed in the new user interface, such as creation of monitors, templates, alerts, and so forth.

Together with the SiteScope Health monitoring, the SiteScope Progress Report Page provides several key indicators you use to monitor the performance of the SiteScope application.

SiteScope Health Group

SiteScope Health monitors can monitor several key aspects of its own environment to help uncover monitor configuration problems as well as SiteScope server load. SiteScope can also monitor its connectivity and related data events when connected to HP Business Availability Center.

Similar to regular monitors, Health monitors can be edited in order to reconfigure their frequency and thresholds. Administrators can enhance the Health group by adding new monitors targeting additional servers and environments.

The Health monitor group is displayed as a health icon within the main SiteScope container. You view the contents of the Health monitor group by clicking the **Health** container.

SiteScope Health monitoring includes the following monitor types:

Monitor Type	Default Name	Description
BAC Integration Statistics Monitor	BAC Integration Statistics	Checks the traffic volume between SiteScope and Business Availability Center when SiteScope is configured as a data collector for HP Business Availability Center.
Log Event Health Monitor	Log Event Checker	Checks for certain events logged to the SiteScope error log.
Monitor Load Monitor	Monitor Load Checker	Checks for data about the number of monitors being run or waiting to run.
Health of SiteScope Server Monitor	Health of SiteScope Server	Checks a large number of server process and resources for the server on which SiteScope is running.

BAC Integration Statistics Monitor

The BAC Integration Statistics monitor checks the health of HP Business Availability Center. When SiteScope is integrated as a data collector for Business Availability Center, this health monitor enables you to track the volume of traffic between SiteScope and Business Availability Center. SiteScope sends metrics to BAC every minutes.

For details on configuring this monitor, see “BAC Integration Statistics Monitor Page” on page 395.

SiteScope Log Events Monitor

The Log Event Monitor is the equivalent of a SiteScope monitor group that watches the SiteScope Error Log (**error.log**) for certain events. These events include Log entries indicating that a monitor has been skipped or there was a problem in reporting data to another application.

This section includes:

- ▶ “Skipped Monitor Events” on page 368
- ▶ “Problems Reporting Data” on page 369

Skipped Monitor Events

A SiteScope monitor is reported as skipped if the monitor fails to complete its actions before it is scheduled to run again. This can occur with monitors that have complex actions to perform, such as querying databases, stepping through multi-page URL sequences, waiting for scripts to run, or waiting for an application that has hung.

For example, assume you have a URL Sequence Monitor that is configured to transit a series of eight Web pages. This sequence includes performing a search which may have a slow response time. The monitor is set to run once every 60 seconds. When the system is responding well, the monitor can run to completion in 45 seconds. However, at times, the search request takes longer and then it takes up to 90 seconds to complete the transaction. In this case, the monitor has not completed before SiteScope is scheduled to run the monitor again. SiteScope detects this and makes a log event in the SiteScope error log. The SiteScope Log Event Monitor detects this and signals an error status.

A monitor may also skip if it is a monitor type that requires a process from the process pool but the process pool limit has been reached. Generally, this is not likely to happen but may occur in some situations with high monitoring load. The SiteScope Health Log Event Monitor also watches for process pool events. Skipped monitors can cause loss of data when a monitor run is suspended due because a previous run has not completed or has become hung by a unresponsive application. They can also cause

SiteScope to automatically stop and restart itself, an event that is also monitored by the SiteScope Health Log Event Monitor. A restart is done in an effort to clear problems and reset monitors. However, this can also lead to gaps in monitoring coverage and data. Adjusting the run frequency at which a monitor is set to run or specifying an applicable timeout value can often correct the problem of skipping monitors.

Note:

- You can enable a setting that automatically disables monitors that exceed the maximum allowed skip count. If this occurs, SiteScope shuts down with an error and sends an e-mail to the SiteScope administrator about the skipping monitor to signal the disable event. To enable this setting, expand **Preferences** in the left menu tree, choose **Infrastructure Settings Preferences**, and select the **Server Settings** section. Select the **Shutdown on monitor skips** check box. This functionality is disabled by default.
- You can control the maximum number of processes available from the **Maximum processes per pool** box in the Infrastructure Settings Preferences page. The default is 50. You should only change this setting if adjustments to monitor configurations do not resolve the monitor performance problems. To access this setting, expand **Preferences** in the left menu tree, choose **Infrastructure Settings Preferences**, and select the **General Settings** section.

Problems Reporting Data

The Log Event Monitor is also configured to report log events that indicate a problem with the transfer of SiteScope monitor and configuration data to an HP Business Availability Center installation. For information about troubleshooting data reporting to Business Availability Center, see “Reporting Data to Business Availability Center” on page 340.

For details on configuring this monitor, see “Log Event Health Monitor Page” on page 396.

SiteScope Monitor Load Monitor

The Monitor Load Monitor is the equivalent of a SiteScope monitor group that watches how many monitors are running and how many are waiting to be run. Watching monitor load is important to help maintain monitoring performance and continuity. If the number monitors waiting approaches or exceeds the number of monitors running, adjustments should be made to monitor configurations to reduce the number of monitors waiting to run. Generally, this can be done by reducing the run frequency of some monitors.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the server being monitored is irrelevant).

For details on configuring this monitor, see “Monitor Load Monitor Page” on page 399.

SiteScope Server Health Monitor

The Health of SiteScope Server Monitor is the equivalent of a SiteScope monitor group that monitors server resources on the server where SiteScope is running. This includes monitors for CPU, disk space, memory, and key processes. A problem with resource usage on the SiteScope server may be caused by monitors with configuration problems or may simply indicate that a particular SiteScope is reaching its performance capacity. For example, high CPU usage by SiteScope may indicate that the total number of monitors being run is reaching a limit. High disk space usage may indicate that the SiteScope monitor data logs are about to exceed the capacity of the local disk drives. For details on SiteScope data logging options, see “Log Preferences” on page 221.

For details on configuring this monitor, see “Health of SiteScope Server Monitor Page” on page 400.

Using Log Files

SiteScope maintains a number of log files that are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions.

Log files can be accessed using the Log File tab. When you click a log file, a new browser window opens displaying the text of the log file. You can use the scroll bars to view the contents of the log or use the browser's text Find utility to locate specific information. For example, you can search for a unique text string that appears in a monitor's **Name** property to locate entries for a particular monitor instance. For details on the various SiteScope log files, see "Log Files Page" on page 404.

The log files are written in plain text and stored in the `<SiteScope_root_path>\logs` directory. In the default configuration, these log files are tab-delimited text files. Understanding the order and content of these files is useful for examining particular monitor results or for porting the SiteScope monitor results to another database. For details, see "SiteScope Log File Columns" on page 383.

Using the Audit Log

SiteScope's audit log provides you with a record of actions performed in SiteScope, the time they were performed, and by whom. It contains configuration changes performed in the new user interface, such as creation of monitors, templates, alerts, and so forth.

Note: When SiteScope is attached to Monitor Administration in HP Business Availability Center, the actions you perform on SiteScope appear in HP Business Availability Center's audit log and not in SiteScope's audit log.

As each operation is performed, an entry is made in the audit log. When the current audit log reaches its size limit, it is closed and a new log is created. Older logs are named `audit.log.1`, `audit.log.2`, and so forth. The higher the number concatenated to the name, the older the log. For details on setting the size limit and the maximum number of backup audit logs to be kept, see "Configure the Audit Log" on page 382.

The name of the current audit log is **audit.log** and it is found in the `<SiteScope root directory>\logs` directory. You can access the audit log from the directory or through the SiteScope application. For details on viewing the audit log, see "Log Files Page" on page 404.

Most operations performed in the monitor tree are recorded in the audit log. For a list of operations that are not recorded in the audit log, see "Audit Log Limitations" on page 409.

Using the SiteScope Progress Report

The SiteScope Progress Report page provides an overview of several key SiteScope server performance metrics. It displays the SiteScope monitoring load statistics and a list of which SiteScope monitors are running, and which monitors have run recently, at what time, and what was the returned status. The report page is updated every 20 seconds.

This section includes:

- ▶ “Viewing the Progress Report” on page 373
- ▶ “Interpreting the Progress Report” on page 373

Viewing the Progress Report

For details on the Progress Report, see “SiteScope Progress Report Page” on page 407.

Interpreting the Progress Report

Monitoring Load can be a key indicator of SiteScope scaling problems, monitor configuration problems, or network performance issues. The following is a brief explanation of the SiteScope monitor execution model and interpreting the Progress Report in the context of this model.

A SiteScope monitor instance is essential as an instruction set that is run by the SiteScope application on a regularly scheduled interval. While a monitor instance is defined, SiteScope queues the monitor for execution based on the run (update) frequency and schedule options. If the monitor instance is marked as disabled, it is still scheduled in the queue but the normal instructions are not run.

As a Java-based application, SiteScope makes use of multi-threading to accomplish parallel execution of monitor tasks. Each monitor instance scheduled for execution is assigned a thread. Once it is assigned a thread, the monitor instance becomes a **Monitor Running**. It remains bound to the thread until the monitor execution instruction has either received a result or the timeout value, if applicable, has been reached.

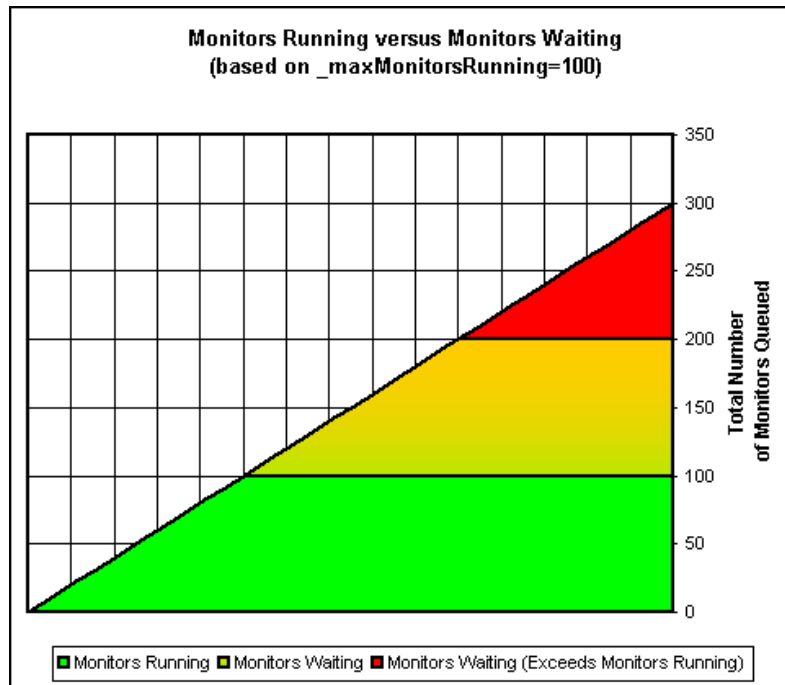
Even in this model, monitor execution is not instantaneous and there is a finite limit to the number of monitor threads that can be run in parallel. If not more threads are available, a monitor that is queued for execution becomes a **Monitor Waiting** for an execution thread.

It is difficult to assign specific values and limits to SiteScope Monitoring Load because the specifics of the server capacity and network deployment can vary widely. The monitoring load may also vary significantly over time simply due to transient network traffic issues or SiteScope monitor configuration problems.

One key warning signal for interpreting monitoring load is the ratio of Monitors Waiting to Monitors Running. Generally, having some monitors waiting for execution is not a problem unless the ratio of Monitors Waiting to Monitors Running is consistently 1:2 or higher. For example, if the number of monitors running is at the maximum of 100 and there are 50 monitors waiting, this represents a ratio of 1 monitor waiting for every two running.

Note: The maximum number of monitor execution threads for monitors to run is controlled by the `_maxMonitorsRunning=100` setting in the **master.config**.

The graph below presents a visualization of the relationship between Monitors Running and Monitors Waiting. This graph is based on the default `_maxMonitorsRunning` setting of 100 monitors. The green region shows that SiteScope is able to run all queued monitors until the number of queued monitors exceeds 100. At that level, additional monitors that are scheduled to run are given the status of Monitor Waiting. The red region represents an area where the number of monitors waiting is more than twice the number of monitors running. This is certain indication that your SiteScope monitor configurations are not well aligned with the capacity of the server and network.



You can adjust the following monitor configuration settings if there are consistently too many monitors waiting:

- ▶ **Update Every (frequency).** This is the basic schedule parameter for every monitor type. A large number of Monitors Running and Monitors Waiting can often be explained by a large number of monitors set to run (or update) at short intervals. The minimum update interval is 15 seconds. Depending on a number of system factors, there are several monitor actions which may take more than 15 seconds to complete. For example, Web transactions, database queries, logging onto remote servers, and some regular expression matches may delay monitor completion. Use the “Monitor Summary Report” on page 1477 to check the frequency setting for groups of monitors and consider increasing the value for some monitors.
- ▶ **Verify Error.** Regular or extensive use of this option has the effect of rapidly increasing the monitor run queue whenever the applicable SiteScope monitors detect an error condition. While this option has its purpose, it should not be used by default on every monitor. Use the “Monitor Summary Report” on page 1477 to list monitors that may have the Verify Error setting enabled.

Analyze SiteScope Health Monitor Data

This task describes the steps involved in analyzing SiteScope Health monitor data and viewing the SiteScope log files and Progress Report.

This task includes the following steps:

- ▶ “Prerequisites” on page 377
- ▶ “Deploy SiteScope Health Monitors” on page 377
- ▶ “View SiteScope Health Monitors” on page 378
- ▶ “View SiteScope Log Files” on page 379
- ▶ “View the SiteScope Progress Report” on page 380

1 Prerequisites

To access the log files and the Progress Report page, you must have the correct user privileges. Select **Preferences > User Preferences** and click the user name. In the contents page, open the **Other Options** pane, and ensure that **View Progress** and **View Logs** are selected.

2 Deploy SiteScope Health Monitors

If the SiteScope Health monitors are not present when you import a SiteScope to System Availability Management in HP Business Availability Center, you must deploy the monitors. For details on how to perform this task, see “Deploy SiteScope Health Monitors” on page 381.

Note: The SiteScope health monitors are normally present, because they are enabled automatically when SiteScope is deployed.

3 View SiteScope Health Monitors

You can view the data collected by the SiteScope Health monitors in the SiteScope Dashboard. For details on the user interface, see “SiteScope Health User Interface” on page 394.

Example

SiteScope -> Health 12/11/07 6:41 AM								
Name ▲	Type	Target	Status	Summary	Updated			
BAC Integration Statistics ▼	BAC Integration Statistics			Currently logging to Bu	12/11/07 6:41 AM			
Health of SiteScope Server ▼	Monitor Load Monitor	SiteScope Ser		LogicalDisk/C:/% Free Process/java/Thread C Process/perfex/Thread Process/java/Handle C Process/perfex/Handle Process/java/Pool Pag Network Interface/MS T Memory/% Committed Process/perfex/Pool P Process/java/Pool Non Memory/Available MB Processor/_Total/% Pr Process/perfex/Pool N Process/perfex/% Proc	12/11/07 6:38 AM			
Log Event Checker ▼	Log Event Health			*skipped #1.*=0 *skipped #2.*=0 *skipped #3.*=0 *skipped #4.*=0 *skipped #5.*=0 *SiteScope is shutting *Reached the limit of *Error. data reporter f *Error. config reporter *Error. Mercury Busine *Error. CacheSender. *Error. CacheSender. *Mercury Business Av *Commit verification f *Error loading monito *Error contacting mirr *Error: open SSH con *Error: failure in base	12/11/07 6:32 AM			
Monitor Load Checker ▼	Monitor Load			Current Monitors Run F Current Monitor Run	12/11/07 6:41 AM			

4 View SiteScope Log Files

You can view the various SiteScope log files in the Log Files tab. For details on the user interface, see “Log Files Page” on page 404.

Example

The screenshot shows the SiteScope Health "Health" interface with the "Log Files" tab selected. The interface displays a list of log files with their descriptions and sizes. The logs listed are:

- Alert log**: Every time an alert is sent, a description of the alert is stored in the Alert log. **(no entries in log yet)**
- Error log**: If there is a problem executing alerts or with SiteScope in general, a description of the error is saved in the Error log. (size is 221K)
- Run Monitor Log**: Monitor processing is stored in the Run Monitor log. (size is 269K)
- HP Business Availability Center Log**: HP Business Availability Center integrations log file. (size is 0 bytes)
- Post Log File**: A log of HTTP post requests. **(no entries in log yet)**
- URL Details**: For each HTTP and HTTPS request made, details are saved in the URL log. **(no entries in log yet)**
- Operator Log**: Operator actions such as acknowledgment are saved in the Operator log. **(no entries in log yet)**
- Audit Log**: Audit log listing configuration changes made to the system. (size is 63 bytes)
- 12/6/07 Monitor Log** (495K)

5 View the SiteScope Progress Report

You can view the load on the SiteScope server and a list of the most recently run monitors in the SiteScope Progress Report. For details on the user interface, see “SiteScope Progress Report Page” on page 407.

Example

The screenshot shows the SiteScope Progress Report page. At the top, there are navigation tabs: Dashboard, Contents, Log Files, and Progress. The main heading is "SiteScope Progress Report".

Monitoring Load

	Monitors Run Per Minute	Monitors Running	Monitors Waiting
Current	2	0	0
Maximum	2.1 at 1:02 PM 11/15/07	3 at 2:40 PM 11/15/07	2 at 12:33 PM 11/15/07

Maximums are since last startup at 3:23 PM 11/15/07

Recent Monitors

Date	Group	Monitor	Status
3:23 PM 11/15/07	Health	will update monitor Monitor Load Checker	in 35 seconds
3:13 PM 11/15/07	Health	BAC Integration Statistics	good, Currently logging to Business Availability Center 0 metrics/minute
3:13 PM 11/15/07	Health	Monitor Load Checker	good, Current Monitors Run Per Minute 1.8, Current Monitors Running 1, Current Monitors Waiting 0, Maximum Monitors Run Per Minute 2.1 1:02 PM 11/15/07, Maximum Monitors Running 3 2:40 PM 11/15/07, Maximum Monitors Waiting 2 12:33 PM 11/15/07
3:14 PM 11/15/07	doc	memory	good, 65% used, 613MB free, 46.00233 pages/sec
3:15 PM 11/15/07	Health	Monitor Load Checker	good, Current Monitors Run Per Minute 2.0, Current Monitors Running 2, Current Monitors Waiting 1, Maximum Monitors Run Per Minute 2.1 1:02 PM 11/15/07, Maximum Monitors Running 3 2:40 PM 11/15/07, Maximum Monitors Waiting 2 12:33 PM 11/15/07

Deploy SiteScope Health Monitors

This task describes how to deploy SiteScope Health monitors to a SiteScope installation if the monitors were not present when you imported a SiteScope to System Availability Management in HP Business Availability Center.

To deploy SiteScope Health Monitors:

- 1 Open the SiteScope container to which you want to display the Health Monitors. Confirm that the SiteScope includes the Health monitor group container.

Note: The Health monitor group container is identified with a health indicator  icon.

- 2 Expand the **Health Templates** container in the monitor tree, and select the Health monitor template for the operating system on which the SiteScope you want to monitor is running. The choices are:
 - ▶ UNIX Health Monitors
 - ▶ Windows Health Monitors
- 3 Right-click the template icon and select **Copy** from the action menu.
- 4 Right-click the **Health** monitor group container of the SiteScope to which you want to deploy the Health monitors and select **Paste**. The monitors in the selected template are then configured and deployed to the selected SiteScope server.

Configure the Audit Log

This task describes the steps involved in configuring the maximum size of the audit log.

To configure the audit log:

- 1** Open the **log4j.properties** file located in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** directory.
- 2** Set **MaxFileSize** to the maximum number of lines in the log.
- 3** Set **MaxBackupIndex** to the maximum number of backup audit logs to be kept before the oldest audit log is deleted.

For example, if **MaxBackupIndex** is 5, no more than 5 backup audit logs are kept. If 5 backup log files exist, then after the current **audit.log** file reaches **MaxFileSize** size, **audit.log.5** is deleted, **audit.log.4** is renamed to **audit.log.5**, **audit.log.3** to **audit.log.4** and so forth. The current **audit.log** is renamed **audit.log.1** and a new **audit.log** is created.

SiteScope Log File Columns

When SiteScope runs a monitor instruction to test the availability of components in the infrastructure, the monitor results are written to data log files. The first six columns of each log entry in a SiteScope monitor data log are the same for each monitor type. After the first six columns of each log entry, the content of each column is specific for each monitor type.

The following table describes the content of these columns. The columns in each log file are written as tab-delimited text.

Column	Data in Column
1	Time and date the sample was recorded.
2	Category (for example, good, error, warning, nodata).
3	Monitor group name where the monitor defined (also called ownerID).
4	Monitor title text.
5	stateString (this is the status string that shows up on the Monitor Group Detail Page).
6	id:sample number (a unique ID for this monitor where group + id is a unique key for a monitor). The sample number is a unique sample number for that monitor.

Audit Log Entries

Each line of the audit log describes an operation performed in SiteScope.

This section includes the following:

- “SiteScope Startup” on page 385
- “Group Operations” on page 385
- “Monitor Operations” on page 386
- “Update to General Preferences” on page 386
- “Update to Other Preferences” on page 387
- “Applying Templates” on page 388
- “Template Containers” on page 388
- “Create, Delete, Modify Templates” on page 389
- “Template Variables” on page 389
- “Template Groups” on page 390
- “Template Remote Objects” on page 390
- “Template Alerts” on page 391
- “Template Monitors” on page 391
- “Alerts” on page 392
- “Reports” on page 392
- “Global Search and Replace Operations” on page 393
- “Login-Logout” on page 393
- “Failed Login” on page 393
- “Changed Password” on page 394
- “Categories” on page 394

SiteScope Startup

When SiteScope is restarted, its entry is:

```
YYYY-MM-DD HH:MM:SS - SiteScope Audit Log initialized
```

Group Operations

Operations performed on groups have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Group  
'<group_name>' '<operation>' '<container>'
```

where:

- ▶ **<group_name>** is the name of the group that was operated on.
- ▶ **<operation>** can be one of the following:
 - ▶ **Created In.** The location where the group was created.
 - ▶ **Updated in.** The location where the group's information was updated.
 - ▶ **Deleted From.** The location from where the group was deleted.
 - ▶ **Pasted On.** The user copied information from one group to another.
- ▶ **<container>** is the name of the group container that was operated on.

Monitor Operations

Operations performed on monitors have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Monitor  
'<monitor_name>' '<operation>' '<container>'
```

- **<monitor_name>** is the name of the monitor that was operated on.
- **<operation>** can be one of the following:
 - **Created In.** The location where the user created a monitor.
 - **Updated in.** The location from where the user updated a monitor's information.
 - **Deleted From.** The location where the user deleted a monitor.
 - **Pasted On.** The user copied information from one monitor to another.
- **<container>** is the name of the container.

Update to General Preferences

Changes made in **General Preferences** under the **Preferences** container in the monitor tree have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed:  
'<preferences_name>' updated
```

where **<preferences_name>** is the name of the preference that was changed.

The nature of the change to the preference is not in the log.

Update to Other Preferences

Changes to preferences other than those listed in **General Preferences** in the monitor tree have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed:  
'<preferences_name>' named '<object_name>' '<operation>'
```

- **<preferences_name>** is the name of the preference.
- **<object_name>** is the name of the object to which the preference refers.
- **<operation>** can be one of the following:
 - **Updated.** The user changed the preference.
 - **Deleted.** The user deleted the preference.

This format is used for the following types of preferences:

- Microsoft Windows Remote Preferences
- UNIX Remote Preferences
- Mail Preferences
- Pager Preferences
- SNMP Preferences
- Absolute Schedule Preferences
- Range Schedule Preferences
- User Preferences

Applying Templates

When an entity is created by deploying a template, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Configuration  
Template '<template_name>' pasted on '<group_name>'
```

- ▶ **<template_name>** is the name of the template from which the entity was created.
- ▶ **<group_name>** is the name of the group that contains the entity that was created from the template.

Note: To see which entities were created by deploying the template, look at the contents of template itself. Information about entities is not included in the audit log.

Template Containers

When a template container is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template  
Container '<container_name>' '<operation>' '<container>'
```

- ▶ **<container_name>** is the name of the template container that was either created, deleted, or updated.
- ▶ **<operation>** can be one of the following:
 - ▶ **Created in.** The location where the user created the template container.
 - ▶ **Deleted from.** The location from where the user deleted the template container.
 - ▶ **Updated in.** The location where the user changed the template container.
- ▶ **<container>** is the name of the container containing the template.

Create, Delete, Modify Templates

When a template is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
'<template_name>' '<operation>' '<container>'
```

- ▶ **<template_name>** is the name of the template that was either created, deleted, or updated.
- ▶ **<operation>** can be one of the following:
 - ▶ **Created in.** The location where the user created the template.
 - ▶ **Deleted from.** The location from where the user deleted the template.
 - ▶ **Updated in.** The location where the user changed the template.
- ▶ **<container>** is the name of the container containing the template.

Template Variables

When a template variable related to an object, such as server ID, is created, deleted, or updated in a container, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
Variable '<variable_name>' '<operation>' '<container>'
```

- ▶ **<variable_name>** is the name of the variable that was either created, deleted, or updated.
- ▶ **<operation>** can be one of the following:
 - ▶ **Created in.** The location where the template variable for the object was created.
 - ▶ **Deleted from.** The location where the template variable for the object was deleted.
 - ▶ **Updated in.** The location where the template variable for the object was updated.
- ▶ **<container>** is the name of the container containing the template variable.

Template Groups

When a template group for a specific type of object is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template Group
'<group_name>' '<operation>' '<container>'
```

- ▶ **<group_name>** is the name of the template group created, updated or deleted.
- ▶ **<operation>** can be one of the following:
 - ▶ **Created in.** The location where the template group for the object was created.
 - ▶ **Deleted from.** The location from where the template group for the object was deleted.
 - ▶ **Updated in.** The location where template for the object was updated.
- ▶ **<container>** is the name of the container containing the template group.

Template Remote Objects

When a template remote server is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
Remote '<remote_name>' '<operation>' '<container>'
```

- ▶ **<remote_name>** is the name of the remote server.
- ▶ **<operation>** can be one of the following:
 - ▶ **Created in.** The location where the remote entity was created.
 - ▶ **Deleted from.** The location from where the remote entity was deleted.
 - ▶ **Updated in.** The location where the remote entity was updated.
- ▶ **<container>** is the name of the container containing the remote entity.

Template Alerts

When a template for an alert is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template Alert
'<alert_name>' '<operation>' '<container>'
```

- **<alert_name>** is the name of the object for which the template alert is defined.
- **<operation>** can be one of the following:
 - **Created in.** The location where the template alert was created.
 - **Deleted from.** The location from where the template alert was deleted.
 - **Updated in.** The location where the template alert was updated.
- **<container>** is the name of the template container.

Template Monitors

When a template for a monitor is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
'<monitor_name>' '<operation>' '<container>'
```

- **<monitor_name>** is the name of the monitor.
- **<operation>** can be one of the following:
 - **Created in.** The location where the template for the monitor was created.
 - **Deleted from.** The location from where the template for the monitor was deleted.
 - **Updated in.** The location where the template for the monitor was updated.
- **<container>** is the name of the container containing the template.

Alerts

Operations performed on alerts are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Alert  
'<alert_name>' '<operation>' '<container>'
```

- **<alert_name>** is the name of the alert.
- **<operation>** can be one of the following:
 - **Created In.** The location where the new alert was created.
 - **Updated in.** The location where the new alert was updated.
 - **Deleted From.** The location from where the new alert was deleted.
 - **Pasted On.** The user copied information from one alert to another.
- **<container >** is the container of the alert.

Reports

Operations performed on report definitions are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Report  
'<report_name>' '<operation>' '<container>'
```

- **<report_name>** is the name of the report.
- **<operation>** can be one of the following:
 - **Created In.** The location where a new report was created.
 - **Updated in.** The location where a new report was updated.
 - **Deleted From.** The location from where a new report was deleted.
 - **Pasted On.** The information was copied from one report to another.
- **<container >**. The container of the report.

Global Search and Replace Operations

Global Search and Replace operations are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: GSAR operation
started
-----
YYYY-MM-DD HH:MM:SS -Global Replace updated group '<group_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated report '<report_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated monitor '<monitor_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated alert '<alert_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated preference '<preference_name>'
-----
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: GSAR operation
finished
```

Start and end operations always appear in the log. The entries appear depending on the actions performed by the Global Search and Replace.

Login-Logout

Login and logout are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: <message>
```

where <message> is either:

- Logged in.
- Logged out.

Failed Login

Failed login attempts are in the format:

```
YYYY-MM-DD HH:MM:SS - Username and password do not match. Failed to login.
```

Changed Password

Password operations are logged and appear in the following format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: <message>
```

where **<message>** is either:

- ▶ Changed password successfully.
- ▶ Failed to change password.

Categories

Operations performed on categories are logged and appear in the following format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Category  
'<category_name>' '<operation>'
```

- ▶ **<category_name>** is the name of the category.
- ▶ **<operation>** can be one of the following:
 - ▶ **Created.** The location where a new category was created.
 - ▶ **Updated.** The location where a new category was updated.
 - ▶ **Deleted.** The location from where a new category was deleted.

SiteScope Health User Interface

This section describes:

- ▶ BAC Integration Statistics Monitor Page on page 395
- ▶ Log Event Health Monitor Page on page 396
- ▶ Monitor Load Monitor Page on page 399
- ▶ Health of SiteScope Server Monitor Page on page 400
- ▶ Log Files Page on page 404

► SiteScope Progress Report Page on page 407

BAC Integration Statistics Monitor Page

Description	Enables you to check the volume of traffic between SiteScope and HP Business Availability Center. To access: Expand Health in the monitor tree and click BAC Integration Statistics .
Important Information	Monitor data is available only if SiteScope is integrated as a data collector for Business Availability Center.
Useful Links	“BAC Integration Statistics Monitor” on page 367

The following elements are included:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	The name of the Business Availability Center Integration Statistics monitor. Default value: BAC Integration Statistics
Frequency	Set how often SiteScope attempts to run the BAC Integration Statistics monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days. Default value: 100 seconds
Counters	Currently logging to Business Availability Center. Shows the amount of metrics currently logging per minute to HP Business Availability Center.

 **Log Event Health Monitor Page**

Description	<p>Enables you to monitor the local SiteScope installation error.log file for certain events. These events include log entries indicating that a monitor has been skipped or there was a problem in reporting data to another application.</p> <p>To access: Expand Health in the monitor tree and click Log Event Checker.</p>
Important Information	<p>Only the first 15 selected counters are configured and monitored. A maximum of 10 measurements can be used as status threshold criteria for alerting.</p>
Included in Tasks	<p>“Analyze SiteScope Health Monitor Data” on page 376</p>
Useful Links	<p>“SiteScope Log Events Monitor” on page 368</p>

The following elements are included:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	The name of the SiteScope Health monitor. Default value: Log Event Checker
Frequency	Set how often SiteScope attempts to run the Log Event Health monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days. Default value: 10 minutes
Counters	<ul style="list-style-type: none"> ▶ skipped #1. A monitor has skipped its scheduled run once. ▶ skipped #2. A monitor has skipped its scheduled run two times. ▶ skipped #3. A monitor has skipped its scheduled run three times. ▶ skipped #4. A monitor has skipped its scheduled run four times. ▶ skipped #5. A monitor has skipped its scheduled run five times. ▶ SiteScope is shutting down. SiteScope has been shut down. ▶ Reached the limit of processes in the process pool. The number of processes requested from the process pool exceeds the number of processes available in the pool. ▶ Error. data reporter failed to report chunk of data. There was a fault in the transfer of SiteScope monitor measurement data to HP Business Availability Center.

GUI Element	Description
<p>Counters</p>	<ul style="list-style-type: none"> ▶ Error. config reporter failed to report chunk of data. There was a fault in the transfer of SiteScope configuration data to HP Business Availability Center System Availability Management. ▶ Error. Topaz failed to process data. HP Business Availability Center reported a fault in processing data sent from SiteScope. ▶ Error. CacheSender. Got to the max number of cached files. SiteScope has reached the maximum number of cached data file awaiting transfer to HP Business Availability Center. This may occur if data transfer between SiteScope and HP Business Availability Center has been interrupted. ▶ Error. CacheSender. Got to the max old dir size. SiteScope has reached the maximum directory size for cached data file awaiting transfer to HP Business Availability Center. This may occur if data transfer between SiteScope and HP Business Availability Center has been interrupted. ▶ Topaz SEVERE. HP Business Availability Center reported a data transfer or processing fault with a status of SEVERE. ▶ Commit verification failed. ▶ Error loading monitor. ▶ Error contacting mirror server. ▶ Error: open SSH connections limit reached.

Monitor Load Monitor Page

Description	Enables you to check several SiteScope load statistics reported by the Progress Report for the local SiteScope installation. To access: Expand Health in the monitor tree and click Monitor Load Checker .
Important Information	Only the first 15 selected counters are configured and monitored. A maximum of 10 measurements can be used as status threshold criteria for alerting.
Included in Tasks	“Analyze SiteScope Health Monitor Data” on page 376
Useful Links	“SiteScope Monitor Load Monitor” on page 370

The following elements are included:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	The name of the SiteScope Health monitor. Default value: Monitor Load Checker
Frequency	Set how often SiteScope attempts to run the Monitor Load monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days. Default value: 100 seconds
Counters	<ul style="list-style-type: none"> ▶ Current Monitors Run Per Minute ▶ Current Monitors Running ▶ Current Monitors Waiting ▶ Maximum Monitors Run Per Minute ▶ Maximum Monitors Running ▶ Maximum Monitors Waiting

Health of SiteScope Server Monitor Page

Description	Enables you to check the SiteScope server resource and process statistics for the local SiteScope installation. To access: Expand Health in the monitor tree and click Health of SiteScope Server .
Important Information	Only the first 15 selected counters are configured and monitored. A maximum of 10 measurements can be used as status threshold criteria for alerting.
Included in Tasks	“Analyze SiteScope Health Monitor Data” on page 376
Useful Links	“SiteScope Server Health Monitor” on page 370

The following elements are included:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	The name of the SiteScope Health monitor. Default value: Health of SiteScope Server
Frequency	Set how often SiteScope attempts to run the Monitor Load monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days. Default value: 5 minutes

GUI Element	Description
Counters (on UNIX)	<ul style="list-style-type: none"> ➤ Used Disk Space on SiteScope Drive ➤ MegaBytes Available on SiteScope Drive ➤ Used Disk Space on / ➤ MegaBytes Available on / ➤ Disk Blocks Written/sec ➤ Disk Blocks Read/sec ➤ Physical Memory Free ➤ Physical Memory Free Megabytes ➤ Swap Free,Swap Free Megabytes ➤ Load Avg 5min ➤ SiteScope Process Memory ➤ SiteScope Process Thread Count ➤ SiteScope Process Handle Count ➤ Average CPU ➤ PageIns/sec ➤ PageOuts/sec ➤ SwapIns/sec ➤ SwapOuts/sec ➤ ContextSwitches/sec ➤ Net_TotalPacketsIn/sec ➤ Net_TotalPacketsOut/sec ➤ Net_TotalCollisions/sec

GUI Element	Description
<p>Counters (on Windows)</p>	<p>skipped #1</p> <ul style="list-style-type: none"> ➤ A monitor has skipped its scheduled run once <p>Memory</p> <ul style="list-style-type: none"> ➤ Page Faults/sec ➤ Pool Paged Bytes ➤ Pool Nonpaged Bytes ➤ % Committed Bytes In Use ➤ Available MBytes <p>System</p> <ul style="list-style-type: none"> ➤ Context Switches/sec ➤ File Data Operations/sec ➤ System Up Time ➤ Processor Queue Length ➤ Processes ➤ Threads <p>Processor</p> <ul style="list-style-type: none"> ➤ _Total <ul style="list-style-type: none"> ➤ % Processor Time ➤ % DPC Time <p>Process</p> <ul style="list-style-type: none"> ➤ java <ul style="list-style-type: none"> ➤ Thread Count ➤ Pool Paged Bytes ➤ Pool Nonpaged Bytes ➤ Handle Count <p>Process</p> <ul style="list-style-type: none"> ➤ perfex <ul style="list-style-type: none"> ➤ % Processor Time ➤ Thread Count ➤ Pool Paged Bytes ➤ Pool Nonpaged Bytes ➤ Handle Count

GUI Element	Description
Counters (on Windows)	<p>Network Interface</p> <ul style="list-style-type: none"> ➤ MS TCP Loopback interface <ul style="list-style-type: none"> ➤ Bytes Total/sec ➤ Current Bandwidth ➤ Bytes Received/sec ➤ Bytes Sent/sec ➤ <Ethernet_hardware> (hardware specific to the particular SiteScope server) ➤ Bytes Total/sec ➤ Current Bandwidth ➤ Bytes Received/sec ➤ Bytes Sent/sec <p>LogicalDisk</p> <ul style="list-style-type: none"> ➤ <logical_drive> (hardware specific to the particular SiteScope server) <ul style="list-style-type: none"> ➤ % Free Space ➤ Free Megabytes ➤ Avg. Disk Bytes/Transfer ➤ _Total <ul style="list-style-type: none"> ➤ % Free Space ➤ Free Megabytes ➤ Avg. Disk Bytes/Transfer <p>PhysicalDisk</p> <ul style="list-style-type: none"> ➤ _Total <ul style="list-style-type: none"> ➤ Current Disk Queue Length ➤ Disk Transfers/sec ➤ <physical_disk(s)> (hardware specific to the particular SiteScope server) <ul style="list-style-type: none"> ➤ Current Disk Queue Length ➤ Disk Transfers/sec

GUI Element	Description
Counters (on Windows)	<p>Server</p> <ul style="list-style-type: none"> ▶ Bytes Total/sec ▶ Errors Logon ▶ Errors Access Permissions ▶ Errors System ▶ Files Open ▶ Server Sessions

Log Files Page

Description	<p>Enables you to inspect the SiteScope log files.</p> <p>To access: Click Health in the monitor tree, and click the Log Files tab.</p>
Important Information	<p>The Log Files tab is available only on the SiteScope root node and for the Health container in the monitor tree.</p>
Included in Tasks	<p>“Analyze SiteScope Health Monitor Data” on page 376</p> <p>“Configure the Audit Log” on page 382</p>
Useful Links	<p>“Using Log Files” on page 371</p> <p>“SiteScope Log File Columns” on page 383</p> <p>“Audit Log Entries” on page 384</p> <p>“Audit Log Limitations” on page 409</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Alert Log	Records alert information whenever SiteScope generates an alert. This can be used to troubleshoot alert actions and to confirm that alerts were sent.
Error Log	Contains a variety of messages relating to the operation of SiteScope. This includes a record of errors that SiteScope may have encountered when trying to perform monitor actions or data communication actions. It also includes messages indicating when SiteScope was stopped or started and if there are monitors that are skipping because they are unable to complete their task.
Run Monitor Log	Records information when specific monitor runs and some actions related to managing monitors. This can be useful in troubleshooting monitors.
HP Business Availability Center Log	Contains information about connectivity and monitor data transfer when SiteScope is configured to report to HP Business Availability Center.
Post Log File	An optional log file used to record HTTP Post requests made to the SiteScope server. This can be used to track administrative actions performed. This log is only enabled when the <code>_postLogFile=true</code> setting exists in the master.config file.
URL Details	An optional log file used to record the complete contents of HTTP and HTTPS requests made by SiteScope URL monitor types. This can be used to troubleshoot URL and URL Sequence monitor types. This log is only enabled when the <code>_urlDetailLogEnabled=true</code> setting exists in the master.config file. This can be used selectively by adding the <code>_urlDetailLogEnabled=true</code> setting into an individual monitor group configuration file that contains a URL monitor type.

GUI Element	Description
Operator Log	An optional log file used to record SiteScope operator actions, primarily information from use of the Acknowledgement function. This log is created when an acknowledgement is added to one or more monitors.
Audit Log	This section contains links to the logs containing all configuration changes that were performed, such as creation of monitors, templates, alerts and so on. For details on audit logs, see “Using the Audit Log” on page 372.
Date Coded Monitor logs	<p>This section contains links to the logs containing individual monitor measurements. SiteScope creates a new monitor log each day to record all monitors run during that 24 hour period. These logs are the basis for SiteScope Reports.</p> <p>Note: The monitor logs can become very large depending on the monitor environment. This may make it impractical to view them using a Web browser.</p>

SiteScope Progress Report Page

The following is an example of the SiteScope Progress report.

Dashboard Contents Log Files **Progress**

SiteScope Progress Report

Monitoring Load

	Monitors Run Per Minute	Monitors Running	Monitors Waiting
Current	2	0	0
Maximum	2.1 at 1:02 PM 11/15/07	3 at 2:40 PM 11/15/07	2 at 12:33 PM 11/15/07

Maximums are since last startup at 3:23 PM 11/15/07

Recent Monitors

Date	Group	Monitor	Status
3:23 PM 11/15/07	Health	will update monitor Monitor Load Checker	in 35 seconds
3:13 PM 11/15/07	Health	BAC Integration Statistics	good, Currently logging to Business Availability Center 0 metrics/minute
3:13 PM 11/15/07	Health	Monitor Load Checker	good, Current Monitors Run Per Minute 1.8, Current Monitors Running 1, Current Monitors Waiting 0, Maximum Monitors Run Per Minute 2.1 1:02 PM 11/15/07, Maximum Monitors Running 3 2:40 PM 11/15/07, Maximum Monitors Waiting 2 12:33 PM 11/15/07
3:14 PM 11/15/07	doc	memory	good, 65% used, 613MB free, 46.00233 pages/sec
3:15 PM 11/15/07	Health	Monitor Load Checker	good, Current Monitors Run Per Minute 2.0, Current Monitors Running 2, Current Monitors Waiting 1, Maximum Monitors Run Per Minute 2.1 1:02 PM 11/15/07, Maximum Monitors Running 3 2:40 PM 11/15/07, Maximum Monitors Waiting 2 12:33 PM 11/15/07

Description	<p>Enables you to view an overview of several key SiteScope server performance metrics. The Load Measurements table displays the load on the SiteScope server and the Recent Monitors table displays which SiteScope monitors are running, and which monitors have run recently, at what time, and what was the returned status.</p> <p>To access: Click Health in the monitor tree, and click the Progress tab.</p>
Important Information	The Progress tab is available only for the Health container in the monitor tree.

Included in Tasks	“Analyze SiteScope Health Monitor Data” on page 376
Useful Links	“Using the SiteScope Progress Report” on page 373

Report Content - Monitoring Load Table

The following elements are included (unlabeled GUI elements are shown in angle brackets). For each statistic, the current and maximum values are displayed.

Parameter	Description
Monitors Run Per Minute	This is a rolling average of the last 10 minutes of monitoring, and tracks the rate (per minute) at which monitors are being run.
Monitors Running	This number represents the number of monitors queued for execution, based on their update frequency or schedule, that currently have execution threads. This means they are being run.
Monitors Waiting	This measurement is the complement of the Monitors Running measurement representing the number of monitors queued for execution, based on their update frequency or schedule, that currently are awaiting execution threads. This means they are not being run.

Report Content - Recent Monitors Table

The following elements are included (unlabeled GUI elements are shown in angle brackets):

Parameter	Description
Date	The date and time the monitor ran.
Group	The group to which the monitor belongs.

Parameter	Description
Monitor	The name of the monitor that SiteScope ran.
Status	The status returned by the monitor.
<The first monitors in the list displayed in bold text>	The monitors that are currently being run.
<Monitors displayed below the blank row divider>	The monitors that have most recently completed running.

Troubleshooting and Limitations

Audit Log Limitations

- ▶ Audit log entries can only be created in English. This means that audit log entries are also displayed only in English, regardless of what language you use to view SiteScope.
- ▶ The following operations are not recorded in the audit log:
 - ▶ When a template is deployed, operations on the various elements in the template are not logged.

For example, you deployed a template that created group MM2_Servers with monitors in the new group. The audit log entry is:

Operation performed: Configuration Template 'MM2' pasted on 'MM2_Servers'.

Note that there are no entries in the audit log about creation of monitors in MM2_Servers group.

- ▶ Attaching and detaching SiteScope to HP Business Availability Center are not logged.

When SiteScope is attached to Monitor Administration in HP Business Availability Center, the actions you perform on SiteScope appear in HP Business Availability Center's audit log and not in SiteScope's audit log.

- ▶ Group configurations that were made by using a <group name>.mg file are not recorded in the audit log. Only group changes made through the monitor tree are recorded in the audit log.

When you create a group in the monitor tree, a <group name>.mg file with all the configuration changes for the group is automatically created for that group. This means that you can configure a group through the monitor tree or by changing its mg file.

Part IV

SiteScope Dashboard

12

Working with SiteScope Dashboard

This chapter includes the main concepts, tasks, and reference information for SiteScope Dashboard.

This chapter includes:

Concepts

- ▶ SiteScope Dashboard Overview on page 414
- ▶ Dashboard Filter Overview on page 415
- ▶ Generating a Server-Centric Report on page 416
- ▶ Acknowledging Monitor Status on page 417
- ▶ Accessing SiteScope Tools on page 418

Tasks

- ▶ Customize SiteScope Dashboard on page 419
- ▶ Analyze Data in SiteScope Dashboard on page 421
- ▶ Monitor Your Microsoft Windows/UNIX Server's Resources on page 424
- ▶ Create a Server-Centric Report – Scenario on page 426

Reference

- ▶ Server-Centric Report Measurements on page 429
- ▶ SiteScope Dashboard User Interface on page 430

SiteScope Dashboard Overview

SiteScope monitoring provides a real-time picture of system availability and performance. You configure SiteScope monitors to collect metrics from a range of infrastructure components, including Web, application, database, and firewall servers. The status and metrics are then aggregated for presentation in SiteScope Dashboard.

Dashboard is linked to the SiteScope monitor tree hierarchy. The data displayed in Dashboard represents the selected context in the monitor tree. The highest level is the SiteScope node and any applicable monitor groups. The lowest-level element for display in a Dashboard view is an individual SiteScope monitor and its measurements.

Dashboard includes functions that you can use to customize the display of monitor information. This includes defining named filter settings to limit the display of data to those matching a defined criteria. You can also select various data display options.

Dashboard also includes hyperlinks and menus that you can use to navigate through the hierarchy of monitor elements, manually run a monitor, disable monitors, and access alert definitions.

Dashboard Filter Overview

You can filter monitors or groups by the following criteria:

- ▶ monitor or group names containing a specific text string
- ▶ monitors or groups monitoring a specific host or server
- ▶ monitors or groups reporting an error
- ▶ measurement results containing a specific text string

Filters are applied primarily to monitors. The filter criteria are not applied to groups, alerts, or reports. You can use view settings to filter on other elements. For more information, see “Views and Categories” on page 195.

Filters are applied to all Dashboard views. This means that some monitors may not be displayed depending on the filter criteria and the selected node. Generally, it is best to use filters together with the **Show all descendent monitors** view option. Filters remain active until you change or reset the filter criteria in the Dashboard Filter window.

Dashboard filters are separate from SiteScope views. You can use either Dashboard filters or views to filter the display of nodes to specific monitor types. However, Dashboard filters are applied to the results of any currently selected view setting. If a view setting is active, this may prevent the Dashboard filter from finding monitors that match the filter criteria, even if such monitors do exist in the SiteScope environment.

You can save a filter setting by defining the filter settings and then saving the view as a Dashboard Favorite. For more information, see “Defining and Managing View Settings” on page 196.

For details on configuring a Dashboard filter, see “Dashboard Filter Page” on page 433.

Generating a Server-Centric Report

For Microsoft Windows Resources Monitors and UNIX Resources Monitors, you can create a Server-Centric Report which displays data from three different metrics about the server being monitored. It is recommended to use Solution Templates when creating the Microsoft Windows Resources Monitor or UNIX Resources Monitor. For details on the Solution Templates, see:

- “AIX Host Solution Templates” on page 1285
- “Linux Host Solution Templates” on page 1299
- “Solaris Host Solution Templates” on page 1363
- “Microsoft Windows Host Solution Template” on page 1325

You can define the monitor manually by selecting **Enable Server Centric Report** in the required monitor settings page, as described in “Microsoft Windows Resources Monitor Settings” on page 927 and “UNIX Resources Monitor Settings” on page 937. When defining the monitor manually, you must select the required metrics for the monitors, according to the table in “Server-Centric Report Measurements” on page 429.

The report displays the following metrics on the same graph:

- **CPU Utilization.** For UNIX Resource Monitors, this metric is calculated as an average of three counters: system processing utilization, user processing utilization, and input/output processing utilization. For Microsoft Windows Resources Monitors, the metric is calculated as processing capacity used out of total processing capacity.
- **Memory Utilization.** Calculated as memory used out of total available memory.
- **Network Utilization.** Calculated by system-specific counters. Calculating network utilization is supported only for Windows servers.

Each metric is displayed by a separate line of a unique color on the graph. The report enables you to easily make a visible correlation between the different metrics.

The report includes tables listing the top five processes by CPU utilization and memory consumption. You can navigate the graph and change the time of the data displayed in the tables. This enables you to focus in on a problematic period in the graph to locate the processes running at that time. For details on the Server-Centric Report interface, see “Server-Centric Report” on page 440.

The report also includes the Annotation Tool that enables you to annotate a snapshot of the report you are viewing, to highlight important areas. You can save, print, or email an annotation report. For details on the user interface, see “Annotation Tool” on page 1484.

Acknowledging Monitor Status

The acknowledgement function can be used to track resolution of problems that SiteScope detects in your system and network infrastructure. With this function, SiteScope keeps a record of when the problem was acknowledged, what actions have been taken, and by which user.

It also enables you to temporarily disable alerting on the monitors. This is useful to avoid redundant alerts while a problem is being actively addressed. You can also use the acknowledgement function as a simple trouble ticket system when more than one person uses SiteScope to manage system availability.

Note: The acknowledgement function is available only in Dashboard views. The acknowledgement icon is displayed only in Dashboard Detailed views.

You can add an acknowledgement to individual monitors or monitor groups. An acknowledgement added to a monitor applies only to that monitor. Any alert disable condition selected in the acknowledgement applies only to that monitor instance. Acknowledging a group applies the acknowledgement description and alert disable conditions to all monitors within the group. Acknowledgements applied to a group can be edited or deleted individually for monitors in the group.

Only one acknowledgement can be in force for a monitor or group at any given time. Acknowledgement comments and acknowledgement indicators continue to be displayed in the interface until they are deleted, even after any applicable alert disable schedule has expired.

Acknowledgement data and comments are written to a log file on the SiteScope machine. A new log entry is made each time you add, edit, or delete an acknowledgement. After a problem monitor is acknowledged, or the acknowledged status is cleared, you can view the history in the Acknowledge Log. The Acknowledge Log for an item can be viewed even if there is no acknowledgment currently in force.

Accessing SiteScope Tools

SiteScope contains a number of tools that can be used to test the monitoring environment. You can use these tools to query the systems you are monitoring and view detailed results of the action. This may include simply testing network connectivity or verifying login authentication for accessing an external database or service. You can run these tools directly from the Dashboard group and monitor status information area by accessing the menu to the right of the **Name** column for the monitor or group.

For details on the different tools that are available, see “SiteScope Tools Overview” on page 1593.

Note: SiteScope Tools option is only available for individual monitors.

Customize SiteScope Dashboard

This task describes the steps involved in customizing the display and content of SiteScope Dashboard by setting the layout and configuring filters.

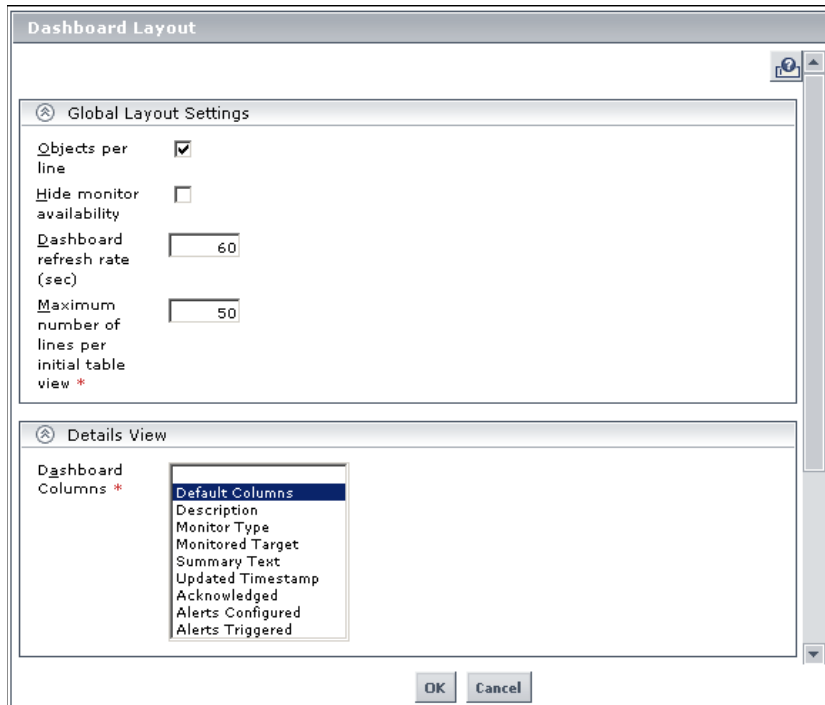
This task includes the following steps:

- “Set the Dashboard Layout” on page 419
- “Select and Set a Dashboard Filter” on page 420

1 Set the Dashboard Layout

Customize the display of group and monitor information using the settings on the Dashboard Layout page. For details on the user interface, see “Dashboard Layout Page” on page 437.

Example



Dashboard Layout

Global Layout Settings

Objects per line

Hide monitor availability

Dashboard refresh rate (sec)

Maximum number of lines per initial table view *

Details View

Dashboard Columns * Default Columns
Description
Monitor Type
Monitored Target
Summary Text
Updated Timestamp
Acknowledged
Alerts Configured
Alerts Triggered

OK Cancel

2 Select and Set a Dashboard Filter

Configure and set a Dashboard filter by selecting from the options available on the Dashboard Filter page. For details on the user interface, see “Dashboard Filter Page” on page 433.

Example

The screenshot shows a 'Dashboard Filter' window with a 'Global Settings' tab. The configuration is as follows:

Monitor Name	monitor1
Monitor Type	SQL Server
Monitored Target	server1
Status	Good, Warning or Error or Data Available
Summary Text	
Acknowledged	Yes
Acknowledgement Notes	
Alerts Configured	Yes
Alerts Triggered	Yes

At the bottom of the window are 'OK' and 'Cancel' buttons.

Analyze Data in SiteScope Dashboard

This task describes the steps to follow to analyze data in SiteScope Dashboard.

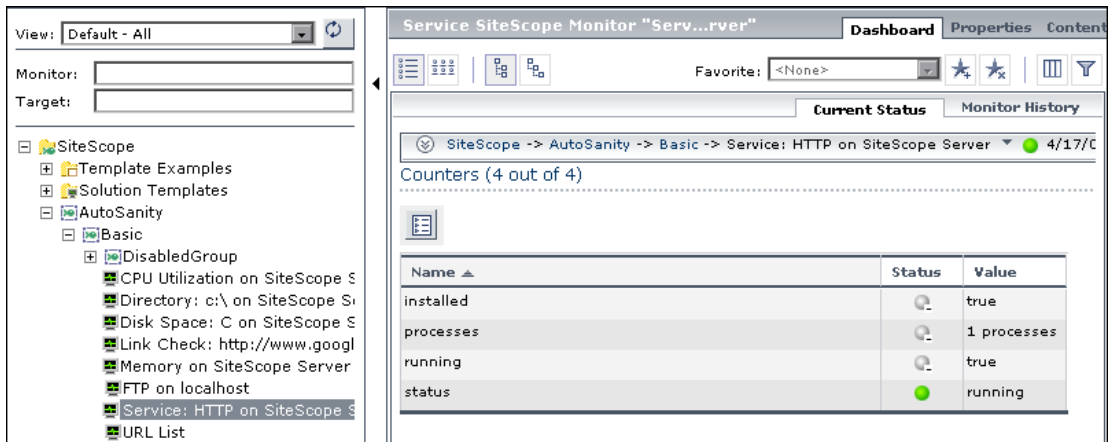
This task includes the following steps:

- ▶ “Drill Down to View Monitor and Measurement Status and Availability” on page 421
- ▶ “View Configured and Triggered Alerts” on page 422
- ▶ “Acknowledge Monitors” on page 423
- ▶ “View Monitor History” on page 423

1 Drill Down to View Monitor and Measurement Status and Availability

When viewing SiteScope data in the Current Status tab of Dashboard, you can drill down in the monitor tree to view monitor and measurement status and availability. For details on navigating in the Dashboard, see “SiteScope Dashboard - Current Status Tab” on page 447.

Example



The screenshot shows the SiteScope Dashboard interface. On the left, a tree view displays the monitor hierarchy: SiteScope > AutoSanity > Basic > DisabledGroup > Service: HTTP on SiteScope Server. The main panel shows the 'Current Status' tab for the selected monitor. The status is '4/17/C' with a green indicator. Below, a table lists counters for the service.

Name	Status	Value
installed		true
processes		1 processes
running		true
status		running

2 View Configured and Triggered Alerts

You can view data about alerts in the configured alerts and triggered alerts columns. If no alerts are configured for a monitor, the alert columns do not appear. For details on the user interface, see “SiteScope Dashboard - Current Status Tab” on page 447.

Example

Name ▾	Type	Target	Status	Summ	Updated	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CPU Utilization on SiteScope Server ▾	CPU	SiteScope Server		12% avg cpu1 8% cpu2 17%	6/6/07 11:10 AM			
Memory on SiteScope Server ▾	Memory	SiteScope Server		13% used 3409M free 0.2666 pages/v	6/6/07 11:11 AM			
FTP on localhost ▾	Port	localhost		0 sec 220	6/6/07 11:11 AM			
URL List ▾	URL List	URLListHost		2 good 0 errors 0 left	6/6/07 10:16 AM			

3 Acknowledge Monitors

To acknowledge monitor status, select **Add Acknowledgement** from the menu in the Name column, and fill in the Acknowledge dialog box. For details on the user interface, see “Acknowledge Dialog Box” on page 430.

Example

Name	Status	Summary	Updated	Alerts	Tools
DisabledGroup	in error	-	-	⚠	
Monitors (8 out of 8)					
CPU Utilization on SiteScope Server	CPU	SiteScope Server 10% avg cpu1 14% cpu2 6%	6/6/07 11:22 AM	⚠	🔊
Memory on SiteScope Server	Memory	SiteScope Server 13% used 2401M	6/6/07 11:23 AM	⚠	

4 View Monitor History

You configure monitor history in the General Preferences container. For details on the user interface, see “Dashboard Monitor History View Options” on page 254.

To view monitor history, click the **Monitor History** tab in SiteScope Dashboard. For details on the user interface, see “SiteScope Dashboard - Monitor History Tab” on page 453.

Example

The screenshot shows the SiteScope Dashboard for a monitor named "cpu on doors". The dashboard includes a breadcrumb trail: SiteScope -> docs -> cpu on doors. Below the breadcrumb, there are navigation controls for "Current Status" and "Monitor History". A table displays the following data:

Run Time	Status	Summary
5/11/08 7:12 AM	● ↑	8% avg, cpu1 7%, cpu2 9%
5/11/08 7:12 AM	● ↑	2% avg, cpu1 3%, cpu2 2%
5/11/08 7:10 AM	● ↑	3% avg, cpu1 3%, cpu2 3%

Monitor Your Microsoft Windows/UNIX Server's Resources

This task describes the steps involved in creating a Microsoft Windows or UNIX Resources Monitor to monitor your Windows or UNIX Server, and generating a Server-Centric report.

For a scenario of this task, see “Create a Server-Centric Report – Scenario” on page 426.

This task includes the following steps:

- ▶ “Create a Windows/UNIX Resources Monitor” on page 425
- ▶ “Generate the Server-Centric Report” on page 425
- ▶ “Analyze Data in the Report” on page 425

1 Create a Windows/UNIX Resources Monitor

To monitor your Windows or UNIX Server, you must create a Microsoft Windows Resources Monitor or UNIX Resources Monitor. It is recommended to do this using Solution Templates.

For details on the Solution Templates, see:

- “Microsoft Windows Host Solution Template” on page 1325
- “AIX Host Solution Templates” on page 1285
- “Linux Host Solution Templates” on page 1299
- “Solaris Host Solution Templates” on page 1363

You can also create a Microsoft Windows Resources monitor or UNIX Resources monitor manually. For details on the Microsoft Windows Resources monitor user interface, see “Microsoft Windows Resources Monitor Settings” on page 927. For details on the UNIX Resource Monitors user interface, see “UNIX Resources Monitor Settings” on page 937. Make sure to select **Enable Server Centric Report** and select the required measurements. For details on the measurements, see “Server-Centric Report Measurements” on page 429.

2 Generate the Server-Centric Report

To monitor your server, navigate to Dashboard, display the data for the applicable Microsoft Windows Resources or UNIX Resources monitor, and click the server name in the **Target** column in the row corresponding to your Windows or UNIX Resources monitor. The Server-Centric Report opens.

3 Analyze Data in the Report

The report enables you to view three different metrics of your server in the same graph – CPU utilization, memory utilization, and network utilization. It also lists the top five processes by CPU utilization and memory consumption. You can drill down to specific times by clicking a data point on the graph. For details on the user interface, see “Server-Centric Report” on page 440.

Create a Server-Centric Report – Scenario

This scenario describes how to create a Server-Centric report.

For a task of this scenario, see “Monitor Your Microsoft Windows/UNIX Server’s Resources” on page 424.

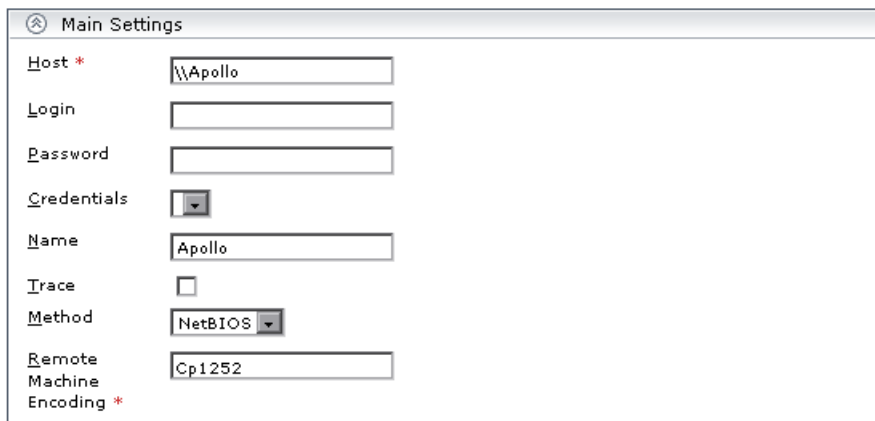
This task includes the following steps:

- ▶ “Configuring a Remote Server” on page 426
- ▶ “Deploying a Microsoft Windows Host Solution Template” on page 427
- ▶ “Creating a Server-Centric Report” on page 428

1 Configuring a Remote Server

David Foster, a SiteScope user at NewSoft Company, wants to create a report that provides data on CPU utilization, memory utilization, and network utilization for a monitored server, Apollo.

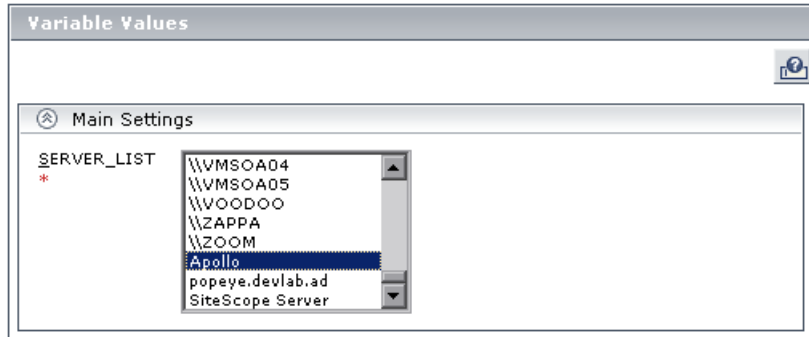
Before he creates the report, David configures SiteScope to monitor the remote Windows server, Apollo, and configures the server in Microsoft Windows Remote Preferences.



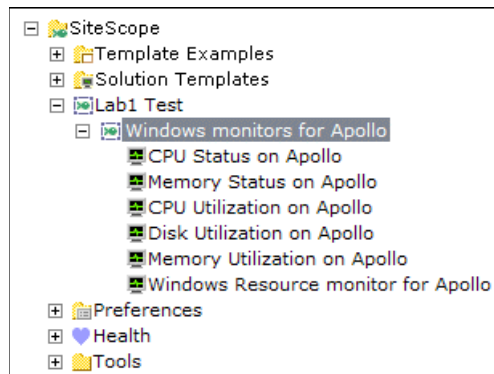
Main Settings	
Host *	\\Apollo
Login	
Password	
Credentials	
Name	Apollo
Trace	<input type="checkbox"/>
Method	NetBIOS
Remote Machine Encoding *	Cp1252

2 Deploying a Microsoft Windows Host Solution Template

After enabling SiteScope to monitor data on Apollo, David deploys the Microsoft Windows Solution Template into the selected group container, and selects Apollo as the server to monitor. David uses the Solution Templates when creating the Microsoft Windows Resource Monitor, because the required monitors and metrics for generating a Server-Centric Report are already configured.



After the solution template is deployed, SiteScope creates a group named Microsoft Windows monitors for Apollo that contains the Microsoft Windows Resources monitor.

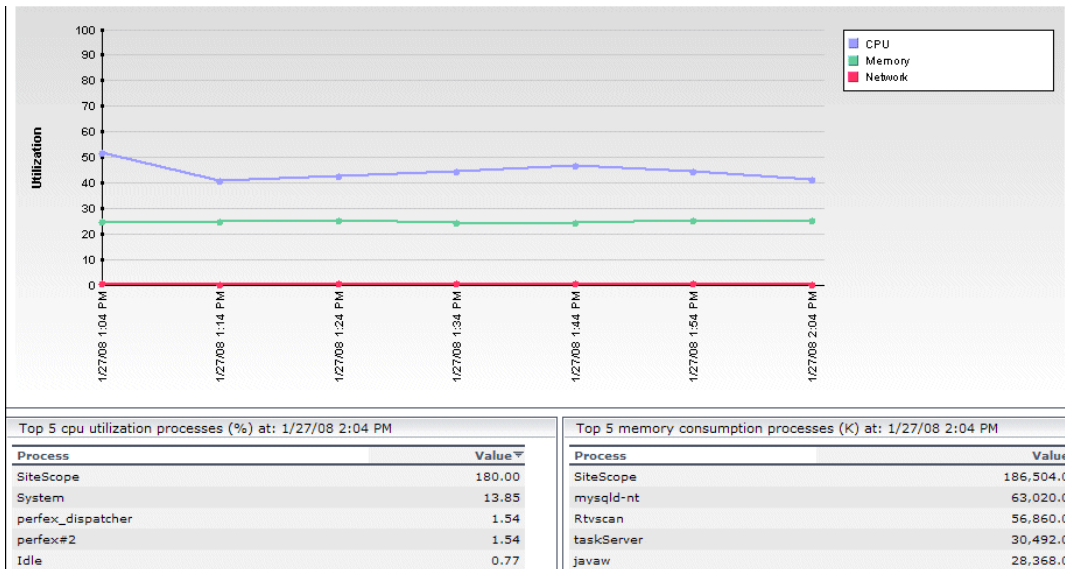


3 Creating a Server-Centric Report

David generates the Server-Centric Report for server Apollo from the Current Status tab of Dashboard.

Name ▲	Type	Target	Status	Summary	Updated	☑	⚠	⚡
CPU Status on Apollo	CPU	Apollo	● ↑	39% avg cpu1 41% cpu2 38%	1/27/08 2:30 PM			
CPU Utilization on Apollo	Windows	Apollo	● ↑	Processor Processor Processor	1/27/08 2:32 PM			
Disk Utilization on Apollo	Windows	Apollo	● ↑	LogicalDis LogicalDis LogicalDis	1/27/08 2:32 PM			
Memory Status on Apollo	Memory	Apollo	● ↑	24% used 3681MB fr 0.00308 p	1/27/08 2:30 PM			
Memory Utilization on Apollo	Windows	Apollo	● ↑	Memory\A	1/27/08 2:32 PM			
Windows Resource monitor for Apollo	Windows	Apollo	● ↑	Processor	1/27/08 2:32 PM			

The Server-Centric Report opens, displaying the CPU Utilization, Memory Utilization, and Network Utilization metrics on the same graph. David can use this data to view the top processes by CPU utilization and memory consumption during different times, and focus in on problematic periods to locate the processes running at that time.



Server-Centric Report Measurements

The following table displays the counters which must be selected when defining the monitor for the Server-Centric Report manually:

OS Type	Server-Centric Mandatory Counters
Counters for Microsoft Windows Resource Monitor	Memory\% Committed Bytes In Use
	Processor_Total\% Processor Time
Counters for UNIX Resource Monitor on Solaris Platform	CPU utilization\%sys
	CPU utilization\%usr
	CPU utilization\%wio
	Memory\swap_avail
	Memory\swap_resv
Counters for UNIX Resource Monitor on AIX Platform	Processor\Total\%sys
	Processor\Total\%usr
	Processor\Total\%wio
Counters for UNIX Resource Monitor on Linux Platform	Memory\MemFree
	Memory\MemTotal
	Processor\Total\System
	Processor\Total\User
	Processor\Total\User low

For details on selecting counters for monitor definition, see “Microsoft Windows Resources Monitor Settings” on page 927 (for Microsoft Windows Resources Monitor counters) and “UNIX Resources Monitor Settings” on page 937 (for Solaris, AIX, and Linux platforms).

SiteScope Dashboard User Interface

This section describes:

- Acknowledge Dialog Box on page 430
- Add Dashboard Favorite Dialog Box on page 432
- Delete Dashboard Favorites Dialog Box on page 433
- Dashboard Filter Page on page 433
- Dashboard Layout Page on page 437
- Server-Centric Report on page 440
- SiteScope Dashboard on page 445
- SiteScope Dashboard - Monitor History Tab on page 453

Acknowledge Dialog Box

Description	Enables you to add or edit an acknowledgement for a monitor. To access: Click the small black arrow in the Name column and select Add Acknowledgement from the menu (for groups).
Included in Tasks	“Analyze Data in SiteScope Dashboard” on page 421
Useful Links	“Acknowledging Monitor Status” on page 417

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Acknowledge Comment	Type an acknowledgement comment which is displayed as a tooltip associated with the acknowledgement icon in the Dashboard view and is recorded in the Acknowledge Log. You can update the comment as new information becomes available. The comment is displayed until the acknowledgement is deleted.
Disable alerts for the next time period	Use this option to disable alerting immediately and to continue suppressing alerting on the selected monitor or group for a duration that you specify.
Disable Description	Type an optional text description for alert icons associated with the monitors in the acknowledged context. The text description is added to the tool tip text that is displayed when the pointer is placed over any alert icon associated with the monitor in the Dashboard view. This text is displayed only while the alert disable option is in force. It is not written to the Acknowledge Log.
Disable on a one-time schedule	Use this option to disable alerting during a period of time that you specify. This can be useful if the system being monitored is expected to be unavailable during a certain period but you want to continue to run the monitor without triggering an alert.
Undo one-time schedule	Cancel a one-time schedule disable alert.
View Acknowledge Log	View all acknowledgement entries for the group from which you invoke the acknowledgement dialog.

Add Dashboard Favorite Dialog Box

Description	Enables you to define combinations of Dashboard filter and layout settings (which were selected using the Dashboard Filter dialog box and the Dashboard Layout dialog box) and save them as a named favorite view. To access: Click the Add Favorite button in Dashboard.
Important Information	Dashboard favorites are limited to settings that are applicable to Dashboard views. This means that Dashboard favorites do not save user-global view settings, or the context that was selected in the monitor tree when the favorite was saved.
Included in Tasks	“Customize SiteScope Dashboard” on page 419
Useful Links	“SiteScope Dashboard Overview” on page 414

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Existing Favorites	A list of the existing favorite views. If you want to replace one of the existing favorites with the current settings, click on the favorite and it appears in the Name box.
Name	Type a display name for the favorite view settings.

Delete Dashboard Favorites Dialog Box

Description	Enables you to delete existing favorite views. To access: Click the Delete Favorites button from Dashboard.
Included in Tasks	“Customize SiteScope Dashboard” on page 419
Useful Links	“SiteScope Dashboard Overview” on page 414


The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Existing Favorites	Select the view or views you want to delete from the list of current favorite views.

Dashboard Filter Page

Description	Enables you to configure a Dashboard filter by entering match criteria and selecting from the menu options. To access: Click the View or edit filter button in Dashboard.
Important Information	Any combination of filter options may be included in a single filter. For example, the filter definition can filter on a combination of Monitor Type , Monitored Target , and Status .
Included in Tasks	“Customize SiteScope Dashboard” on page 419
Useful Links	“Dashboard Filter Overview” on page 415

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click the Show Descriptions button to display additional information about the dialog box elements.
Acknowledged	Use this option to filter monitors based on their Operator Acknowledgement status. To filter on monitors that have been acknowledged, select Yes from the drop-down menu. To filter on unacknowledged monitors, select No from the drop-down menu. Note: The Operator Acknowledgement function is an optional interface functionality that is enabled using the SiteScope General Preferences.
Acknowledgement Notes	Use this option to filter monitors based on text that may appear in their Operator Acknowledgement notes. You can type a literal text string or a regular expression to match a text pattern. For details about regular expressions see “Using Regular Expressions” on page 1493.
Alerts Configured	Use this option to filter monitors based on whether alerts have been configured on them. To filter on monitors that have one or more alerts configured on them, select Yes from the drop-down menu. To filter on monitors that do not have configured alerts, select No from the drop-down menu.
Alerts Triggered	Use this option to filter monitors based on whether they have triggered an alert event. To filter on monitors that have generated one or more alerts, select Yes from the drop-down menu. To filter on monitors that have not generated alerts, select No from the drop-down menu.
Monitored Target	Type the server name to filter monitors based on a particular host or server being monitored.

GUI Element (A-Z)	Description
Monitor Name	Type a text string or regular expression that matches the name of one of more monitors. When you apply this filter to the Dashboard view, only the monitors that match the Monitor Name criterion are displayed.
Monitor Type	Use this list to create a filter to display only selected monitor types.
Status	<p>Use this option to filter monitors by reported status. The status filter criterion can be defined in terms of monitor category status.</p> <p>The following status options are available:</p> <ul style="list-style-type: none"> ▶ Any Status. Show all monitors with any status. This is the default option. This can be used in combination with the Data Available option to filter out monitors that are in error due to connectivity or availability factors. ▶ Good, Warning, or Error. Show all monitors except those reported as disabled. ▶ Error. Show only monitors reporting an error status. ▶ Warning or Error. Show only monitors reporting a warning or error status. ▶ Warning. Show only monitors reporting a warning status. ▶ Warning or Good. Show only monitors reporting a warning or good status. ▶ Good. Show only monitors reporting a good or OK status. ▶ Disabled. Show only monitors reported as disabled. <p>Example: Create a filter that displays only those monitors reporting a warning or error.</p>

GUI Element (A-Z)	Description
<p>Status (with Availability)</p>	<p>Use this option to create a compound filter by combining the monitor status category with the data availability status.</p> <p>The following data availability status options are available:</p> <ul style="list-style-type: none"> ▶ Data Available. Show monitors for which data is available, meaning the monitor was able to retrieve measurements from the target system. ▶ Data Unavailable. Show monitors for which data is not available, meaning SiteScope was not able to retrieve measurements from the target system. <p>Example: Create a filter that displays only those monitors reporting Error and Data Available. This means that the filter shows monitors that indicate an error status for which the monitor was able to receive data from the monitored system as opposed to monitors that are reporting an error because the monitor was not able to communicate with the monitored system (that is, Data Unavailable).</p>
<p>Summary Text</p>	<p>Use this option to filter monitors based on text included in their summary string. You can type a literal text string or a regular expression to match a text pattern.</p> <p>For details about regular expressions see “Using Regular Expressions” on page 1493.</p>


The Monitor History Settings area of the Dashboard Filter dialog box includes the following elements:

GUI Element (A-Z)	Description
Display Time Period	Select the time frame for past events. Default value: Past 1 hour
Monitor Runs per Screen	Type the number of rows of data to display on the screen. Default value: 100
Monitor Run Status	Select the required event status, relational operator, and data availability.

Dashboard Layout Page

Description	You use the Dashboard Layout settings to customize the display of group and monitor data in the Dashboard views. This allows you to enable or suppress the display of monitor measurement details, alert information, and acknowledgement functions. To access: Click the View or edit layout button in Dashboard.
Important Information	Layout options apply only to the Detailed view. They are ignored when using the Icon view.
Included in Tasks	“Customize SiteScope Dashboard” on page 419

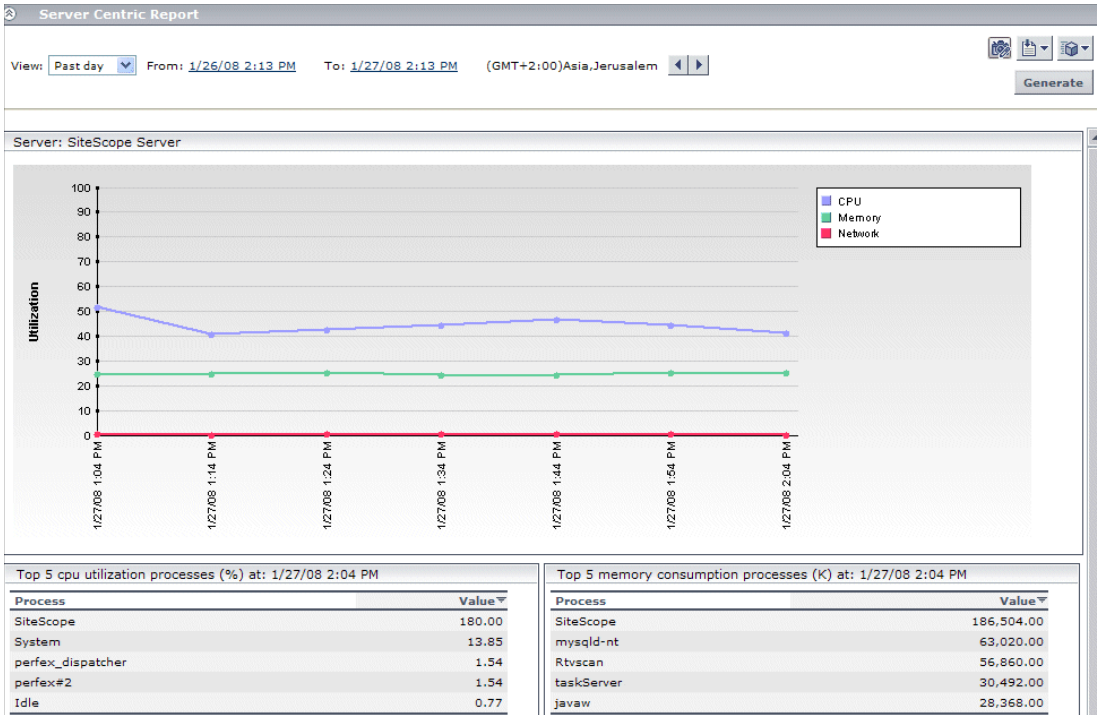
The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	<p>Click the Show Descriptions button to display additional information about the dialog box elements.</p>
<p>Dashboard Columns</p>	<p>You use the Dashboard Columns list to select optional columns to be displayed in the detailed tables. Your selections are applied to all applicable group and monitor elements.</p> <p>The columns available for display are:</p> <ul style="list-style-type: none"> ➤ Description ➤ Monitor Type ➤ Monitored Target ➤ Summary Text ➤ Updated Timestamp ➤ Acknowledged ➤ Alerts Configured ➤ Alerts Triggered <p>Select the Default Columns option to display only the Name and Status columns.</p> <p>For details regarding the optional columns, see “SiteScope Dashboard - Current Status Tab” on page 447.</p>
<p>Dashboard refresh rate (sec)</p>	<p>Use this option to control the Dashboard refresh rate, in seconds. A value significantly less than 30 seconds may have a negative effect on SiteScope performance.</p> <p>Default value: 30 seconds</p> <p>Maximum value: 3600 seconds</p>
<p>Hide monitor availability</p>	<p>Select to hide icons in the Dashboard that indicate whether SiteScope was able to connect to a remote system or if a remote system was unavailable due to a connection problem.</p> <p>Default value: Cleared. Dashboard includes availability icons.</p>

GUI Element (A-Z)	Description
Maximum number of lines per initial table view	Type the maximum number of lines for an initial view in a table. If a view exceeds this maximum, you can go to the next page.
Objects per line	Use this option to restrict the display of monitor elements in Dashboard to a single line. The option affects monitors and groups status or description text requiring more than one text line for display. The default behavior is to display all summary text in multiple lines in the Dashboard view. When this option is enabled, the summary text is truncated to the amount of text that can be displayed on a single line for the applicable field. The full summary text is viewable as a tool tip when a user moves the pointer over the summary field.
Status Icon Tooltip	<p>You can customize the tooltip by selecting the properties to display from the Status Icon Tooltip list.</p> <p>The properties available for display are:</p> <ul style="list-style-type: none"> ▶ Description ▶ Monitor Type ▶ Monitored Target ▶ Summary Text ▶ Updated Timestamp ▶ Acknowledged ▶ Alerts Configured ▶ Alerts Triggered <p>Select the Default option to display only the Name and Status in the tooltip.</p>

Server-Centric Report






The following is an example of the Server-Centric report.



Description	<p>A graphical report showing the metrics CPU utilization, memory utilization, and network utilization for a selected server.</p> <p>To access: Click the server name link in the Target column of SiteScope Dashboard for a Microsoft Windows Resources Monitor or UNIX Resources Monitor.</p>
Important Information	<p>This report is available only on those servers being monitored by a dedicated Microsoft Windows Resources monitor or UNIX Resources monitor created for the purpose of running the report.</p> <p>It is highly recommended to deploy these monitors using the applicable solution templates for these monitors. The templates are preconfigured with the correct measurement counters and options already selected.</p> <p>Note: If a monitor encounters a problem and returns non-applicable data, that data point is skipped. Thus, you may see missing data points in the graph.</p>
Included in Tasks	<p>“Monitor Your Microsoft Windows/UNIX Server’s Resources” on page 424</p>
Useful Links	<p>“Generating a Server-Centric Report” on page 416</p> <p>“Create a Server-Centric Report – Scenario” on page 426</p>

Graph Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Click to create a snapshot of the report you are viewing and highlight important areas of the report by drawing shapes, lines, and adding text to the snapshot. For details on the Annotation Tool user interface, see “Annotation Tool” on page 1484.</p>
	<p>Click to format the report data to a file for exporting. Select the format for the file. The options are printer-friendly, CSV, Excel, or XML.</p>
	<p>Click to export the report data in an E-mail. Select the option for sending the file. The options are HTML mail, HTML attachment, or PDF.</p> <p>Note: To use the export functionality, you must add the SiteScope machine to the trusted sites.</p>
	<p>Click to view the report one time frame earlier than the currently displayed time frame.</p> <p>Tooltip: Back</p> <p>Example: If the value of the View box is Day, clicking this button displays data for one day earlier than the currently displayed report.</p>
	<p>Click to view the report one time frame later than the currently displayed time frame.</p> <p>Tooltip: Forward</p> <p>Example: If the value of the View box is Day, clicking this button displays data for one day later than the currently displayed report.</p>
<p>View</p>	<p>Select a time range for which you want to view the report. Available time ranges include the following:</p> <ul style="list-style-type: none"> ▶ Custom (enables you to configure any range) ▶ Hour, Day, Week ▶ Past hour, Past day, Past week

GUI Element	Description
From/To <date links>	<p>Click the From link to configure a start date and time for the report. Click the To link to configure an end date and time for the report. The calendar contains the following buttons:</p> <ul style="list-style-type: none"> ▶ OK. Updates the date link for the selected date and closes the calendar. ▶ Revert. Returns to the previously selected report date. ▶ Current. Selects today's date in the calendar. ▶ Cancel. Closes the calendar without making any changes.
Generate	Click to create a report for the date range displayed in the date links.

Graph Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):



GUI Element	Description
<Tooltip>	Hold the pointer over any data point on the graph to display a tooltip showing the value at the selected time of the utilization for the selected metric, as well as the date and time.
Server name	The name of the server appears above the Utilization graph.







GUI Element	Description
Utilization graph	<p>A graph displaying utilization over time. The different colored lines represent CPU utilization, memory utilization, and network utilization. All three metrics are scaled as percents (that is, out of 100% utilization).</p> <p>You can click on a data point in the graph to focus in on a shorter timer range. The data tables are updated to show results for the time of the data point you selected (clicking any of the three data points for the same time updates the report in the same way). This is useful when you notice a point with particularly high utilization. By clicking on the point, you can determine the cause of the high utilization.</p> <p>Note: Network utilization is supported for Windows servers only.</p>
Top 5 CPU Utilization Processes table	<p>A table displaying the top five processes in terms of CPU utilization at any point in the graph. The table displays the process name and the CPU utilization value as a percent of total available CPU processing potential.</p>
Top 5 Memory Consumption Processes table	<p>A table displaying the top five processes in terms of memory consumption at any point in the graph. The table displays the process name and the memory consumption value in kilobytes.</p>

SiteScope Dashboard

Description	<p>Displays current performance data for the infrastructure elements being monitored by SiteScope and provides access to functions you use to define filters, layout options, and other view customizations.</p> <p>You can use the functions in Dashboard to access individual monitor information by navigating or drilling down the group and monitor hierarchy.</p> <p>To access: Select an object in the monitor tree and click the Dashboard tab in the right pane.</p>
Important Information	<p>From the Dashboard, you can access the following SiteScope functions:</p> <ul style="list-style-type: none"> ▶ Server-Centric Report ▶ Acknowledge Monitor Status ▶ Monitor Tools ▶ SiteScope Health Status ▶ Monitor History Information
Included in Tasks	“Analyze Data in SiteScope Dashboard” on page 421
Useful Links	“SiteScope Dashboard Overview” on page 414

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Detailed view displays groups and monitors in tabular list format with the element name, status, and other information arranged in individual table rows.
	Icon view displays groups and monitors as an array of status icons with the name of the element below the icon.


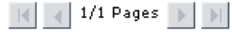



GUI Element	Description
	<p>Show child groups and monitors displays only those elements that are direct children of the selected node. Subgroups and monitors are displayed in separate sections in the group and monitor status information area.</p>
	<p>Show all descendent monitors displays all descendent nodes of the selected node. In combination with the Detailed view option, monitors are displayed in areas divided by group context submenus that provide the path to the applicable groups. In combination with the Icon view option, only descendent monitor icons and names are displayed.</p>
	<p>Click the Add Favorite button to open the Add Dashboard Favorite dialog box which enables you to save the current Dashboard filter and layout settings as a favorite view.</p>
	<p>Click the Delete Favorites button to open the Delete Dashboard Favorites dialog box which enables you to delete existing favorite views.</p>
	<p>Click the View or edit layout button to open the Dashboard Layout page which enables you to customize the Dashboard display. For details, see “Dashboard Layout Page” on page 437.</p>
	<p>Click the View or edit filter button to open the Dashboard Filter page. For details, see “Dashboard Filter Page” on page 433.</p>

GUI Element	Description
Favorite	The Favorite box contains a drop-down list of the existing favorite views of Dashboard filter and layout settings. You can select the one you want to display in the detailed view.
<Table Header path>	<p>Enables you to see the position of the currently displayed view in the SiteScope hierarchy and to navigate to parent nodes using the paths displayed. The path can be expanded by clicking the icon on the left end of the path to show additional details about the current node or element, including acknowledgement data for the group.</p> <p>Clicking the down arrow on the Path opens an alert link menu for the context that enables you to add/delete acknowledgements, edit settings, enable/disable alerts or monitors, or to run monitors.</p> <p>Clicking the alert icon enables you to view the configured alerts for the group or container.</p>

SiteScope Dashboard - Current Status Tab

Description	<p>Displays a table of groups and monitors for the element highlighted in the monitor tree or listed in the path. You use functions and links in the group and monitor status information area to navigate to child nodes and monitors and access other actions.</p> <p>To access: Click the Current Status tab within SiteScope Dashboard.</p>
Included in Tasks	“Analyze Data in SiteScope Dashboard” on page 421








The Group and Monitor Status tables under the Current Status tab include the following elements (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click the Reset Column Width button to restore the table's columns to their original width.
	Click to navigate through the results page by page or to jump to the first or last page.
	The Acknowledge column indicates that a SiteScope user has acknowledged the current status of a monitor and may have temporarily disabled alert actions associated with that monitor. This icon is only displayed in Dashboard Detailed views. Moving the pointer over the icon displays the acknowledgement information as a tool tip. For details, see “Acknowledging Monitor Status” on page 417.
	The Configured Alerts column indicates that one or more alerts are associated with the group or monitor. If the pointer is passed over the icon, a tool tip displays the number of configured alerts. Clicking the icon displays the Configured Alerts window. Selecting an applicable alert definition name from the list changes the focus in the monitor tree to the subject alert definition and displays the alert properties view in the group and monitor status information area. For details, see “SiteScope Alerts” on page 1385.
	The Triggered Alerts column indicates that at least one alert has been triggered in the monitor. If no alert was triggered, the icon is not displayed. If a single alert was triggered, an icon representing the specific alert type is displayed. If multiple alerts were triggered, an icon representing multiple alerts is displayed. Clicking the alert icon displays alert details. The Triggered Alert column only appears for a table that contains monitors. For details, see “SiteScope Alerts” on page 1385.

GUI Element (A-Z)	Description
Description	<p>The Description column can contain either text that describes the monitor or group or it can contain HTML that performs various actions when you click it.</p> <p>You can type information in the Description column by right-clicking either the monitor or the group in the monitor tree and then selecting Edit. In the page that opens in the group and monitor status information area, select Advanced Settings and scroll down to the Description text box.</p>
Name	<p>A display name (alias) for the monitor instance or group. When a new group is created, you type its name. When a new monitor is created, you select its type from the list of available monitors. If you do not override this type in the Name box, the monitor is identified by the type of monitor. You can then optionally type an alias that helps you identify this monitor.</p> <p>In a table for groups, you can click on the small black arrow in the Name column to open a context menu. For details, see “Name Column Context Menu” on page 452.</p>
Status	<p>A colored ball is displayed for each node in a Dashboard view, representing the operational status assigned to that component for its current performance level.</p> <p>You can point at the ball to display a tooltip which can be customized to show the information you choose. For details, see “Dashboard Layout Page” on page 437.</p> <p>A color-coded icon is also displayed for each element in a Dashboard view, representing the data availability status of the monitor.</p> <p>The monitor status and availability icons are described in “Status and Availability Levels” below.</p>

GUI Element (A-Z)	Description
Summary	<p>For monitors, the Summary column displays the most recent measurement results reported by the monitor. This may include more than one measurement, depending on the monitor type. For monitor groups, the summary displays the number of monitors within the group and the number of monitors, if any, that are reporting an error status.</p>
Target	<p>The Target column contains the name of the remote server containing the monitored object (if such a server exists). If, for example, the monitor type is CPU, then the target would be the name of the server on which the CPU being monitored is installed.</p> <p>The name displayed in the Target column can be either the system ID of the server or the user-assigned name (alias), depending on what was entered in the Name box when the server was added to the monitor tree.</p> <p>If the group contains a Microsoft Windows Resources Monitor or UNIX Resources Monitor, the server name in the Target column appears as a link. You can click the link to open the Server-Centric Report for the server. For details, see “Server-Centric Report” on page 440.</p>
Type	<p>The type of monitor being displayed. You select the monitor type in the New Monitor page when you create the monitor instance.</p>
Updated	<p>The date and time when the last event occurred in the group or monitor.</p>
Value	<p>The value of the monitor counter when the monitor instance was last run.</p> <p>Note: This column appears only for a counter table displayed for a monitor.</p>

Status and Availability Levels

Icon	Description
	OK Status. All performance measurements are within the OK threshold level.
	Warning Status. At least one performance measurement is within the Warning range, but no measurements are within the Error or Poor range.
	Error/Poor Status. At least one performance measurement is within the Error or Poor range. This indicates either of the following: <ul style="list-style-type: none"> ▶ The performance measurement has a value, but at poor quality level. ▶ There is no measurement value due to some error.
	No thresholds breached Status. No thresholds were defined for the monitor, so no status is assigned.
	Data Collected Availability. Indicates that SiteScope was able to connect to the remote system and perform the action defined by the respective monitor configuration. The resulting monitor status represents the results of the monitor action. If an error or warning is indicated, it represents an accurate measure of the target system's performance or the availability of the target resource.
	Availability Warning. Indicates that SiteScope has detected a possible problem with the connectivity to the remote system.
	No Data Availability. Indicates that SiteScope was not able to connect to the remote system. Any resulting error status for the respective monitor may be attributed to the failure to communicate with a remote server. It does not necessarily mean the target resource has failed.

Name Column Context Menu

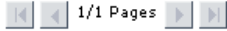

The following options are available by clicking the small black arrow in the Name column for Groups:

GUI Element (A-Z)	Description
Add Acknowledgement	Opens the Acknowledge dialog box which enables you to add an acknowledgement to a monitor.
Delete Acknowledgement	Deletes the monitor's acknowledgement.
Edit	Opens the Properties page for the selected group which enables you to edit the group's properties.
Enable/Disable Alerts in Group	Opens the Enable/Disable Alert Settings dialog box which enables you to enable or disable all the alerts for all monitors in the group. If you select Disable , the alerts are disabled until you return to this page and select Enable .
Enable/Disable Monitors in Group	Opens the Enable/Disable Monitor Settings dialog box which enables you to enable or disable all the monitors in the group. If you select Disable , the monitors are disabled until you return to this page and select Enable .
Run	Runs all the monitors in the group.

SiteScope Dashboard - Monitor History Tab

Description	Displays information about monitors, monitor groups, and alerts over the last 24 hours. This information is filtered by the number of hours, monitor status, and the number of data entries. To access: Click the Monitor History tab within SiteScope Dashboard.
Important Information	You enable this function in General Preferences. You can determine exactly how much data you want saved for this function so that your database does not get overloaded.
Included in Tasks	“Analyze Data in SiteScope Dashboard” on page 421
Useful Links	“Dashboard Monitor History View Options” on page 254

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click to navigate through the results page by page or to jump to the first or last page.
	The Triggered Alert icon appears next to any monitor that triggered an alert.
Availability	This box only appears if you have selected Show monitor availability in the Details View pane of Dashboard Layout.
Group	The name of the group to which the monitor belongs. This box appears only if you have selected Show all descendants in Dashboard.
Name	The name of the monitor.
Run Time	The time the monitor ran.

GUI Element (A-Z)	Description
Status	The monitor's status at runtime (Error, Warning, or Good).
Summary	The description of the monitor run.

Part V

Monitors

13

Working with SiteScope Groups

This chapter includes the main concepts, tasks, and reference information for working with SiteScope groups.

This chapter includes:

Concepts

- ▶ SiteScope Groups Overview on page 457

Tasks

- ▶ Manage a Group – Workflow on page 460

Reference

- ▶ New SiteScope Group Page on page 462

SiteScope Groups Overview

You create group containers to make deployment of monitors and associated alerts manageable and effective for your environment and organization. Each SiteScope monitor instance that you create must belong to a SiteScope group, either a top level group or a subgroup nested within other group container.

For example, if you intend to monitor a large number of processes running on your system, you may want all of them to be in a single group named **Processes**. If you are monitoring processes on several machines using remote monitors, you could create a primary group called **Processes** with several subgroups named after each of the remote machines that you are monitoring.

When you add a new monitor you either add it to an existing group, or you must first create a group for it. You can add groups individually to SiteScope, or you can deploy groups along with multiple monitors by using templates.

Copying or Moving Existing Groups

In addition to creating groups, you can copy or move existing groups to a new location within the SiteScope tree. Copying or moving a group duplicates the configuration settings for the group and all monitors within the group. After copying or moving a group, you normally need to edit the group and the configuration properties for each individual monitor within the group to direct the monitors to a unique system or application. Otherwise, the monitors in the group duplicate the monitoring actions of the original group.

Notes:

- ▶ Instead of copying groups which can lead to redundant monitoring, it is recommended to use templates to more efficiently replicate common group and monitor configuration patterns. For more information about working with templates, see “SiteScope Templates”.
 - ▶ To avoid group identity problems within SiteScope, object names must be unique within the parent container. If you copy or move a monitor group to a container in which there is another group with exactly the same name, SiteScope automatically adds a suffix (number) to the end of the monitor group's name.
 - ▶ You cannot move or copy a monitor group to its subgroup.
-

Creating Group Alerts and Reports

After creating a group, you can create alerts and reports for the group. By default, group alerts and reports are associated with all monitors within the group.

You create an alert by adding an alert definition to a group container. This means that when any one monitor in the group reports the status category defined for the alert (for example, **error** or **warning**), the group alert is triggered. You can configure a group alert to exclude one or more of the monitors in the group by using the **Alert Targets** selection tree. For details on this topic, see “SiteScope Alerts Overview” on page 1386.

You create a group report by adding a report definition to a group container. You can configure a group report to exclude one or more of the monitors in the group by using the **Monitors and Groups to Report on** selection tree. For details on this topic, see “SiteScope Reports Overview” on page 1439.

If you delete a group, SiteScope removes the applicable monitor actions and disables any alert actions associated with the group.

Manage a Group – Workflow

This task describes the steps involved in managing a group.

This task includes the following steps:

- “Create a Group” on page 460
- “Create Monitor Instances” on page 460
- “Set Group Dependencies” on page 461
- “Set Up Group Alerts” on page 461
- “Set Up Group Reports” on page 461
- “Results” on page 462

1 Create a Group

Create SiteScope groups according to the monitor hierarchy which you want to implement.

- To create a new group, right-click the SiteScope or group container in which to create the group, and click **New Group**. For details on the user interface, see “New SiteScope Group Page” on page 462.
- To create a group by copying or moving an existing group, right-click the group you want to copy or move, and click **Copy** or **Cut**. Right-click the location in the monitor tree where you want to copy or move the group container, and click **Paste**.

2 Create Monitor Instances

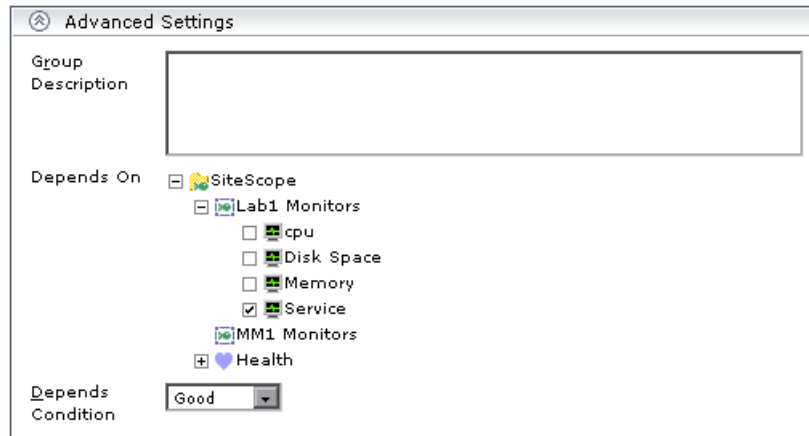
Select the monitors instances you want to add to the group. For details on how to perform this task, see “Deploy a Monitor – Workflow” on page 489.

3 Set Group Dependencies

You can set group dependencies to make the running of monitors in this group dependent on the status of another monitor. For details on this topic, see “Monitoring Group Dependencies” on page 473.

Example

The monitors in the group being configured run normally as long as the monitor selected in the **Depends On** box reports the condition selected in the **Depends Condition** box. In this example, the group being configured is enabled only when the **Service** monitor in the **Lab1 Monitors** group reports a status of **Good**.



4 Set Up Group Alerts

To create an alert for the group, right-click the group and click **New Alert**. For each alert scheme, you can create one or more alert actions. In the New Alert page, click **Add Action** to start the Alert Action wizard. For details on how to perform this task, see “Configure an Alert” on page 1409.

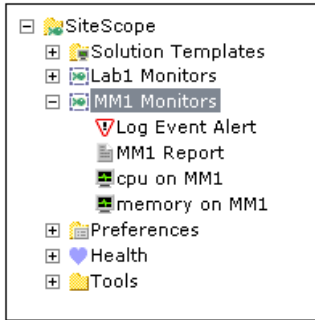
5 Set Up Group Reports

To create a report for the group, right-click the group and click **New Report**. Select a report type from the New SiteScope Report page and configure the report settings. For details on how to perform this task, see “Create a Report” on page 1444.

6 Results

The monitor group, including its monitors, alerts, and reports, is added to the monitor tree.

Example



New SiteScope Group Page

Description	<p>Enables you to define a new group for SiteScope, or a subgroup for an existing monitor group.</p> <p>To access:</p> <p>Right-click the SiteScope container, or an existing monitor group and select New Group.</p>
Important Information	<p>You cannot delete a monitor group if it has dependent alerts or reports at the container level. To delete a monitor group with dependencies, you must remove the monitor group from Alert Targets and Monitors and Groups to report on in the Main Settings for each dependency, and then delete the monitor group. You can delete monitor groups that have dependencies at the child level.</p>
Included in Tasks	<p>“Manage a Group – Workflow” on page 460</p>
Useful Links	<p>“SiteScope Groups Overview” on page 457</p>

The following elements are found throughout the New Group page:

Main Settings

GUI Element	Description
Group Name	<p>Type a name that describes the content of the group, or the purpose of the monitors added to the group. For example, <hostname> or <business_unitresource_name> or <resource_type>.</p> <p>Note:</p> <ul style="list-style-type: none">▶ The group name cannot be sitescope or contain any of the following characters: ' ; & < > / \ + =▶ The group name is case sensitive. This means that you can have more than one group with the same name provided they each have a different case structure.

Advanced Settings

GUI Element	Description
Group Description	<p>Type additional information to describe a group. The description can include HTML tags such as the
, <HR>, and tags to control display format and style. The description text appears on the Content tab for the group in the SiteScope node.</p> <p>Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> ➤ Tags: script, object, param, frame, iframe. ➤ Any tag that contains an attribute starting with on is declined. For example, onhover. ➤ Any attribute with javascript as its value.
Depends On	<p>Select a monitor on which the monitor group is depended. This monitor acts as the "heartbeat" monitor and checks the basic availability of the system. If the "heartbeat" monitor detects a problem in the target system, the dependency relationship automatically disables all the monitors in the monitor group. Use this option to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system.</p> <p>Default: No dependency is set for a monitor group.</p>

GUI Element	Description
Depends Condition	<p>Select the Depends Condition that the Depends On monitor should have for the current monitor group to run normally. If the selected condition is not satisfied then the monitor selected in the Depends On box is automatically disabled. The conditions are:</p> <ul style="list-style-type: none"> ➤ Good ➤ Error ➤ Available
Source Template	<p>Displays the path of the source template if the group was created from a template. If you are using deployed templates created in older versions of SiteScope, enables you to manually associate the root groups with the source template by typing the path of the source template.</p>

Category Settings

GUI Element	Description
Assigned categories	<p>Filters items in the SiteScope views. For more details, see “Views and Categories” on page 195.</p>

14

Working with SiteScope Monitors

This chapter includes the main concepts, tasks, and reference information for working with SiteScope monitors.

This chapter includes:

Concepts

- ▶ SiteScope Monitors Overview on page 468
- ▶ SiteScope Monitor Categories on page 469
- ▶ Monitoring Remote Servers on page 471
- ▶ Monitoring Group Dependencies on page 473
- ▶ Setting Status Thresholds on page 476
- ▶ Setting Status Thresholds Using a Baseline on page 478

Tasks

- ▶ Deploy a Monitor – Workflow on page 489
- ▶ Set Monitor Thresholds Using a Baseline on page 493

Reference

- ▶ Monitors Supported in Windows Environments Only on page 501
- ▶ Ports Used for SiteScope Monitoring on page 503
- ▶ SiteScope Monitors User Interface on page 507

SiteScope Monitors Overview

SiteScope monitors are tools for automatically connecting to and querying different kinds of systems and applications used in enterprise business systems. The different monitor types provide the generic capabilities for performing actions specific to different systems. You create one or more instances of a monitor type to instruct SiteScope how to monitor specific elements in your IT infrastructure.

For example, you can create 100 monitor instances that instruct the SiteScope CPU Monitor type to connect to and measure CPU utilization on remote servers. Each monitor instance contains a different setting defining which remote server is to be monitored and how often. SiteScope is then configured to automatically monitor the CPU utilization on 100 servers at regular intervals.

Monitor instances that you create must be added within a SiteScope monitor group container. You use group containers to help you organize the monitor instances that you create.

Note: For a list of counters or metrics that can be configured for SiteScope monitors, as well as versions of applications or operating systems that are supported, see *HP SiteScope Monitors and Metrics* located in `<SiteScope root directory>\sisdocs\pdfs\SiteScope_Monitors_Metrics.doc`.

SiteScope Monitor Categories

SiteScope monitor categories are grouped according to classes that indicates their availability and category that reflect their function. When you select to add a new monitor to a SiteScope agent, the list of available monitor types for that agent are displayed both alphabetically and divided by category in the product interface. The availability of the monitor category is dependent on the class of monitor. This section describes the monitor classes and the category listing formats.

Solution Template Monitors

Solution template monitor types are a special class of monitors that enable new monitoring capabilities for specific applications and environments. As part of a solution template, these monitor types are deployed automatically together with other, standard monitor types to provide a monitoring solution that incorporates best practice configurations. These monitor types are controlled by option licensing and can only be added by deploying the applicable solution template. Once they have been deployed, you can edit or delete them using the same steps as with other monitor types. For more information, see “SiteScope Solution Templates” on page 1273.

The monitor types using solution templates include:

- ▶ Active Directory (with and without Global Catalog)
- ▶ IIS Server
- ▶ Microsoft Exchange 5.5, 2000, 2003, 2007
- ▶ Microsoft SQL Server
- ▶ Microsoft Windows Resources Monitor
- ▶ Oracle Database 9i and 10g
- ▶ SAP Application Server (NetWeaver and R3)
- ▶ Siebel Application/Gateway/Web Server (for UNIX and for Windows)
- ▶ UNIX Resources
- ▶ WebLogic Application Server
- ▶ WebSphere Application Server

Standard Monitors

Standard monitor categories represent the monitor categories available with a general SiteScope license. These monitor categories include many of the general purpose monitor categories. For information about the usage and configuring each monitor type, see the section for the particular monitor category.

- ▶ **Application Monitors.** Monitors in this category monitor 3rd party applications. These monitors enable SiteScope to access and retrieve data from the monitored applications. For more information about Application Monitor capabilities, see the section on “Application Monitors” on page 549.
- ▶ **Database Monitors.** Monitors in this category monitor different types of database applications. There are monitors that access data from specific database applications and generic monitors that can be configured to monitor any database application. For more information about Database Monitor capabilities, see the section on “Database Monitors” on page 723.
- ▶ **Generic Monitors.** Monitors in this category monitor various type of environment. These monitors can monitor networks, applications, and databases depending on how they are configured. For more information about Generic Monitor capabilities, see the section on “Generic Monitors” on page 773.
- ▶ **Network Monitors.** Monitors in this category monitor network health and availability. For more information about Network Monitor capabilities, see the section on “Network Monitors” on page 823.
- ▶ **Server Monitors.** Monitors in this category monitor server health and availability. For more information about Server Monitor capabilities, see the section on “Server Monitors” on page 891.
- ▶ **Stream Monitors.** Monitors in this category monitor applications that play media files and stream data. For more information about Stream Monitor capabilities, see the section on “Stream Monitors” on page 941.
- ▶ **Web Transaction Monitors.** Monitors in this category monitor web-based applications. For more information about Web Transaction Monitor capabilities, see the section on “Web Transaction Monitors” on page 957.

Integration Monitors

This group of optional monitor types are used to integrate HP products with other commonly used Enterprise Management systems and applications. They are presented in a separate section on the New SiteScope Monitor panel.

These monitor types require additional licensing and may only be available as part of another HP product. For more information about Integration Monitor capabilities, see the section on “Working with SiteScope Integration Monitors” on page 1045.

Monitoring Remote Servers

Some SiteScope monitors use Internet protocols to test Web systems and applications. Other SiteScope monitors use network file system services and commands to monitor information on remote servers. These monitors are limited to:

- CPU
- Disk Space
- Memory
- Microsoft Windows Event Log
- Microsoft Windows Performance Counter
- Script (UNIX only)
- Service
- Web Server (Windows only) monitors

Monitoring remote Windows servers requires:

- ▶ SiteScope for Windows XP/2000/2003. In general, SiteScope for UNIX cannot monitor remote Windows servers.
- ▶ The SiteScope service must run in a user or administrative account that has permission to access the Windows Performance registry on the remote servers to be monitored. For details on how to change the SiteScope account user, see “Change the User Account of the SiteScope Service” on page 240.

To monitor certain server level parameters on a remote server using the network files system services, you must create a remote server profile. A table of server profiles is listed on the Microsoft Windows/Unix Remote Preferences page in the Preferences container. The remote server profiles contain the address and connection information that SiteScope needs to make a remote connection. After creating remote server profiles, set up monitors to use the remote connection profile. For details on creating remote profiles and remotely monitoring either Windows or UNIX servers, see “Microsoft Windows Remote Preferences” on page 219 or “UNIX Remote Preferences” on page 220.

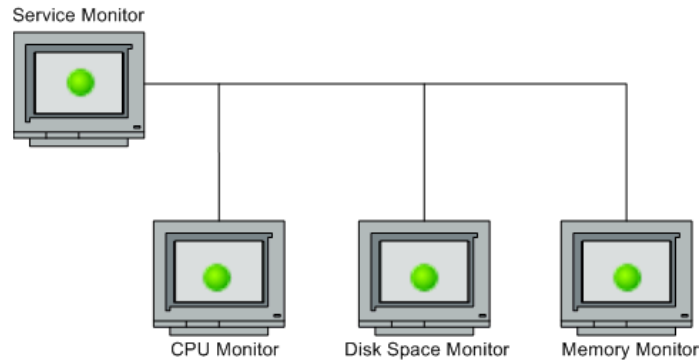
The requirements for monitoring services and applications that are running on remote servers vary according to the application and network policies in your environment. For information about how SiteScope monitors connect to remote systems, see “Monitors Supported in Windows Environments Only”. You can also check for other information relating to monitoring remote servers in the HP Software Self-solve knowledge base (<http://h20230.www2.hp.com/selfsolve/documents>). To enter the knowledge base, you must log in with your HP Passport ID.

Monitoring Group Dependencies

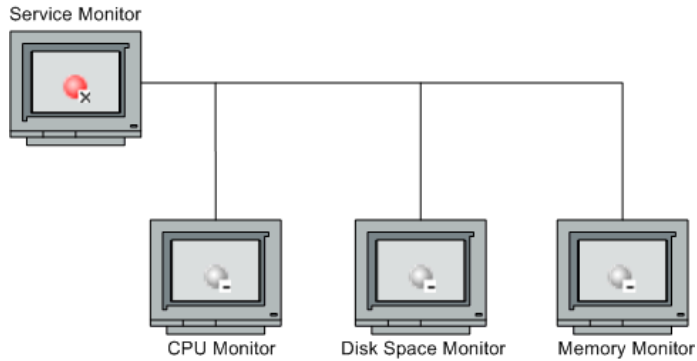
To prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system, select one monitor to check the basic availability of the system and then create other monitors that perform more detailed tests of that system. This creates a dependency relationship that enables you to make the running of a monitor group dependent on the status of a selected monitor.

Depends On

You use this option to make the running of this monitor dependent on the status of another monitor. This can be used to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system. You can create a simple system monitor to check the basic availability or heartbeat of a system and then create other monitors that perform more detailed tests of that system. The figure below shows an example dependency relationship where three system monitors have been made dependent on a Service Monitor instance.



The detailed test monitors can be made dependent on the status of the heartbeat monitor by selecting that monitor. This means the dependent monitors run as long as the dependency condition is satisfied. If the heartbeat monitor detects that the target system has become unavailable, the dependency relationship automatically disables the other monitors. This has the effect of disabling any alerts that would have been generated by those monitors. The figure below shows the example monitors are disabled because the monitor on which they depend is reporting an error condition.



By default, no dependency is set for a monitor instance. To make the running of the monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which you want to create dependence, and select the check box next to the required monitor. To remove dependence on a monitor, clear the required check box.

Depends Condition

If you choose to make a monitor dependent on the status of another monitor (by using the **Depends On** setting), you use this option to select the status category or condition that the **Depends On** monitor should have for the current monitor to run normally.

The status categories include:

- Good
- Error
- Available
- Unavailable

The monitor being configured is run normally as long as the monitor selected in the **Depends On** box reports the condition selected in this box. If you have selected **Unavailable** and the **Depends On** monitor reports this status, the current monitors are not disabled.

For example, by selecting **Good**, this monitor is only enabled as long as the monitor selected in the **Depends On** box reports a status of **Good**. The current monitor is automatically disabled if the monitor selected in the **Depends On** box reports a category or condition other than the condition selected for this setting. See the examples for the **Depends On** setting.

For information about configuring dependency settings, see “**Depends On**” and “**Depends Condition**” on page 513.

Setting Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status is based on the results or measurements returned by the monitor action on the target system as compared to the thresholds set for the monitor.

You can set status threshold criteria for each monitor instance to determine an **Error** status, a **Warning** status, and a **Good** status. Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value that you may specify. The parameter and the value depend on the monitor type. For example, the measurement parameter for a CPU monitor is CPU utilization (%).

You can set up one or more status threshold criteria for each status condition. Most monitor types include one default setting for each of the three status conditions. By default, only one threshold is displayed when you first configure the monitor.

Scheduling

You can also select a schedule to determine the status of the monitor instance if you want to define when to check the monitor run result against the threshold. This is useful if you want to restrict checking the monitor run results against the threshold to certain days or hours only. For example, you may want the monitor status to be based on results gathered during business hours only. At times outside the threshold schedule period, the monitor is assigned the predefined status in the **Default status** box. By default, monitor run results are checked against the threshold on an **every day, all day** schedule.

Availability

When the monitor is not available, it is assigned a status that is based on the user definition in the **If Unavailable** drop-down list. A monitor can have a state of **Unavailable** as well as a status of **Good**, **Warning**, or **Error**. Alerts are triggered according to availability, status, or both availability and status.

Baseline Thresholds

Instead of setting logic conditions manually in the threshold settings for each monitor instance, you can have SiteScope calculate thresholds for one or more monitor instances using a baseline. For information about this topic, see “Setting Status Thresholds Using a Baseline” on page 478.

Threshold Status Impact

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the monitor detects that the system has become unavailable, the status change from **Good** to **Error** is used to trigger an alert on error.

A change of status may also affect the state of a dependency between monitors. For example, a monitor that detects a change that results in an **Error** status may be a trigger to disable one or more other monitors that are dependent on the system. For information about dependency settings, see “Monitoring Group Dependencies” on page 473.

The threshold setting also affects the status of the monitor in the SiteScope Dashboard. When viewing SiteScope data in the Current Status tab of Dashboard, you can drill down in the monitor tree to view monitor and measurement status and availability. The status is displayed by color and a status icon in the SiteScope Dashboard. For information on measurement status and availability in the Dashboard user interface, see “Status and Availability Levels” on page 451.

Multiple Thresholds

The individual threshold criteria results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status condition setting the status of the monitor is set to the highest valued status condition.

For example, if one condition selected as **Error if** and another condition selected as **Warning if** are both met, the status would be reported as an **Error**, with **Error** being the highest value, **Warning** the next highest and **Good** the lowest value.

For details on configuring monitor status thresholds, see “Set Monitor Thresholds” on page 490.

Setting Status Thresholds Using a Baseline

Baseline data is gathered from monitor performance metrics over a period of time and is used to provide a comparison for establishing acceptable or expected threshold ranges. When the monitor's performance exceeds that range by some value, the monitor can signal an error or warning. The acceptable threshold range of a monitor is determined by how far the current performance is from the baseline. Baselines enable you to understand how your applications typically perform and determine whether a performance problem is an isolated incident or a sign of a significant downward performance trend.

This section contains the following topics:

- “Calculating the Baseline” on page 479
- “Activating the Baseline” on page 479
- “Notes and Limitations” on page 481
- “Setting the Baseline Adherence Level” on page 482

- “Understanding the Good and Error Boundaries” on page 483
- “Understanding Baseline Threshold Values” on page 485

Calculating the Baseline

To enable SiteScope to begin calculating baselines, you select the groups and/or monitors to be used for collecting baseline data. You can also select the schedule ranges used for collecting baseline threshold data. This enables you to restrict to certain days or hours of the week the periods during which SiteScope collects data for the baseline calculation. For example, you may want the monitor status to be based on results gathered during peak business hours only.

You can also select the adherence level used for determining the extent to which values for the baseline calculation affect the threshold values and set threshold boundaries for all monitor measurements. For details, see “Setting the Baseline Adherence Level” on page 482 and “Understanding the Good and Error Boundaries” on page 483.

The baseline engine calculates the baseline for each schedule using measurements collected from the monitors during the data collection period. SiteScope uses a percentile algorithm in the baseline calculation, in which a percentile value is used to determine the value of the baseline. For details on how baseline thresholds are calculated, see “Understanding Baseline Threshold Values” on page 485.

Activating the Baseline

After the baseline is calculated, you can review a summary of calculated monitors and analyze the baseline data in the Baseline Summary table. The table lists all the monitor instances for which a baseline was calculated, the date of the baseline calculation, and the reduction in the number of error and warning statuses that would have been generated for a monitor if the baseline thresholds were applied.

You can also view a graph that displays the current thresholds, the baseline thresholds, and historic data of all baseline-related monitor measurements over a 24-hour time period for each monitor measurement. The graph includes an annotation tool that enables you to annotate a snapshot of the graph you are viewing, to highlight important areas. You can save, print, or e-mail an annotation graph. For details on the user interface, see “Annotation Tool” on page 1484.

If SiteScope is unable to calculate a baseline for a monitor, the monitor is listed in the Failed Monitors list. If a monitor fails for the reason **Insufficient data**, you can still select the monitor for baseline activation using the limited measurement samples that were collected.

After reviewing the baseline data, you can activate baseline threshold configuration. This applies the baseline values to the thresholds for the selected monitors. By default, all monitors with a successfully calculated baseline are selected. It is recommended that you select the option to save the current monitor configuration before activating the baseline threshold, because you cannot undo configuration changes after the baseline has been activated.

When the baseline is activated, the baseline thresholds are displayed in the Threshold Settings area for each monitor. Each day when SiteScope restarts, the baseline value is recalculated according to the history samples collected for the measurement and the current day’s readings, and the baseline threshold values are recalculated and updated accordingly.

At any time, you can create a baseline summary report showing the baseline status and baseline status description for each monitor in the selected context.

Notes and Limitations

- You cannot add or delete thresholds or measurements, or copy or move monitors during the baseline calculation process (up until the point that the monitor baseline is activated).
- Before the baseline is calculated, the monitors should be enabled and allowed to run for a period long enough for SiteScope to accumulate sufficient data to calculate the baseline. This period depends on the **Minimum number of days required for baselining** and **Minimum number of samples required for baselining** settings in the Baseline Settings. For details, see “Baseline Settings” on page 273.
- During the baseline calculation and after the baseline is activated, only certain baseline threshold changes are supported. For details on the threshold changes that are allowed, see “Changing Threshold Settings” on page 523.
- After you define a set of counters for a browsable monitor and the monitor runs with these counters for some time, if you later change the counters (for example, remove existing counters and/or add new counters), and then you attempt to calculate baseline, the calculation results may be incorrect. This can occur because old data, possibly for counters that no longer exist, interferes with the new data. The calculation may also be incorrect for counters that have not changed since the monitor was created. To avoid this problem, you should not make any changes to a monitor’s browsable counters during the minimum number of days period required for calculating the baseline.
- You can change threshold related properties using Global Search and Replace, regardless of whether the threshold was created using a baseline or manually.
- Using Global Search and Replace, you cannot activate a baseline threshold for a monitor. You can only remove a baseline threshold from a monitor.
- If SiteScope restarts before the baseline calculation or activation process is complete, it automatically continues the process after the restart. Monitors with any other baseline status (**Calculated, not activated**; **Activation failed**; **Calculation failed**; **Baseline activated**) are not affected by the restart.

- ▶ If you make changes directly to the SiteScope group (.MG) files in the `<SiteScope_root_directory>\groups` directory, only the threshold changes permitted in the user interface are supported (any other changes are ignored).
- ▶ Baseline thresholds are not copied or moved along with the other group or monitor objects when copying or moving a group or monitor with an activated baseline.
- ▶ Memory consumption increases for each monitor threshold set using a baseline. To reduce memory consumption, you can set the **Interval for saving accumulated baseline data to disk** settings in the Baseline Settings. For details, see “Baseline Settings” on page 273.

For details on setting thresholds using a baseline, see “Set Monitor Thresholds Using a Baseline” on page 493.

Setting the Baseline Adherence Level

You can select the baseline adherence level used for determining the threshold value. This is the extent to which values for the baseline calculation affect the threshold values for all monitor measurements. You can select **High Adherence**, **Medium Adherence**, or **Low Adherence**. The higher the adherence level, the closer the threshold range is to the monitor measurement baseline values. Conversely, the lower the adherence level, the further the threshold range is from the monitor measurement baseline values.

In addition to selecting the adherence level, you can also fine-tune the adherence level for individual monitor measurements by configuring adherence percentiles separately for each monitor measurement. Adherence levels are based on adherence percentiles—a measurement value that determines when a measurement is in error or warning. For browsable monitor measurements, you can configure only one set of adherence percentiles that is used by all browsable monitors.

To manually fine-tune the adherence level, you should understand how the threshold values are created. For details on this topic, see “Understanding Baseline Threshold Values” on page 485.

Understanding the Good and Error Boundaries

Configuring good and error boundaries is useful to avoid setting off errors and warnings unnecessarily when using baseline thresholds. You can manually set a good boundary for each monitor measurement and the browsable monitor counters. SiteScope automatically configures the error boundary for each monitor measurement.

Note: To set good boundaries, it is important to understand how baseline threshold values are created. For details on this topic, see “Understanding Baseline Threshold Values” on page 485.

Good Boundary

This is the value of a measurement that is not considered to be in error status, even though according to existing baseline percentiles it should report an error. For example, consider a low load system where CPU utilization measurements are constantly below 3%. Based on these measurements, SiteScope might calculate a baseline threshold with a 5% error threshold. Because this is not an accurate measure of CPU load error, you may want to define 70% CPU utilization as the good boundary to avoid generating false errors. Provided CPU utilization remains below this limit (even though it is above the baseline error threshold), the monitor is not in error status.

You manually set the Good Boundary in the Edit Adherence Level and Good Boundary Dialog Box. For details on the user interface, see “Edit Adherence Levels and Good Boundary Dialog Box” on page 534.

Error Boundary

This is the value of a measurement that is considered to be in error status, even though according to existing baseline percentiles it should not report an error. This can occur when a measurement value grows slowly over a period of time, for example, due to a slow memory leak. Because the baseline threshold is recalculated and updated every day as the measurement average increases, the measurement value does not cross the new threshold.

To overcome this problem, SiteScope automatically sets the error boundary for each monitor measurement. It does this by setting a limit that triggers errors when monitor measurements exceed a specified value, regardless of the baseline. For example, if SiteScope sets an error boundary of 80% CPU utilization, values over 80% CPU utilization are in error status even if the calculated baseline error threshold is not exceeded.

For information on how the error boundary is calculated, see “How SiteScope Calculates the Error Boundary” on page 487.

Understanding Baseline Threshold Values

To help you fine-tune the percentile value used in the baseline calculation at each adherence level and to set the error and good boundaries (for details, see “Understanding the Good and Error Boundaries” on page 483), it is important to understand:

- the types of threshold values
- how they are applied to measurements
- how measurements are used to calculate baseline thresholds and boundaries

Baseline thresholds are added or updated dynamically to the monitor configuration for each measurement the monitor had before the baseline was calculated. Baseline thresholds are added for each schedule selected for collecting baseline data.

In general, there are two types of thresholds: baseline thresholds and static thresholds. Baseline thresholds have a percentile value that is used to determine when a measurement is in error or warning status, while static thresholds have an actual fixed value. Baseline threshold measurements have a condition of either \geq or \leq depending on the direction of the measurement.

Baseline thresholds are changed, added, or deleted on measurements provided the following two conditions are met:

- The measurement can be used in the baseline calculation. To be used in the baseline calculation, a measurement must be numeric and it must have a direction. An example of a measurement that cannot be used in the baseline calculation is a URL 404 error code (it is numeric, but it has no direction).
- The measurement has a static threshold defined for any schedule and any category (Good, Warning, Error) prior to the baseline calculation.

Measurements that do not adhere to these conditions are not affected (in terms of the thresholds defined on them), and a baseline is not calculated for these measurements.

How SiteScope Calculates Thresholds

When SiteScope calculates the baseline, it creates a percentile value for each baselinable threshold measurement for each schedule. SiteScope makes an adjustment for extreme measurements by discarding, by default, 2% of the most extreme samples (considered "noise" measurements), and calculates the percentiles on the remaining measurements. For example, if most monitor run results on a server show CPU utilization of no more than 20% and one peak value of 50%, the peak value is not used to determine the baseline. You can change the percentage of discarded measurement samples in the Baseline Settings.

SiteScope also uses the percentile value to create an error boundary for each measurement. This is the value of a measurement that is considered to be in error status, even though according to existing baseline percentiles it should not report an error. For details, see "How SiteScope Calculates the Error Boundary" on page 487.

The baseline engine uses a sliding-window approach to calculate thresholds. This means that newer data samples have more influence on the baseline calculation than older samples, and that after a period of time (by default 30 days), the historic data becomes obsolete. You can set the number of days to include in the calculation in the Baseline Settings.

For information about configuring Baseline Settings in the Infrastructure Settings Preferences, see "Baseline Settings" on page 273.

How SiteScope Calculates the Error Boundary

SiteScope calculates the error boundary in one of the following ways:

- ▶ If the measurement has a static error threshold for the specific schedule, the percentile value of the baseline threshold is calculated into an actual value and this value is then compared to the value of the static threshold as follows:
 - ▶ If the static error threshold value is more extreme than the baseline threshold value, the static error threshold value is used as the error threshold boundary for that measurement.
Example: If the static error threshold is 100% CPU utilization and the computed baseline threshold is 67% CPU utilization, the static error threshold value (100% CPU utilization) is used as the error boundary.
 - ▶ If the baseline threshold value is more extreme than the static error threshold value, then the offset value is used. The offset is a percentage value that SiteScope adds to the baseline threshold value (or subtracts from, depending on the direction of the measurement), and the resulting value is used as the error boundary for that measurement. You can determine the offset value in the Baseline Settings area of Infrastructure Settings Preferences.
Example: If the static error threshold for a schedule is 60% CPU utilization and the computed baseline threshold value is 65% CPU utilization, the error boundary is calculated as:
 $65\% \text{ CPU utilization} * 130\%$ (using the default offset value of 0.3) = 84.5% CPU utilization.
- ▶ If there is no error threshold value for the measurement with the specific schedule prior to calculating the baseline (the measurement has a warning or good threshold value but no error threshold value), and the **Automatically create an Error Boundary if no error thresholds are defined** option is selected in the Baseline Properties, the percentile value of the baseline threshold is calculated into an actual value and the offset value is added to/subtracted from the baseline threshold value (depending on the direction of the measurement). The resulting value is used as the error boundary for the measurement.

- If there is no error threshold value for the measurement with the specific schedule prior to calculating the baseline (for example, the measurement has a warning or good threshold value but no error threshold value), and the **Automatically create an Error Boundary if no error thresholds are defined** option is not selected, no error boundary is created.

For details on defining the offset value and automating error boundary creation, see “Baseline Settings” on page 273.

Deploy a Monitor – Workflow

This task describes the steps involved in deploying a monitor.

- “Prerequisites” on page 489
- “Create Monitor Instances” on page 489
- “Set Monitor Thresholds” on page 490
- “Set Monitor Dependencies” on page 491
- “Set Up Monitor Alerts” on page 491
- “Set Up Monitor Reports” on page 492
- “Results” on page 492

1 Prerequisites

- Monitors can be created only in a SiteScope group. For details on how to create a group, see “Create a Group” on page 460.
- To enable SiteScope to monitor data on remote servers, you must configure remote Windows or UNIX servers. For details on enabling SiteScope to monitor data on remote Windows servers, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236. For details on enabling SiteScope to monitor data on remote UNIX servers, see “UNIX Remote Preferences” on page 220.

2 Create Monitor Instances

You can create new monitor instances, or copy or move existing monitor instances to the group.

- To create a new monitor, right-click the group into which you want to add the monitor instance, and click **New Monitor**. Select the monitor you want to add from the New SiteScope Monitor list, and complete the monitor properties form. For details on the user interface, see “New SiteScope Monitor Page” on page 508.

- ▶ To create a monitor by copying or moving an existing monitor, right-click the monitor you want to copy or move, and click **Copy** or **Cut**. Right-click the location in the monitor tree where you want to copy or move the monitor, and click **Paste**. After copying a monitor, you normally need to change the system or application that the monitor is targeting, otherwise the copied monitor duplicates the monitoring actions of the original monitor instance.

3 Set Monitor Thresholds

You can manually set logic conditions that determine the reported status of each monitor instance, or you can set thresholds for one or multiple monitors using a baseline.

- ▶ For details on how to set monitor thresholds manually, see “Threshold Settings” on page 518.
- ▶ For details on how to set monitor thresholds using a baseline, see “Set Monitor Thresholds Using a Baseline” on page 493.

Example

If you are monitoring a CPU and acceptable thresholds are 60%-90%, set the threshold settings as follows:

The screenshot shows the configuration interface for setting monitor thresholds. It is divided into three sections: Error if, Warning if, and Good if. Each section has a checkbox, a dropdown menu for the metric (utilization%), a dropdown for the comparison operator, a text input for the threshold value, a dropdown for the frequency (every day, all day), and a 'New' button.

Condition Type	Checkbox	Metric	Operator	Value	Frequency	Action
Error if	<input type="checkbox"/>	utilization(%)	>=	90	every day, all day	New Error if
Warning if	<input type="checkbox"/>	utilization(%)	>=	60	every day, all day	New Warning if
Good if	<input type="checkbox"/>	always (default)	<	60	every day, all day	New Good if

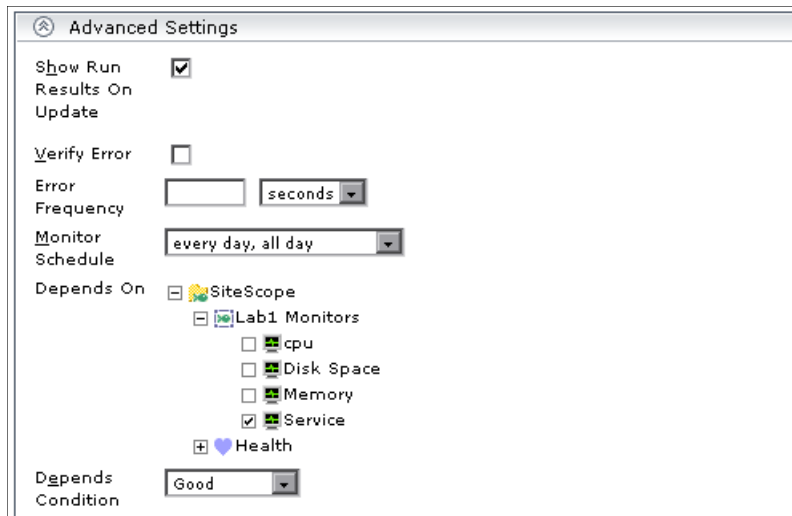
CPU utilization of less than 60% results in a good status; CPU utilization equal to or greater than 60% but lower than 90% results in a warning status; CPU utilization equal to or greater than 90% results in an error status.

4 Set Monitor Dependencies

You can set monitor dependencies to make the running of this monitor dependent on the status of another monitor. For details on this topic, see “Monitoring Group Dependencies” on page 473.

Example

The monitor being configured is run normally as long as the monitor selected in the **Depends On** box reports the condition selected in the **Depends Condition** box. In this example, the monitor being configured is enabled only when the **Service** monitor in the **Lab1 Monitors** group reports a status of **Good**.



5 Set Up Monitor Alerts

To create an alert for the monitor, right-click the monitor and click **New Alert**. For each alert scheme, you can create one or more alert actions. In the New Alert page, click **Add Action** to start the Alert Action wizard. For details on how to perform this task, see “Configure an Alert” on page 1409.

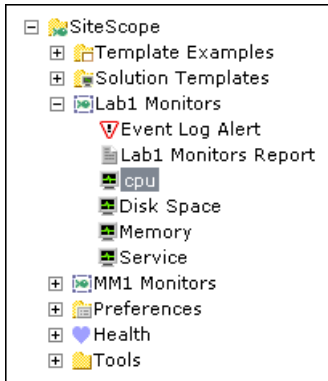
6 Set Up Monitor Reports

To create a report for the monitor, right-click the monitor and click **New Report**. Select a report type from the New SiteScope Report page and configure the report settings. For details on how to perform this task, see “Create a Report” on page 1444.

7 Results

The monitor is added to the specified monitor group in the monitor tree.

Example



Set Monitor Thresholds Using a Baseline

This task describes the steps involved in setting monitor thresholds using a baseline.

This task includes the following steps:

- “Configure Baseline Settings Preferences” on page 493
- “Calculate the Baseline” on page 493
- “Review the Baseline Settings” on page 497
- “View the Baseline Monitor Measurements Graphs” on page 498
- “Activate the Baseline Settings” on page 499
- “View Baseline Properties in the Status Report” on page 499
- “View and Modify Baseline Thresholds” on page 500

1 Configure Baseline Settings Preferences

You can view and define the values of global SiteScope baseline settings in Infrastructure Settings Preferences. This includes calculation and activation priority settings, the number of days of historical data to include in baseline calculations, the minimum number of days and samples required to calculate the baseline, and the offset for calculating the error boundary. For details on the user interface, see “Baseline Settings” on page 273.

2 Calculate the Baseline

Define thresholds on the monitor measurements for which the baseline should be calculated.

- a** Select the monitor instances you want to baseline. For details on the user interface, see “Select Monitors for Baseline Calculation Dialog Box” on page 528.

- b** To configure advanced baseline settings, click the **Advanced Settings** button. The following options are available:
- ▶ You can select one or more schedule ranges to be used for collecting baseline data, or accept the default schedule (every day, all day). For details on the user interface, see “Baseline Calculation Advanced Settings Dialog Box” on page 529.
 - ▶ You can select the global baseline adherence level that is used for determining the extent to which values for the baseline calculation affect the threshold values for all monitor measurements. For details on the user interface, see “Select Level of Adherence to Baseline” on page 531.
 - ▶ You can individually fine-tune the baseline adherence level for any monitor measurement by clicking the **Fine-Tune Adherence Levels/Set Boundary** button. For details on the user interface, see “Configure Adherence Percentiles” on page 532.
 - ▶ You can define a good boundary for each monitor measurement by clicking the **Fine-Tune Adherence Levels/Set Boundary** button. A measurement within this boundary is not in error status, even though it should report an error according to existing baseline percentiles. For details on the user interface, see “Configure Adherence Percentiles” on page 532.
- c** Click the **Calculate** button to perform the baseline threshold calculation.

Note: Before the baseline is calculated, the monitor should be enabled and allowed to run for a period long enough for SiteScope to accumulate sufficient data to calculate the baseline. This period depends on the Baseline Settings. For details on the user interface, see “Baseline Settings” on page 273.

Example - Select Monitors for Baseline Calculation

Select Monitors for Baseline Calculation

Select the monitors to include in the baseline calculation.

- Lab1 Monitors
 - cpu
 - Service
 - Memory

[Advanced Settings](#)

Example - Configure Advanced Settings

Baseline Calculation Advanced Settings

Select Threshold Range Schedule

Schedule ranges can be selected for collecting baseline threshold data. You can also define new ranges in Preferences > Range Schedule Preferences. If you do not select a range, the default 24/7 schedule is used.

/1 Pages

Schedule Range Name ▲
<input type="checkbox"/> every day, 09:00-18:00
<input type="checkbox"/> every day, 18:00-09:00
<input type="checkbox"/> weekdays, 09:00-18:00
<input type="checkbox"/> weekdays, all day

Select Baseline Adherence Level

Select the adherence level used for determining the extent to which values for the baseline calculation affect the threshold values for all monitor measurements. The higher the adherence level, the closer the values used to update the thresholds are to the values calculated by the baseline. To fine-tune the adherence level for individual monitor measurements or to set the Good Boundary, click **Fine-Tune Adherence Levels/Set Boundary**.

High Adherence
 Medium Adherence
 Low Adherence

[Fine-Tune Adherence Levels/Set Boundary](#)

Example - Fine-Tune Adherence Levels/Set Boundary

Fine-Tune Adherence Levels/Set Boundary

Displays the value used in the baseline calculation at each adherence level (percentile value) and the Good Boundary (actual value) for each monitor measurement in the selected context. Click 'Edit' to modify the default percentiles or boundary value.

1 / 1 Pages

Monitor Type : Measurement Name	Warning Percentiles			Error Percentiles			Good Boundary		
	Low	Medium	High	Low	Medium	High			
CPU : utilizationPercentage	110	93	90	120	98	95		Edit	Reset
Memory : percentFull	110	93	90	120	98	95		Edit	Reset
Memory : freeSpace	110	93	90	120	98	95		Edit	Reset
Memory : pageFaultsPerSecond	110	93	90	120	98	95		Edit	Reset
All browsable monitor's measurements	110	93	90	120	98	95		Edit	Reset

3 Review the Baseline Settings

Review the summary of calculated monitors and baseline data. For details on the user interface, see “Review & Activate Dialog Box” on page 536.

Example

Review & Activate

Review the list of monitors on which baseline configuration can be performed. Since you cannot undo changes after clicking **Activate**, it is recommended that you first save a backup of the current configuration by clicking **Backup Configuration**.

Baseline calculation succeeded for 9 SiteScope monitors. Backup Configuration

	SiteScope Monitor Name	Calculation Date	Error Status Reduction ▲	Warning Status Reduction	Threshold Graphs
<input checked="" type="checkbox"/>	SiteScope\docs\Basic\CPU Utilizatio	12/16/2007	1	0	View Graphs
<input checked="" type="checkbox"/>	SiteScope\docs\Basic\Directory: c:\	12/16/2007	0	0	View Graphs
<input checked="" type="checkbox"/>	SiteScope\docs\Basic\DisabledGrou	12/16/2007	0	0	View Graphs
<input checked="" type="checkbox"/>	SiteScope\docs\Basic\Disk Space: C	12/16/2007	0	0	View Graphs
<input checked="" type="checkbox"/>	SiteScope\docs\Basic\FTP on localh	12/16/2007	1	1	View Graphs
<input checked="" type="checkbox"/>	SiteScope\docs\Basic\Link Check: h	12/16/2007	2	0	View Graphs
<input checked="" type="checkbox"/>	SiteScope\docs\Basic\Memory on Si	12/16/2007	0	0	View Graphs
<input checked="" type="checkbox"/>	SiteScope\docs\Basic\Service: HTTP	12/16/2007	0	0	View Graphs
<input checked="" type="checkbox"/>	SiteScope\docs\Basic\URL List	12/16/2007	2	0	View Graphs

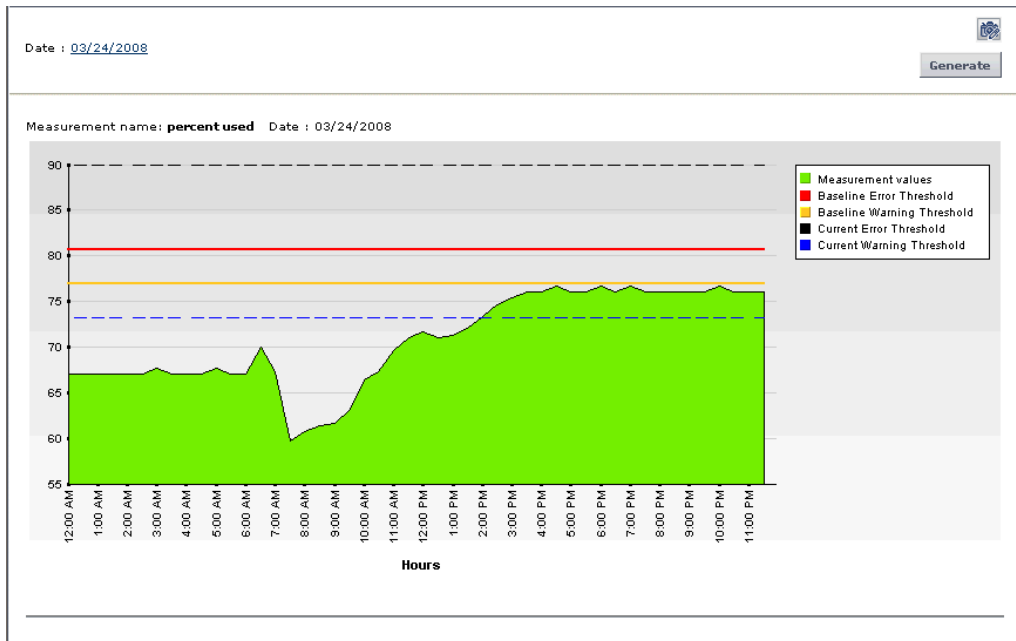
Activate
Cancel
Help

4 View the Baseline Monitor Measurements Graphs

You can view a graphical display of each monitor’s baselined measurements to analyze the baseline data for a selected day. You can also use the annotation tool to create a snapshot of the graph you are viewing and highlight important areas. For details on the user interface, see “Baseline Monitor Measurement Graphs Dialog Box” on page 541.

Note: The data displayed in the graphs is an aggregate of the measurement data and as such, the time periods may not accurately reflect the time the data was actually collected.

Example



5 Activate the Baseline Settings

Select the monitors for which you want to set thresholds using a baseline, and click **Activate**. By default, all monitors with a successfully calculated baseline are selected for baseline threshold configuration. The monitor thresholds are configured according to the baseline calculation, and are set to change status when the settings are exceeded. For details on the user interface, see “Review & Activate Dialog Box” on page 536.

Note: If you want to revert to the current monitor configuration, select the option to save the current monitor configuration before activating the baseline configuration.

6 View Baseline Properties in the Status Report

You can create an ad hoc report showing information about each monitor in the selected context, including each monitor’s baseline status and baseline status description. For details on the user interface, see “Status Report” on page 545. You can also track the baseline status for a monitor in the monitor’s Main Settings. For details on the user interface, see “Main Settings” on page 510.


Example

Status Report			
Displays information about the baseline status for all monitors in the selected context.			
Total of 9 monitors. 8 monitors are in calculation process. 1 are not baselined.			
			/1 Pages
SiteScope Monitor Name ▲	SiteScope Monitor Type	Baseline Status	Baseline Status Details
CPU Utilization on SiteScope Server	CPU	Calculating baseline	Finished reading the log files.
Directory: c:\ on SiteScope Server	Directory	Calculating baseline	Finished reading the log files.
DisabledGroup\disabledMonitor	CPU	Monitor not selected for baselining	
Disk Space: C on SiteScope Server	Disk Space	Calculating baseline	Finished reading the log files.
FTP on localhost	Port	Calculating baseline	Finished reading the log files.
Link Check: http://www.google.com	Link Check	Calculating baseline	Finished reading the log files.
Memory on SiteScope Server	Memory	Calculating baseline	Finished reading the log files.
Service: HTTP on SiteScope Server	Service	Calculating baseline	Finished reading the log files.

7 View and Modify Baseline Thresholds

In the Threshold Settings, you can view the baseline thresholds and manually fine-tune the thresholds by changing the percentile value from which the threshold value is derived. For details on the user interface, see “Threshold Settings” on page 518.

Example

In the example, the **Error if percent used (%)** threshold value is 73.22 (non-editable) and the percentile value is 98. To change the threshold value, you must change the percentile value from which the threshold value is derived. To help you understand what the new threshold value will be after you change the percentile value, click the **Percentiles Table**  button to open the percentile table that shows the threshold value mapped to each percentile range.

Threshold Settings

If Unavailable: Set monitor status according to Thresholds

Default status: Good

Error if

<input type="checkbox"/>	percent used (%)	>=	73.22	98		every day, all day
<input type="checkbox"/>	percent used (%)	=	'n/a'			every day, all day
<input type="checkbox"/>	percent used (%)	>	90			every day, all day

X New Error if

Warning if

<input type="checkbox"/>	percent used (%)	>=	69.74	93		every day, all day
--------------------------	------------------	----	-------	----	--	--------------------

X New Warning if

Good if

<input type="checkbox"/>	always (default)	>=				every day, all day
--------------------------	------------------	----	--	--	--	--------------------

X New Good if

Note: The **Error if percent used (%) > 90** threshold is the error boundary. This is the value of a measurement considered to be in error status, even though according to existing baseline percentiles it should not report an error. For example, if the baseline threshold were updated to **Error if percent used (%) >= 96**, all measurements greater than 90 are in error status, even if the calculated baseline error threshold of 96 is not exceeded. For details on this topic, see “Error Boundary” on page 484.

Monitors Supported in Windows Environments Only

The following table lists the SiteScope monitors that are supported on Windows versions of SiteScope only. The servers that are being monitored can be running on either Windows or UNIX platforms.

Monitor Type
ASP Server Monitor
Browsable Windows Performance Counter Monitor
Citrix Server Monitor
ColdFusion Server Monitor
DB2 Monitor
IIS Server Monitor
MAPI Monitor
Microsoft Exchange 2003 Mailbox Monitor
Microsoft Exchange 2003 Message Traffic Monitor
Microsoft Exchange 2007 Message Traffic Monitor
Microsoft Exchange 2003 Public Folder Monitor
Microsoft Exchange 5.5 Message Traffic Monitor
Microsoft SQL Server Monitor
Microsoft Windows Dialup Monitor
Microsoft Windows Event Log Monitor
Microsoft Windows Media Player Monitor
Microsoft Windows Media Server Monitor
Microsoft Windows Performance Counter Monitor
Microsoft Windows Resources Monitor
Microsoft Windows Services State Monitor
Monitor Load (SiteScope Health) Monitor

Monitor Type
Network Monitor
Real Media Player Monitor
Real Media Server Monitor
SAP CCMS Monitor
Sybase Monitor
Tuxedo Monitor

Ports Used for SiteScope Monitoring

The following table lists the network ports that are generally used for SiteScope monitoring. In many cases, alternate ports may be configured depending on the security requirements of your environment.

Monitor Type	Ports Used
Apache Server Monitor	Port which Apache Server Admin pages located. Configurable by using server configuration file.
ASP Server	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
BroadVision App Server	Uses the Object Request Broker (ORB) port number for the BroadVision server you are trying to monitor.
Checkpoint Firewall -1	SNMP monitor. Default is port 161.This is configurable.
Cisco Works	Cisco Works resources are usually available by using port 161 or 162 (SNMP), depending on the configuration of the server.
Citrix Server	Ports 137, 138, and 139 (NetBIOS).
ColdFusion Server	Ports 137, 138, and 139 (NetBIOS).
CPU Utilization	For local CPU, no ports required. For CPUs on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS). For CPUs on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).
Database Query	This is configurable and depends on ODBC or JDBC driver and DB configuration.
DB2	Default is port 50000. This is configurable.
DHCP	Default is port 68.

Monitor Type	Ports Used
Directory	<p>For local directory, no ports required.</p> <p>For directories on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS).</p> <p>For directories on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).</p>
Disk Space	<p>For local disk space, no ports required.</p> <p>For disk space on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS).</p> <p>For disk space on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).</p>
DNS	Default is port 53.
Dynamo Application	Uses SNMP. This is configurable.
F5 Big IP	Uses SNMP. This is configurable.
File	<p>Local disk. No ports required.</p> <p>For files on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS).</p> <p>For files on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).</p>
FTP	Default is port 21. This is configurable.
IIS Server	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
iPlanet Server	Configurable by using the iPlanet server administration page.
LDAP	The default is port 389. This is configurable.
Link Check	The default is port 80. This is configurable.
Log File	<p>Ports 137, 138, and 139 (NetBIOS) for Windows based systems.</p> <p>Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.</p>

Monitor Type	Ports Used
Mail	Port 110 for POP3, port 25 for SMTP, port 143 for IMAP.
MAPI	MAPI uses the Name Service Provider Interface (NSPI) on a dynamically assigned port higher than 1024 to perform client-directory lookup.
Memory	Ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Microsoft SQL Server	Ports 137, 138, and 139 (NetBIOS).
Microsoft Windows Media Player	Same port as media content to be monitored.
Microsoft Windows Media Server	Ports 137, 138, and 139 (NetBIOS).
Microsoft Windows Performance Counter	Ports 137, 138, and 139 (NetBIOS).
Network	No ports required; monitors only the local machine.
News	Default is port 144. This is configurable.
NT Event Log	Ports 137, 138, and 139 (NetBIOS).
Oracle Database (JDBC)	This is configurable. Depends on target DB. Default is port 1521.
Oracle9i App Server	This is configurable. Port which Webcaching admin page located.
Ping	Default is port 7.
Port	Monitors any port.

Monitor Type	Ports Used
Radius	<p>Currently supports Password Authentication Procedure (PAP) authentication but not the Challenge Handshake Authentication Protocol (CHAP) or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). The RADIUS servers must be configured to accept PAP requests. Default is port 1645. In recent changes to the RADIUS spec, this may be changed to 1812. The monitor is configurable.</p>
Real Media Player	<p>Uses Real Media client on SiteScope box. Uses the port from which the media content is streamed (based on the URL).</p>
Real Media Server	<p>Ports 137, 138, and 139 (NetBIOS).</p>
RTSP	<p>Uses the port from which the media content is streamed.</p>
SAP	<p>Uses SAP Client software (SAP Front End) to run certain SAP transactions. Therefore, same ports as SAP.</p>
Script	<p>Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.</p>
Service	<p>Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.</p>
SilverStream	<p>Configurable URL (Port number included in URL) to the applicable SilverStream server administration web page.</p>
SNMP	<p>Default is port 161. This is configurable.</p>
SNMP Trap	<p>Uses port 162 for receiving traps. This is configurable.</p>

Monitor Type	Ports Used
SunOne Webserver	URL to the stats-xml file on the target SunONE server. The port is configurable.
Sybase	Monitor requires Sybase Central client on the machine where SiteScope is running to connect to the Adaptive Server Enterprise Monitor Server. Port number the same as Sybase client.
Tuxedo	The default port for the TUXEDO workstation listener is port 65535. This is configurable.
URL	Generally port number 80. This is configurable.
Web Server	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Web Service	This is configurable.
WebLogic App Server	BEA WebLogic Application Server monitor uses the Java JMX interface. Port is configurable.
WebSphere App Server	Same port as the IBM WebSphere Administrator's Console.
WebSphere Performance Servlet	WebSphere Performance Servlet. Port is configurable.

SiteScope Monitors User Interface

This section describes:

- New SiteScope Monitor Page on page 508
- Common Monitor Settings on page 510
- Percentile Range Mapping Table on page 526
- Select Monitors for Baseline Calculation Dialog Box on page 528
- Baseline Calculation Advanced Settings Dialog Box on page 529

- ▶ Fine-Tune Adherence Levels/Set Boundary Dialog Box on page 532
- ▶ Edit Adherence Levels and Good Boundary Dialog Box on page 534
- ▶ Review & Activate Dialog Box on page 536
- ▶ Failed Baseline Calculations Dialog Box on page 539
- ▶ Baseline Monitor Measurement Graphs Dialog Box on page 541
- ▶ Status Report on page 545

New SiteScope Monitor Page

<p>Description</p>	<p>Enables you to define a new monitor in a monitor group.</p> <p>To access: Right-click a monitor group. Select New Monitor.</p> <p>Alternatively, select a monitor group, and click the Contents tab in the right pane. Click the New Monitor button.</p>
<p>Important Information</p>	<ul style="list-style-type: none"> ▶ Monitors can be created only in a SiteScope group. ▶ You cannot delete a monitor if it has dependent alerts or reports at the container level. To delete a monitor with dependencies, you must remove the monitor from Alert Targets and Monitors and Groups to report on in the Main Settings for each dependency, and then delete the monitor. You can delete monitors that have dependencies at the child level. ▶ HTML code entered in monitor description fields is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected.
<p>Included in Tasks</p>	<p>“Deploy a Monitor – Workflow” on page 489</p>

The following elements are found in the New Monitor page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Recently Used Monitors	<p>Select a monitor from a display of monitors that were recently added to the SiteScope Monitor Groups.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ The five most recently selected monitors are listed here. ▶ The displayed monitors may change as more selections are made.
Monitors List and Category Filter	<p>You select a monitor to deploy by selecting it from the full list of available monitors or by one of the following:</p> <ul style="list-style-type: none"> ▶ Monitor: Type a monitor name in the Monitor box. To search for a monitor name, you can also enter a regular expression. ▶ Category: Click the arrow to the right to select a monitor category from the list detailed below. <p>Note: Click on the arrow in the header of the Monitor column to change the alphabetical order (ascending or descending) of the listed monitors.</p>
Category	<p>You can add a monitor by selecting one of the following categories and clicking on a monitor in that category:</p> <ul style="list-style-type: none"> ▶ Application Monitors ▶ Database Monitors ▶ Generic Monitors ▶ Integration Monitors Overview ▶ Network Monitors ▶ Server Monitors ▶ Stream Monitors ▶ Web Transaction Monitors

Common Monitor Settings

The following monitor settings tabs contain the common GUI elements on the New Monitor page. For details on other monitor elements not listed here, see the user interface page for the specific SiteScope monitor.

Note: HTML code entered in monitor text boxes is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected.

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Name	<p>Type a name that describes the element or system being monitored. Use a useful naming convention for all monitors to make creating view filters and category assignments more effective.</p> <p>Example: <hostname:resource_type> or <business_unit resource_name monitored_element></p> <p>Default value: SiteScope creates a default name based on the host, system, and/or URL being monitored or the default name defined for the monitor type.</p>
Frequency	<p>Set how often SiteScope attempts to run the action defined for the monitor instance. Each monitor run updates the status of the monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p>Default value: Monitor runs once every 10 minutes.</p> <p>Minimum value: 15 seconds</p>

GUI Element	Description
Baseline mode	<p>This option is available, and selected by default, only after a baseline threshold has been calculated for the monitor (even if the baseline calculation failed). When this option is selected, you can view and manually update the baseline thresholds (if successfully created) in the Threshold Settings. For details on this topic, see “Setting Status Thresholds” on page 476.</p> <p>Clear this option to disable baseline thresholds. When Baseline mode is cleared, the baseline thresholds are removed and the static threshold value is used to create a threshold. You can recalculate the baseline thresholds only when this option is cleared. For details on this topic, see “Setting Status Thresholds Using a Baseline” on page 478.</p>
Baseline status	<p>Indicates the monitor’s baseline status. The following statuses are available:</p> <ul style="list-style-type: none"> ▶ Monitor not selected for baselining. The monitor has not been selected for baselining. ▶ Calculating baseline. SiteScope is in the process of calculating the baseline. ▶ Calculation failed. SiteScope was unable to calculate a baseline. ▶ Calculated, not activated. A baseline was calculated for the monitor, but it has not yet been activated. ▶ Activating baseline. SiteScope is in the process of activating the baseline. ▶ Activation failed. SiteScope was unable to activate the baseline. ▶ Baseline activated. The baseline has been activated for the monitor. <p>The Baseline mode check box is selected if the baseline status is anything other than Monitor not selected for baselining.</p> <p>For details on using the baseline threshold, see “Setting Status Thresholds Using a Baseline” on page 478.</p>

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Show Run Results on Update	<p>Whenever a change is made to a monitor's configuration settings, the monitor is run. Select this option to display the results of that monitor run in a popup dialog box.</p> <p>Note: The updated run results are always displayed in the applicable dashboard views for the monitor.</p>
Verify Error	<p>Select to automatically run the monitor again if it detects an error.</p> <p>Note: It is recommended not to use this option in large monitoring environments. Significant monitoring delays may result if multiple monitors are rescheduled to verify errors at the same time.</p> <p>The status returned by the Verify Error run of the monitor replaces the status of the originally scheduled run that detected an error. The data from the verify run may be different than the initial error status, causing the loss of important performance data.</p>
Error Frequency	<p>Set a new monitoring interval for monitors that have reported an error condition.</p> <p>Example: You may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected. When the monitor's status is no longer in error, the monitor reverts to the run interval specified in the Frequency setting.</p> <p>Note: Increasing the run frequency of a monitor affects the number of alerts generated by the monitor.</p>

GUI Element	Description
Monitor Schedule	<p>Select a schedule if you want the monitor to run only on certain days or on a fixed schedule. The schedules created in Preferences appear in the drop-down list. For more information about creating monitor schedules, see “Range Schedule Preferences” on page 225.</p> <p>Default value: every day, all day</p> <p>Note: If you select a threshold schedule in the Threshold Settings, at least one threshold schedule must coincide with the monitor run schedule (at least one minute of the monitor run schedule must be covered by one of the threshold schedules).</p>
Depends On	<p>Select to make the running of this monitor dependent on the status of another monitor.</p> <p>In the representation of the monitor tree, expand the group node and select the check box next to the monitor to which to you want to create dependence.</p> <p>To remove dependence on a monitor, clear the required check box.</p> <p>Use this option to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system.</p> <p>Example: Create a system monitor to check the basic availability of a system and then create other monitors that perform more detailed tests of that system. Set the detailed test monitors to be dependent on the status of the monitor checking basic availability.</p> <p>If the system monitor detects that the target system has become unavailable, the dependency relationship automatically disables the other monitors. This also disables any alerts that would have been generated by the dependent monitors.</p> <p>Default value: No dependency is set for a monitor instance.</p>

GUI Element	Description
<p>Depends Condition</p>	<p>If you make this monitor dependent on the status of another monitor (by using the Depends On setting), use this option to select the status condition of the Depends On monitor for the current monitor to run normally.</p> <p>The status categories include:</p> <ul style="list-style-type: none"> ➤ Good ➤ Error ➤ Available ➤ Unavailable <p>The monitor being configured is run normally as long as the monitor selected in the Depends On box reports the condition selected in this box.</p> <p>Example: Select Good and this monitor is enabled only when the monitor selected in the Depends On box reports a status of Good. The current monitor is automatically disabled if the monitor selected in the Depends On box reports a category or condition other than Good. You can also enable dependent monitors specifically for when a monitor detects an error.</p>

GUI Element	Description
Monitor Description	<p>Type additional information to describe a monitor. The Monitor Description can include HTML tags such as the
, <HR>, and tags to control display format and style. The description text appears on the Content tab for the group to which the monitor belongs and in the Dashboard if the Description parameter is a selected column.</p> <p>Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> ➤ Tags: script, object, param, frame, iframe. ➤ Any tag that contains an attribute starting with on is declined. For example, <code>onhover</code>. ➤ Any attribute with javascript as its value.
Report Description	<p>Type an optional description for this monitor to make it easier to understand what the monitor does. This description is displayed on each bar chart and graph in Management Reports.</p> <p>Example: Network traffic or main server response time.</p> <p>Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> ➤ Tags: script, object, param, frame, iframe. ➤ Any tag that contains an attribute starting with on is declined. For example, <code>onhover</code>. ➤ Any attribute with javascript as its value.

Enable/Disable Monitor

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Enable Monitor	If the monitor has previously been disabled, select to enable the monitor. Default value: Selected
Disable Monitor Indefinitely	When a monitor has been disabled, SiteScope continues to schedule the monitor to run based on the Frequency setting for the monitor but the monitor action is not run. SiteScope records a monitor data log entry for the monitor when it was scheduled to be run but reports the monitor status as disabled in the place of measurement data.
Disable Monitor for the Next Time Period	Type a time period that the monitor should remain disabled. Select seconds, minutes, hours, or days to define the disable time period as applicable.
Disable Monitor on a One Time Schedule	Use this option to temporarily disable the monitor for a time period in the future. The time period can span more than one day. Type the start time and end time for the disable period using the format hh:mm. Type the start and end dates for the disable period using the mm/dd/yy format.
Disable Description	Type optional descriptive text. This description appears as part of the monitor status in the monitor group display. The disable status text also includes a string indicating which disable option is in force for the monitor, for example Disabled manually indicates that the monitor was disabled using the Disable Monitor Indefinitely option.

Enable/Disable Alert

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Disable Alerts with respect to this monitor	<p>Displays all the alerts, within a monitor tree hierarchy, that are associated with the current monitor instance, including alerts added to the monitor's parent group or to the SiteScope.</p> <p>If no alerts have been configured for this monitor instance, the monitor's parent group, or globally for the SiteScope, a message appears instead of the alert list.</p>
Enable All Associated Alerts	<p>If the alerts associated with this monitor have previously been disabled, select to enable the alerts.</p> <p>Default value: Selected</p>
Disable All Associated Alerts for the Next Time Period	<p>Type a time period that the associated alerts should remain disabled. Select seconds, minutes, hours, or days to define the disable time period as applicable.</p>
Disable All Associated Alerts on a One Time Schedule	<p>Use this option to temporarily disable the associated alerts for a time period in the future. The time period can span more than one day.</p> <p>Type the start time and end time for the disable period using the format hh:mm. Type the start and end dates for the disable period using the mm/dd/yy format.</p>
Disable Description	Type optional descriptive text.

Threshold Settings


<p>Description</p>	<p>Use to set conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system during a specified period of time.</p> <p>Status threshold criteria for each monitor instance can be set for the following status conditions:</p> <ul style="list-style-type: none"> ➤ Error if ➤ Warning if ➤ Good if <p>Note: You can also set monitor thresholds using a baseline. For details, see “Setting Status Thresholds Using a Baseline” on page 478.</p>
<p>Important Information</p>	<ul style="list-style-type: none"> ➤ You can apply multiple status threshold criteria for each status condition per monitor instance. A single monitor instance may have one or more criteria used to determine Error status, one or more conditions to determine Warning status, and one or more conditions to indicate Good status. Most monitor types include one default setting for each of the three status conditions. ➤ When setting a baseline threshold, you can only change certain threshold conditions during the baseline calculation and after the baseline is activated. For details on the threshold changes that are allowed, see “Changing Threshold Settings” on page 523. ➤ When working with Global Search and Replace, if you select to replace threshold settings, the Override Category option appears. When selected, all the threshold settings for the selected monitor instances are overridden with the settings you entered for the replace operation. If this option is cleared and you selected to replace threshold settings, the settings you entered are added to the existing threshold settings for the monitor instances.

Included in Tasks	<p>“Deploy a Monitor – Workflow” on page 489</p> <p>“Set Monitor Thresholds Using a Baseline” on page 493</p>
Useful Links	<p>“Setting Status Thresholds” on page 476</p> <p>“Setting Status Thresholds Using a Baseline” on page 478</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
If Unavailable	<p>Select a status assignment for when the monitor is not available from the following options:</p> <ul style="list-style-type: none"> ▶ Set monitor status according to thresholds. The monitor gets a new status according to the thresholds. ▶ Set monitor status to Good. The monitor’s status is set to Good when it is unavailable without thresholds being checked. ▶ Set monitor status to Warning. The monitor’s status is set to Warning when it is unavailable without thresholds being checked. ▶ Set monitor status to Error. The monitor’s status is set to Error when it is unavailable without thresholds being checked. <p>Note: A monitor instance can have a status of Unavailable as well as a status of Good, Warning, or Error. Alerts are triggered according to availability, status, or both availability and status, depending on how the alert is configured. For details, see “SiteScope Alerts Overview” on page 1386.</p>
Default status	<p>The status of the monitor (Good, Warning, or Error) if the threshold criteria for the monitor instance are not met.</p> <p>Default value: Good</p>
Error if	<p>Set the conditions for the monitor instance to report an Error status.</p>

GUI Element	Description
<measurement>	<p>Select the measurement parameter from the drop-down list to determine the status of this monitor instance. The list of measurements is dynamically updated based on the type of monitor you are configuring.</p> <p>Default value: Default measurements exist for many monitor types and differ per monitor type. For many default measurements, there are corresponding defaults for the operator and value boxes.</p>
<operator>	<p>Select an operator for the measurement from the drop-down list. The corresponding value is entered in the next box.</p> <ul style="list-style-type: none"> ▶ >= Greater than or equal to ▶ > Greater than ▶ == Equals ▶ != Not the same as ▶ <= Less than or equal to ▶ < Less than ▶ contains Contains the value entered ▶ !contains Does not contain the value entered
<measurement value>	<p>Type a value applicable to the measurement parameter in the box following the operator selected.</p> <p>Note: If a monitor has an activated baseline, its measurement values are non-editable and are displayed in grey. You can edit the baseline measurement value only by changing the current percentile value.</p>

GUI Element	Description
<current percentile>	<p>(Only displayed for monitors with an activated baseline)</p> <p>Displays the percentile value used by the baseline calculation engine to calculate the baseline threshold. You can change the baseline threshold value by modifying the current percentile value. Click the Percentiles Table  button to view the actual value that corresponds to the percentile value, and update the percentile value accordingly. For details on the user interface, see “Percentile Range Mapping Table” on page 526.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ You cannot change the measurement value, operator or schedule for threshold conditions that include the current percentile value. ▶ You can set the current percentile to a value over 100%. This enables you to raise the threshold level above the level that would have been set, based on the sample measurements collected. For example, if measurements collected for CPU Utilization are between 10%-60%, and you only want to get errors above 80% CPU Utilization, set the percentile value to a percentile that raises the error threshold level to the desired level. In this instance, set the percentile to 134% (60% CPU Utilization * 134% = 80.4% CPU Utilization).

GUI Element	Description
<schedule>	<p>Select a schedule to determine the status of this monitor instance if you want to define when to check the monitor run result against the threshold. This is useful, for example, if you want to check the monitor run result against the threshold only on certain days or during peak hours. The schedules created in Preferences appear in the drop-down list. For more information about creating monitor schedules, see “Range Schedule Preferences” on page 225.</p> <p>Default value: every day, all day</p> <p>Note: When selecting threshold schedules, at least one threshold schedule must coincide with the Monitor Schedule in the Advanced Settings (at least one minute of the monitor run schedule must be covered by one of the threshold schedules).</p>
New Error if	<p>Click this button to configure additional thresholds that determine Error status. For each threshold, select the measurement and operator, and type a value for the measurement.</p> <p>By default, two thresholds are displayed when you first configure the monitor.</p>
Warning if	<p>Set the conditions for the monitor instance to report a Warning status. For each threshold, select the measurement and operator, and type a value for the measurement.</p>
New Warning if	<p>Click this button to configure additional thresholds that determine Warning status. By default, only one threshold is displayed when you first configure the monitor.</p>
Good if	<p>Set the conditions for the monitor instance to report a Good status. For each threshold, select the measurement and operator, and type a value for the measurement.</p>
New Good if	<p>Click this button to configure an additional threshold that determines Good status. By default, only one threshold is displayed when you first configure the monitor.</p>

Changing Threshold Settings

You can make changes to threshold conditions according to the baseline status of the monitor instance.

Monitor Baseline Status	Change Threshold Condition	Add/Delete Threshold Condition
Not Baselined	You can change any condition of any threshold.	Allowed
In Calculating/ Activating Process	You can only change the measurement value for static thresholds. For example, Error if CPU \geq 70 every day, all day, you can only change the value 70 to another value.	Not Allowed
Baselined	<ul style="list-style-type: none"> ➤ You can change any condition for static thresholds. ➤ You can only change the percentile value for baseline thresholds. 	Allowed for static thresholds only

Link Monitor to CI

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Select CIs button	<p>You can link between this monitor instance and any existing, logical configuration item (CI) in HP Business Availability Center's Universal configuration management history database. This link or relationship enables the monitor to pass KPI status to the CI to which it is linked. This is in addition to the monitor's corresponding CI that is created automatically when the monitor instance is created.</p> <p>The Select CIs button opens the dialog box in which you select an existing CI from a CMDDB view to link to this monitor instance. For details on selecting and working with views, see "View Explorer" in <i>Reference Information</i>.</p> <p>Note: The Link Monitor to CI Settings are available only when adding a SiteScope monitor and cannot be set while editing a monitor.</p>

Custom Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<custom property>	<p>This area lists those custom properties that have been created for this SiteScope. If no custom properties have been created, this section appears but is empty. If custom properties have been created, they are listed here and you configure as needed.</p> <p>For details on creating custom properties, see "Creating Custom Properties" on page 1581.</p>

HP BAC Logging

Description	Use the HP BAC Logging settings area to control what data a monitor forwards to the HP Business Availability Center database.
Important Information	Your selection should be based on how much data is relevant to report to BAC for this monitor and how much space the BAC database has for this data.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element	Description
Do not report to HP Business Availability Center	Select when you do not want any of the measurements for this monitor to be transferred to HP Business Availability Center.
Report everything (all monitors and all measurements)	Select to send all monitor data to HP Business Availability Center for each time that the monitor runs. This option enables the largest data transfer load.
Report monitor level data (no measurements)	Select this option to send only monitor category (error, warning, good), status string, and other basic data for each time that the monitor runs. No information on specific performance counters is included.
Report monitor level data and measurements with thresholds	Select to send monitor category (error, warning, good), status string, as well as performance counter data for only those measurement counters that have thresholds configured thresholds (for example, Error If, Warning If, etc.). The data is sent for each time that the monitor is run.
Report status changes (no measurements)	Select to send only monitor category (error, warning, good), status string, and other basic data only when the monitor reports a change in status. No information on specific performance counters is included. This option enables the smallest data transfer load.

Category Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Assigned categories	<p>The Category settings are used to filter items in the monitor tree. If no categories have been created for the SiteScope, this section appears but is empty. If categories have been created, they are listed here and you configure as needed.</p> <p>For details on creating categories, see “Working with Categories” on page 197.</p>

Percentile Range Mapping Table

Description	<p>Displays the actual value that is mapped to each percentile range. SiteScope uses the percentile value to define the baseline error and warning thresholds.</p> <p>Use this table to choose the appropriate actual value when you manually change the percentile value.</p> <p>To access: In the monitor tree, right-click a monitor with an activated baseline, and click Edit. Expand Threshold Settings, and click the Percentiles Table  button.</p>
Important Information	This table is available for monitors with an activated baseline only.
Included in Tasks	“Set Monitor Thresholds Using a Baseline” on page 493
Useful Links	“Setting Status Thresholds Using a Baseline” on page 478

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Percentiles Ranges	<p>The percentile range that correlates to the actual value used for defining the baseline error and warning thresholds. You can set the number of percentile ranges displayed in the table from the SiteScope Preferences (Preferences > Infrastructure Settings Preferences > Baseline Settings).</p> <p>Note: The left-hand value is exclusive and the right-hand value is inclusive. This means that for a percentile range of 33-100, all values above 33 (but not 33 itself) up to 100 are included in the range. The value 33 falls into the previous range and 100.01 falls into the next range.</p>
Actual Value	The actual value that is mapped to the percentile range.

Select Monitors for Baseline Calculation Dialog Box

Description	Use to select the groups and/or monitors to include in the baseline calculation, to configure advanced settings, and to calculate the baseline threshold. To access: In the monitor tree, right-click the SiteScope container, a group, or a monitor, and select Baselining > Calculate .
Included in Tasks	“Set Monitor Thresholds Using a Baseline” on page 493
Useful Links	“Setting Status Thresholds Using a Baseline” on page 478

The following elements are included (unlabeled GUI elements are shown in angle brackets):


GUI Element	Description
<List of available groups and/or monitors>	Select the groups and/or monitors to include in calculating the baseline threshold. The list includes the currently selected container and all of the child containers. Default value: The current container and all child elements are selected. Note: You cannot select a monitor instance if: <ul style="list-style-type: none"> ➤ its baseline has already been activated ➤ there is another monitor in SiteScope with the same name (the file path, group name, and monitor name are identical). In such cases, Duplicate name is displayed next to the monitor name.

GUI Element	Description
Advanced Settings	Click to open the Baseline Calculation Advanced Settings dialog box. You can select the relevant schedule time range for collecting baseline data and the baseline adherence level. For details, see “Baseline Calculation Advanced Settings Dialog Box” on page 529.
Calculate	<p>Click to perform the baseline threshold calculation. The amount of time required to calculate the baseline thresholds depends on the speed of the SiteScope server and the number of monitors selected for baselining. If SiteScope needs to restart before the calculation process is complete, SiteScope automatically continues the process after the restart.</p> <p>Note: You should enable the monitors to run for a period that is long enough for SiteScope to accumulate sufficient data to calculate the baseline. This period depends on the Minimum number of days required for baselining and Minimum number of samples required for baselining settings in Baseline Settings of Infrastructure Settings Preferences. For details, see “Baseline Settings” on page 273.</p>

Baseline Calculation Advanced Settings Dialog Box

Description	<p>Enables you to choose the relevant time range schedule for collecting baseline data, and select the adherence level that determines the extent to which monitor measurement sample values used in calculating the baseline affect the threshold values. You can also fine-tune the adherence level for individual monitor measurements, and set the Good Boundary.</p> <p>To access: In the monitor tree, right-click the SiteScope container, a group, or a monitor, and select Baselining > Calculate. Click the Advanced Settings button.</p>
Included in Tasks	“Set Monitor Thresholds Using a Baseline” on page 493
Useful Links	“Setting Status Thresholds Using a Baseline” on page 478

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element	Description
	<p>Change the sort order in the Schedule Range Name column by clicking the up and down arrow in the column title.</p> <p>Default: The Schedule Range Name column is in alphabetical order, from top to bottom.</p>
<p>Schedule Range Name</p>	<p>Select the schedule ranges used for collecting baseline threshold data. This enables you to restrict to certain days or hours of the week the periods during which monitor data is collected for the baseline calculation. The baseline thresholds that are created are only effective for the same schedule range period. The schedules created in Range Schedule Preferences appear in the drop-down list. For more information about creating monitor schedules, see “Range Schedule Preferences” on page 225.</p> <p>Default value: If no schedule range is selected, baseline threshold data is collected all day, every day (the default option is not displayed).</p>

GUI Element	Description
Select Baseline Adherence Level	<p>Enables you to select the adherence level used for determining the extent to which values for the baseline calculation affect the threshold values. The adherence level is based on a percentile value that is applied to all monitor measurements to determine when a measurement is in error or warning.</p> <ul style="list-style-type: none"> ▶ High. The closer the values used to update the thresholds are to the values calculated by the baseline. Select this option if you are less tolerant to extreme measurement values having an effect on the baseline. ▶ Medium. (Default) The values used to update the thresholds are at a mid-range from the values calculated by the baseline. ▶ Low. The further the values used to update the thresholds are from the values calculated by the baseline. Select this option if you are more tolerant to extreme measurement values having an effect on the baseline. <p>For more details on this topic, see “Setting the Baseline Adherence Level” on page 482.</p>
Fine-Tune Adherence Levels/Set Boundary	<p>Click to open the Fine-Tune Adherence Levels/Set Boundary dialog box. Enables you to fine-tune the baseline adherence level and define a good boundary for any measurement of any monitor type within the selected context. For details on the user interface, see “Fine-Tune Adherence Levels/Set Boundary Dialog Box” on page 532.</p>

Fine-Tune Adherence Levels/Set Boundary Dialog Box

Description	<p>Displays the percentile value used in the baseline calculation at each adherence level and the good boundary (if configured), for each monitor measurement in the selected context.</p> <p>This enables you to fine-tune the baseline adherence level and set good boundaries for any measurement of any monitor type.</p> <p>To access: In the monitor tree, right-click the SiteScope container, a group, or a monitor, and select Baselining > Calculate. Click the Advanced Settings button, and then click the Fine-Tune Adherence Levels/Set Boundary button.</p>
Important Information	<p>You can set adherence level percentile values to over 100%. This enables you to raise the threshold level above the level that would have been set, based on the sample measurements collected. For example, if measurements collected for CPU Utilization are between 10%-60%, and you only want to get errors above 80% CPU Utilization, set the Error Percentiles Low value to a percentile that raises the error threshold level to the desired level. In this instance, set the percentile to 134% (60% CPU Utilization * 134% = 80.4% CPU Utilization).</p>
Included in Tasks	<p>“Set Monitor Thresholds Using a Baseline” on page 493</p>
Useful Links	<p>“Setting Status Thresholds Using a Baseline” on page 478</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Change the sort order in the Monitor Type: Measurement Name column by clicking the up and down arrow in the column title.</p> <p>Default: The column is in alphabetical order, from top to bottom.</p>
<p>Monitor Type: Measurement Name</p>	<p>For each monitor in the selected context, displays the measurements that are used in the baseline calculation. It also displays one measurement that represents the measurements for all browsable monitors (at the bottom of the list).</p>
<p>All browsable monitor measurements</p>	<p>Displays the Low, Medium, and High adherence level percentile value that is used to calculate the warning and error baseline threshold for all browsable monitors.</p> <p>Default Warning values: Low 110; Medium 93; High 90</p> <p>Default Error values: Low 120; Medium 98; High 95</p>
<p>Warning Percentiles</p>	<p>Displays the Low, Medium, and High adherence level percentile value that is used to calculate the warning baseline threshold. For more details on this topic, see “Setting the Baseline Adherence Level” on page 482.</p> <p>Default value: Low 110; Medium 93; High 90</p>
<p>Error Percentiles</p>	<p>Displays the Low, Medium, and High adherence level percentile value that is used to calculate the error baseline threshold. For more details on this topic, see “Setting the Baseline Adherence Level” on page 482.</p> <p>Default value: Low 120; Medium 98; High 95</p>

GUI Element	Description
Good Boundary	Displays the actual value for the Good Boundary for each monitor measurement type. This is the value of a measurement that is not considered to be in error status, even though according to existing baseline percentiles it should report an error. For more details on this topic, see “Understanding the Good and Error Boundaries” on page 483. Default value: No value
Edit	Click to edit the adherence level values for error and warning thresholds and set a Good Boundary. For details on the user interface, see “Edit Adherence Levels and Good Boundary Dialog Box” on page 534.
Reset	Click to restore the default error and warning threshold adherence level values for the monitor measurement and to remove the Good Boundary.

Edit Adherence Levels and Good Boundary Dialog Box

Description	Enables you to modify the adherence level percentile value for each measurement that is used to calculate the warning and error baseline threshold. You can also set a Good Boundary. To access: In the monitor tree, right-click the SiteScope container, a group, or a monitor, and select Baselining > Calculate . Click Advanced Settings , and then click Fine-Tune Adherence Levels/Set Boundary . Select a measurement and click Edit .
Included in Tasks	“Set Monitor Thresholds Using a Baseline” on page 493
Useful Links	“Setting Status Thresholds Using a Baseline” on page 478


The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Warning <Adherence Level>	Type a Low, Medium, and High percentile value to use to calculate the warning threshold for the monitor measurement. For more details on this topic, see “Setting the Baseline Adherence Level” on page 482.
Error <Adherence Level>	Type a Low, Medium, and High percentile value to use to calculate the error threshold for the monitor measurement. For more details on this topic, see “Setting the Baseline Adherence Level” on page 482.
Good Boundary	Type an actual value to use to calculate the good boundary for the monitor measurement. This is the value of a measurement that you do not consider to be in error status, even though according to existing baseline percentiles it should report an error. For more details on this topic, see “Understanding the Good and Error Boundaries” on page 483.

Review & Activate Dialog Box

Description	<p>Displays a summary of the calculated monitor's baseline data. You can:</p> <ul style="list-style-type: none"> ▶ Save the current monitor configuration. ▶ View failed operations. ▶ View baseline measurement graphs. ▶ Activate baseline threshold configuration. <p>To access: In the monitor tree, right-click the SiteScope node, a group, or a monitor and select Baselining > Review & Activate.</p>
Important Information	To revert to the current monitor configuration, you must create a backup configuration before activating the baseline configuration.
Included in Tasks	"Set Monitor Thresholds Using a Baseline" on page 493
Useful Links	"Setting Status Thresholds Using a Baseline" on page 478

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Change the sort order of any column by selecting a column title, and then clicking the up and down arrow that is displayed.</p> <p>Default: The SiteScope Monitor Name column is in alphabetical order.</p>
Failed Monitors	<p>Click to open the Failed Baseline Calculations dialog box to display the list of failed monitors. For details of the user interface, see "Failed Baseline Calculations Dialog Box" on page 539.</p> <p>Note: This button is displayed only if SiteScope is unable to calculate a baseline for a monitor.</p>


GUI Element	Description
Backup Configuration	<p>Click to save a backup of the current monitor configuration. In the Backup Configuration dialog box, type the target directory and a name for the backup file, and click Save Configuration. By default, the target directory is the SiteScope installation directory. SiteScope saves a backup file in zip format to the specified location. Use the Configuration Tool to restore the configuration settings. For details, refer to the <i>HP SiteScope Deployment Guide</i> PDF.</p> <p>Note: If you do not create a backup, you cannot revert to the current configuration settings after activating the baseline.</p>
SiteScope Monitor Name	The name of the SiteScope monitor selected for baselining.
Calculation Date	The date on which the baseline was calculated.
Error Status Reduction	<p>The reduction in the number of error statuses for a monitor if the baseline threshold were applied. A negative number indicates an increase in error statuses for a monitor if the baseline threshold were applied.</p> <p>Example: Suppose you manually configure the threshold status for CPU Utilization to Error if $\geq 65\%$ and there are 5 error statuses for the CPU monitor (of which 3 errors are for data samples between 65%-70%, and 2 errors for above 70%). If you have SiteScope calculate the threshold using a baseline and the threshold is set to Error if $\geq 70\%$, Error Status Reduction would be 3.</p> <p>Note: The Error Status Reduction value is based on data collected on the calculation date. If more than three days have elapsed since the calculation date, it is recommended to recalculate the baseline.</p>

GUI Element	Description
Warning Status Reduction	<p>The reduction in the number of warning statuses for a monitor if the baseline threshold were applied. A negative number indicates there would be more warning statuses for a monitor if the baseline threshold were applied.</p> <p>Example: Suppose you manually configure the threshold status for CPU Utilization to Warning if $\geq 55\%$ and there are 3 warning statuses for the CPU monitor (of which 2 warnings are for data samples between 55%-60%, and 1 warnings for above 60%). If you have SiteScope calculate the threshold using a baseline and the threshold is set to Warning if $\geq 60\%$, Warning Status Reduction would be 2.</p> <p>Note: The Warning Status Reduction value is based on data collected on the calculation date. If more than three days have elapsed since the calculation date, it is recommended to recalculate the baseline.</p>
Threshold Graphs	<p>Click the View Graphs link to display a graphical representation of baseline data for all the measurements of the monitor. For details, see “Baseline Monitor Measurement Graphs Dialog Box” on page 541.</p>
Activate	<p>Click to activate the baseline threshold configuration.</p> <p>Note: The amount of time required to activate the baseline threshold depends on the speed of the SiteScope server and the number of monitors selected for baselining. If SiteScope needs to restart before the activation process is complete, SiteScope automatically continues the process after the restart.</p>

Failed Baseline Calculations Dialog Box

Description	<p>Displays the monitors for which SiteScope was unable to calculate a baseline together with the reason for the calculation failure. You can select monitors that failed due to insufficient data, and have SiteScope activate the baseline using the limited measurement samples that were collected.</p> <p>To access: In the monitor tree, right-click the SiteScope node, a group, or a monitor and select Baselining > Review & Activate. Click the Failed Monitors button.</p>
Important Information	This dialog box is available only if SiteScope fails to calculate a baseline for a monitor.
Included in Tasks	“Set Monitor Thresholds Using a Baseline” on page 493
Useful Links	“Setting Status Thresholds Using a Baseline” on page 478

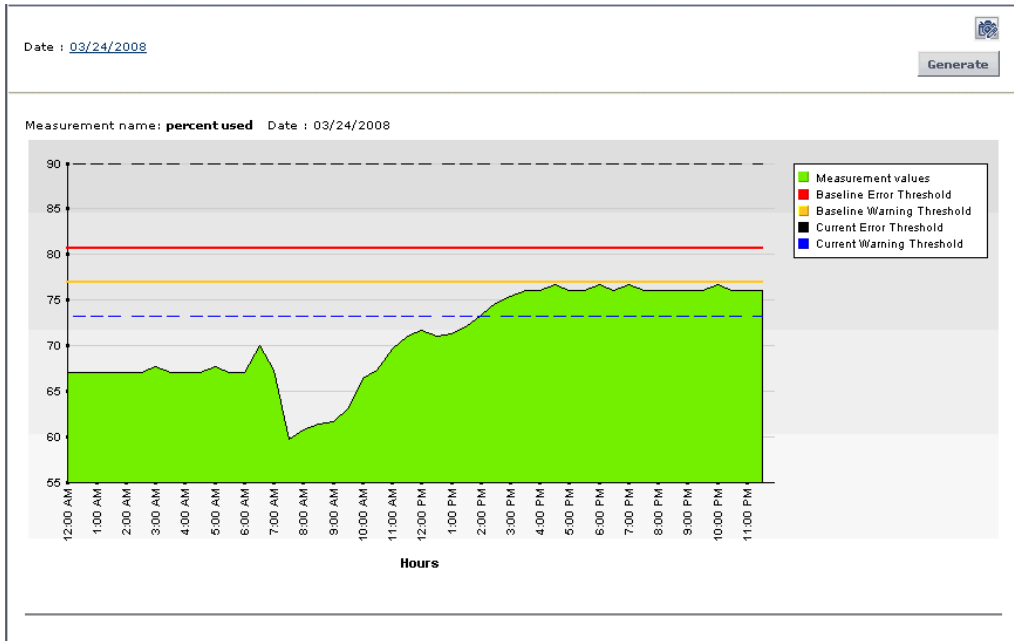
The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Change the sort order in the SiteScope Monitor Name column by clicking the up and down arrow in the column title.</p> <p>Default: The SiteScope Monitor Full Name column is in alphabetical order, from top to bottom.</p>

GUI Element	Description
SiteScope Monitor Name	The name of the monitor for which SiteScope was unable to calculate a baseline.
Reason for Failure	<p>The reason that SiteScope was unable to calculate a baseline value for the monitor. They include:</p> <ul style="list-style-type: none"> ➤ Insufficient data. The monitor has not run for a sufficient period of time to collect data to produce a meaningful baseline threshold. This period depends on the Minimum number of days required for baselining and Minimum number of samples required for baselining settings in Baseline Settings of Infrastructure Settings Preferences. If a monitor fails for this reason, you can still select the monitor for baseline activation using the limited measurement samples that were collected. For details on configuring the Baseline Settings, see “Baseline Settings” on page 273. ➤ No samples for the requested schedule. No data samples were collected for the range schedule specified. You cannot select the monitor for baseline activation. ➤ Zero measurement coverage. The monitor has no measurements that can be used in the baseline calculation. You cannot select the monitor for baseline activation. ➤ Unknown. The reason for baseline calculation failure is unknown. You cannot select the monitor for baseline activation.

Baseline Monitor Measurement Graphs Dialog Box


The following is an example of a Baseline Monitor Measurement graph.



<p>Description</p>	<p>Displays a graph per measurement, for all the measurements of the monitor. The default date selected for displaying the graph is the day with the maximum error reduction.</p> <p>Each graph shows:</p> <ul style="list-style-type: none"> ▶ The current warning and error thresholds. ▶ The baseline warning and error thresholds. ▶ Historic data of all baseline-related monitor measurements over a 24-hour time period (from 00:00-23:59). <p>To access: In the monitor tree, right-click the SiteScope node, a group or a monitor container, and select Baselining > Review & Activate. In the Threshold Graphs column for a monitor with calculated baseline data, click the View Graphs link.</p>
<p>Important Information</p>	<ul style="list-style-type: none"> ▶ If the baseline threshold is the same as the current threshold, the baseline threshold line is not displayed on the graph. ▶ The data displayed in the monitor measurement graphs is an aggregate of the measurement data and as such, the time periods may not accurately reflect the time the data was actually collected.
<p>Included in Tasks</p>	<p>“Set Monitor Thresholds Using a Baseline” on page 493</p>
<p>Useful Links</p>	<p>“Setting Status Thresholds Using a Baseline” on page 478</p>

Graph Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Click to create a snapshot of the graph you are viewing and highlight important areas of the graph by drawing shapes, lines, and adding text to the snapshot. For details on the user interface, see “Annotation Tool” on page 1484.</p>
Historic date <date link>	<p>Click the date link to open the calendar, and select the date for which you want to create monitor measurement graphs. The calendar contains the following buttons:</p> <ul style="list-style-type: none"> ▶ Revert. Returns to the previously selected report date. ▶ Current. Selects today's date in the calendar. ▶ OK. Updates the date link for the selected date and closes the calendar. ▶ Cancel. Closes the calendar without making any changes.
Generate	<p>Click to create a report for the date displayed in the date link.</p>

Graph Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Legend>	Describes the color coding used in the graph.
Measurement Name	The name of the measurement appears above the graph.
<Data points>	Displays for each 2 hour period of time on the Time axis, the value for the selected monitor measurement. Tooltip: The measurement value.
<Measurement Type> <y-axis>	Displays the monitor measurement type.
Time <x-axis>	The time division units for the date specified when generating the report (from 0-24 hours).
Baseline Error Threshold	Shows the baseline threshold line that determines Error status. Measurements beyond this line exceed the error baseline status threshold for the monitor. This is displayed on the graph as a solid red line.
Baseline Warning Threshold	Shows the baseline threshold line that determines Warning status. Measurements beyond this line exceed the warning baseline status threshold for the monitor. This is displayed on the graph as a solid orange line.
Current Error Threshold	Shows the threshold line that determines Error status. Measurements beyond this line exceed the error status threshold for the monitor. This is displayed on the graph as a dashed black line.
Current Warning Threshold	Shows the threshold line that determines Warning status. Measurements beyond this line exceed the warning status threshold for the monitor. This is displayed on the graph as a dashed blue line.

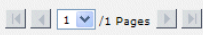
Status Report

The following is an example of the Status Report.

Status Report

Displays information about the baseline status for all monitors in the selected context.


Total of 8 monitors.
2 monitors are in calculation process.
6 are not baselined.

 / 1 Pages

SiteScope Monitor Name ▲	SiteScope Monitor Type	Baseline Status	Baseline Status Details
Monitor\124	CPU	Calculating baseline	Reading SiteScope2008_01_28.log file. Overall parsing progress 43 %.
Monitor\url	URL Content	Calculating baseline	Reading SiteScope2008_01_28.log file. Overall parsing progress 43 %.
Windows monitors for SiteScope Se	CPU	Monitor not selected for baselining	
Windows monitors for SiteScope Se	Windows Resourc	Monitor not selected for baselining	
Windows monitors for SiteScope Se	Windows Resourc	Monitor not selected for baselining	
Windows monitors for SiteScope Se	Memory	Monitor not selected for baselining	
Windows monitors for SiteScope Se	Windows Resourc	Monitor not selected for baselining	
Windows monitors for SiteScope Se	Windows Resourc	Monitor not selected for baselining	

Description	Displays information about the baseline status for all monitors in the selected context. To access: In the monitor tree, right-click the SiteScope node, a group, or a monitor and select Baselining > Status Report .
Important Information	This is an ad hoc report that is not saved to the SiteScope configuration data for later use.
Included in Tasks	“Set Monitor Thresholds Using a Baseline” on page 493
Useful Links	“Setting Status Thresholds Using a Baseline” on page 478

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Change the sort order in any column by clicking the up and down arrow in the column title.</p> <p>Default: The SiteScope Monitor Full Name column is in alphabetical order.</p>
<p>SiteScope Monitor Name</p>	<p>The name and path of the SiteScope monitor depending on the context.</p>
<p>SiteScope Monitor Type</p>	<p>The type of SiteScope monitor.</p>
<p>Baseline Status</p>	<p>The monitor's baseline status. The following statuses are available:</p> <ul style="list-style-type: none"> ▶ Monitor not selected for baselining. The monitor has not been selected for baselining. ▶ Calculating baseline. SiteScope is in the process of calculating the baseline. ▶ Calculation failed. SiteScope was unable to calculate a baseline. ▶ Calculated, not activated. A baseline was calculated for the monitor, but it has not yet been activated. ▶ Activating baseline. SiteScope is in the process of activating the baseline. ▶ Activation failed. SiteScope was unable to activate the baseline. ▶ Baseline activated. The baseline has been activated for the monitor.

GUI Element	Description
Baseline Status Details	Displays additional details for monitors with the following status: <ul style="list-style-type: none">▶ Calculating baseline. Displays the baseline calculation stage for the monitor.▶ Calculation failed. Displays the reason that the baseline calculation failed (Insufficient data, No measurements to baseline). Monitors that failed due to insufficient data are selected by default for automatic baseline calculation after the monitors have run for a period that is sufficient for SiteScope to accumulate data for the baseline period. For details, see “Failed Baseline Calculations Dialog Box” on page 539.
Refresh	Click during the calculation process to update the data in the status report.

15

Application Monitors

This chapter includes the main concepts and reference information for monitoring third-party applications. The monitors described enable SiteScope to access and retrieve data from the monitored applications.

This chapter includes:

Concepts

- ▶ Active Directory Replication Monitor Overview on page 551
- ▶ ASP Server Monitor Overview on page 552
- ▶ Apache Server Monitor Overview on page 553
- ▶ BroadVision Application Server Monitor Overview on page 554
- ▶ Check Point Firewall-1 Monitor Overview on page 554
- ▶ Cisco Works Monitor Overview on page 555
- ▶ Citrix Server Monitor Overview on page 555
- ▶ ColdFusion Server Monitor Overview on page 558
- ▶ COM+ Server Monitor Overview on page 559
- ▶ Dynamo Application Server Monitor Overview on page 561
- ▶ F5 Big-IP Monitor Overview on page 561
- ▶ IIS Server Monitor Overview on page 562
- ▶ iPlanet Server Monitor Overview on page 563
- ▶ Microsoft Exchange 2003 Mailbox Monitor Overview on page 566
- ▶ Microsoft Exchange 2003 Public Folder Monitor Overview on page 567

- ▶ Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Overview on page 568
- ▶ Microsoft Exchange 2007 Monitor Overview on page 569
- ▶ Microsoft Exchange 5.5 Message Traffic Monitor Overview on page 574
- ▶ News Monitor Overview on page 575
- ▶ Oracle 9i Application Server Monitor Overview on page 576
- ▶ Oracle 10g Application Server Monitor Overview on page 577
- ▶ Radius Monitor Overview on page 578
- ▶ SAP CCMS Monitor Overview on page 579
- ▶ SAP CCMS Alerts Monitor Overview on page 585
- ▶ SAP Java Web Application Server Monitor Overview on page 588
- ▶ SAP Performance Monitor Overview on page 590
- ▶ SAP Work Processes Monitor Overview on page 592
- ▶ Siebel Application Server Monitor Overview on page 597
- ▶ Siebel Log File Monitor Overview on page 601
- ▶ Siebel Web Server Monitor Overview on page 602
- ▶ SilverStream Server Monitor Overview on page 604
- ▶ SunONE Server Monitor Overview on page 605
- ▶ Tuxedo Monitor Overview on page 606
- ▶ UDDI Monitor Overview on page 607
- ▶ VMware Performance Monitor Overview on page 608
- ▶ WebLogic Application Server Monitor Overview on page 610
- ▶ WebSphere Application Server Monitor Overview on page 613
- ▶ WebSphere MQ Status Monitor Overview on page 617
- ▶ WebSphere Performance Servlet Monitor Overview on page 622

Reference

- ▶ Application Monitors User Interface on page 623

Active Directory Replication Monitor Overview

Use the Active Directory Replication Monitor to monitor the time that it takes a change made on one Domain Controller to replicate to up to as many as ten other Domain Controller. This allows you to verify that replication, a key part of the Active Directory System, is occurring within set thresholds. Create a separate Active Directory Replication Monitor for each Domain Controller that is being replicated throughout your system.

Note:

- ▶ The Active Directory Replication Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ This monitor can only be added by deploying an Active Directory Solution template. For information about using templates to deploy monitors, see “SiteScope Templates” on page 1189.

No additional setup is required other than to enable access to a Domain Admin account.

The Active Directory Replication Monitor works by making a small change to part of the Directory Service tree of the configured Domain Controller. It then checks each of the configured Replicating Domain Controllers for this small change. As the change is detected the difference between when the change was made and when it was replicated is computed.

For details on configuring this monitor, see “Active Directory Replication Monitor Settings” on page 625.

ASP Server Monitor Overview

Use the ASP Server Monitor to monitor the server performance parameters for Microsoft ASP servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each ASP Server you are running.

The Remote Registry service must be running on the machine where the ASP server is running if the ASP Server is running on Windows 2000.

The ASP Server Monitor makes use of Performance Counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you must define the connection to these servers under the Microsoft Windows Remote Preferences option in the SiteScope Preferences.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

For details on configuring this monitor, see “ASP Server Monitor Settings” on page 627.

Apache Server Monitor Overview

Use the Apache Server Monitor to monitor the content of server administration pages for Apache servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Apache server you are running.

Setup Requirements

Before you can use the Apache Server Monitor, you must do the following:

- ▶ Configure the Apache server you want to monitor so that status reports (server-status) are enabled for the server. The steps needed to do this may vary depending on the version of Apache you are using.
- ▶ Enable extended status (`ExtendedStatus On`) in the configuration file.
- ▶ Know the URL of the server statistics page for the server you want to monitor.
- ▶ The SiteScope Apache Server Monitor currently supports the server status page available at `http://<server_address>:<port>/server-status?auto`. The port is normally port 80, although this may vary depending on the server set up and your environment. For some Apache server configurations, you may need to use the server name rather than an IP address to access the server statistics page.

For details on configuring this monitor, see “Apache Server Monitor Settings” on page 629.

BroadVision Application Server Monitor Overview

Use the BroadVision Application Server Monitor to monitor the server performance data for BroadVision servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each BroadVision server in your environment.

You must know the Object Request Broker (ORB) port number for the BroadVision server you are trying to monitor.

In a BroadVision Production-style environment where there is one primary root server and other secondary servers (for example, Interaction Manager node) on different machines, you can only define a monitor against the primary root node. Metrics for the other nodes in the configuration are available for selection during root node monitor definition. In other words, monitoring is always accomplished through the primary root node, for all servers.

For details on configuring this monitor, see “BroadVision Application Server Monitor Settings” on page 631.

Check Point Firewall-1 Monitor Overview

Use the Check Point Firewall-1 Monitor to monitor the content of event logs and other data from Check Point Firewall-1 servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate Check Point Firewall-1 monitor instance for each Check Point Firewall-1 server in your environment.

For details on configuring this monitor, see “Check Point Firewall-1 Monitor Settings” on page 632.

Cisco Works Monitor Overview

Use the Cisco Works Monitor to monitor the content of event logs and other data from Cisco Works servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate Cisco Works monitor instance for each Cisco Works server in your environment.

For details on configuring this monitor, see “Cisco Works Monitor Settings” on page 634.

Citrix Server Monitor Overview

Use the Citrix Server Monitor to monitor the server performance statistics from Citrix Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate Citrix monitor instance for each Citrix Server in your environment.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

The Citrix Server Monitor makes use of performance objects and counters to measure application server performance. The Citrix Server Monitor keeps track of the following performance objects:

- Citrix IMA Networking
- Citrix Presentation Server (Citrix MetaFrame XP)
- ICA Session
- Terminal Services Session

You can find information about the Citrix performance objects and their counters in Appendix C of the Presentation Server 4.0 Administrator's Guide (<http://support.citrix.com/article/CTX106319>), and about the Terminal Services Session Object at <http://technet2.microsoft.com/windowsserver/en/library/9784cf82-9d06-4efa-b6fc-51c803fe78671033.mspx?mfr=true>.

Setup Requirements

The following are important requirements for using the SiteScope Citrix Server Monitor:

- ▶ SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you must define the connection to these servers under the Microsoft Windows Remotes option in the SiteScope Preferences.
- ▶ The Remote Registry service must be running on the machine where the Citrix Server is running if Citrix is running on a Windows 2000 platform.
- ▶ The Citrix Resource Manager must be available, installed, and running on the Citrix servers you want to monitor.
- ▶ One or more Citrix vusers must have established a connection with the Citrix server to enable viewing of ICA Session object.
- ▶ The Citrix Server Monitor requires the same permissions (trust level between monitoring and monitored machines) in Windows 2003 as Microsoft Windows Resources monitor. For details, see “Configuring the Microsoft Windows Resources Monitor to Run on Windows 2003 as a Non-Administrator User” on page 900.

Troubleshooting Tips

The following are troubleshooting tips for the Citrix Server Monitor:

- 1 Open a command line window (DOS prompt).
- 2 Type the following command, substituting the host name as required:

```
C:\>perfx \\hostname -u username -p password -h | find "ICA"
```

- 3 This should return the following response:

```
(3378) ICA Session  
(3386) ICA Session  
(3379) This object has several counters that can be used to monitor the  
performance in ICA sessions  
(3387) This object has several counters that can be used to monitor the  
performance in ICA sessions"  
ICA Session" 3386 performance in ICA sessions
```

If you do not get a similar response, either the counters are not available on the remote server or you will get a more descriptive error message indicating what might be the problem.

For details on configuring this monitor, see “Citrix Server Monitor Settings” on page 638.

ColdFusion Server Monitor Overview

Use the ColdFusion Monitor to monitor the server performance statistics from ColdFusion servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate ColdFusion monitor instance for each ColdFusion server in your environment.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

The ColdFusion Server Monitor makes use of performance counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you must define the connection to these servers under the Microsoft Windows Remote Preferences option in the SiteScope Preferences container. For details on how to define the Windows server connection, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.

The Remote Registry service must be running on the machine where the ColdFusion server is running if ColdFusion is running on Windows 2000.

For details on configuring this monitor, see “ColdFusion Server Monitor Settings” on page 640.

COM+ Server Monitor Overview

Use the COM+ Server Monitor to monitor the performance of software components registered and running on Microsoft COM+ servers. When you specify the host and port number of this probe instance, SiteScope retrieves all the functions running on the COM+ server for your monitoring selection. Error and warning thresholds for the monitor can be set on one or more function measurements.

Note: The COM+ Server Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

Setup Requirements

The following are several key requirements for using the COM+ Server Monitor:

- ▶ A COM+ probe component from HP must be installed and running on the target COM+ server you want to monitor.
- ▶ There must be HTTP connectivity between the SiteScope server and the server running the COM+ probe.
- ▶ To enable this monitor type in SiteScope, an Option license for the COM+ Monitor must be obtained and input into SiteScope.

Note: You cannot have multiple SiteScope instances share one probe instance. You can have multiple COM+ monitors within a single SiteScope installation access the same probe instance (uniquely identified by the probe host and port). The probe cannot serve data to multiple SiteScope installations.

COM+ Probe Installation

Go to the HP Software Support site (<http://www.hp.com/go/hpsoftwaresupport>) and in the **Where do I find** section, click **Software patches**. In the **Product** section, select **SiteScope** and type **COM+** in the optional search box. Download the COM+ probe from the results. You must log in with your HP user name and password to access the Software Patches page.

After downloading, follow the instructions for installing the probe on the COM+ server to be monitored.

Once the probe is successfully installed, you must start it prior to running or defining a SiteScope COM+ monitor, by invoking **mon_cplus_probe.exe** found in the COM+ probe's bin directory. By default, the installation creates this file at C:\Program Files\Mercury Interactive\COMPlusMonitor\bin\.

COM+ Functions

After you have specified the COM+ Probe for the target COM+ Server, you use the Browse Counters Utility in the monitor configuration page. The COM+ probe is queried for a list of available functions to monitor, and a browse tree is displayed. See the Browsable Counter Utility help page for instructions on how to navigate this hierarchy tree and select your functions or counters of interest.

For details on configuring this monitor, see “COM+ Server Monitor Settings” on page 642.

Dynamo Application Server Monitor Overview

Use the Dynamo Application Server Monitor to monitor the server performance data for ATG Dynamo servers using SNMP. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each ATG Dynamo server in your environment.

For details on configuring this monitor, see “Dynamo Application Server Monitor Settings” on page 644.

F5 Big-IP Monitor Overview

Use the F5 Big-IP Monitor to monitor the content of event logs and other data from F5 Big-IP load balancing device. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate F5 Big-IP monitor instance for each F5 Big-IP load balancing device in your environment.

For details on configuring this monitor, see “F5 Big-IP Monitor Settings” on page 648.

IIS Server Monitor Overview

Use the IIS Server Monitor to monitor the server performance statistics from IIS servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate IIS Server monitor instance for each IIS server in your environment.

Note:

- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of an IIS 6 server. For details, see “Microsoft IIS Solution Template” on page 1313.
- ▶ This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

The IIS Server Monitor makes use of performance counters to measure application server performance. SiteScope must be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you must define the connection to these servers under the Microsoft Windows Remote Preferences option in the SiteScope Preferences container.

The Remote Registry service must be running on the machine where the IIS server is running if IIS is running on Windows 2000.

The IIS Server Monitor supports monitoring HTTP/HTTPS services on IIS 4 and IIS 5, and HTTP/HTTPS, FTP, NNTP and MSMQ Queue on IIS 6.

For details on configuring this monitor, see “IIS Server Monitor Settings” on page 651.

iPlanet Server Monitor Overview

Use the iPlanet Server Monitor (formerly the Netscape Server Monitor) to monitor the content of server administration pages for iPlanet and Netscape servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each server you are running.

Note: Several file, name, and performance counter changes have been made to reflect the changes in the server product name and capabilities of the monitor.

Setup Requirements

The following are requirements for using the iPlanet Server Monitor:

To monitor current activity statistics for iPlanet 4.1 servers:

- 1** You must know the user name and password to access the iPlanet administrative server page. The URL for the main administrative page normally has the format
`http://serveraddress:adminport/https-admserv/bin/indextype`
- 2** Identify the virtual server instance name you want to monitor. This should be available in the box to the right of the **Manage** button. Type it in the place of **virtualserveraddressname** in the URL (see below).
- 3** Set up monitor using iPlanet 4.1 current activity counters using the URL of the following format
`http://serveraddress:adminport/https-virtualserveraddressname/bin/sitemon?doit:`

To monitor performance dump statistics for iPlanet 4.1 servers:

- 1** Modify the **obj.conf** file for each virtual server instance you want to monitor adding the line to enable perf dump. The **conf** entry normally has the format
`<Object path="path/Netscape/Server4/docs/.perf">Service fn=service-dump
</Object>`.
- 2** Restart the servers.
- 3** Access the performance dump page using the URL with the format
`http://serveraddress:http_port/.perf`.
- 4** Set up the iPlanet Server Monitor using iPlanet 4.1 performance dump counters (see below).

To monitor server statistics for iPlanet 6.0 servers using HTTP:

- 1** You must know the user name and password to access the iPlanet administrative server page. The URL for the main administrative page normally has the format
`http://serveraddress:adminport/https-admserv/bin/index`
- 2** Identify the specific server instance names as shown in the drop-down box next to the **Manage** button. The server instance names are used as the `virtualserveraddressname` the URL for monitoring that server instance.

The URL needed to monitor the server statistics normally has the format:

```
http://serveraddress:adminport/https-virtualserveraddressname/  
bin/instance-app/<pageStats>.jsp?pollInterval=15&vsname=All
```

where `<pageStats>` is replaced with a specific statistics page name as outlined below.

Note:

For the value for vsname (virtual server name), you can replace all with a specific virtualserveraddressname to monitor specific server instances. For example,

```
http://serveraddress:adminport/https-virtualserveraddressname/bin  
/instance-app/<pageStats>.jsp?pollInterval=15&vsname=  
virtualserveraddressname
```

- ▶ To monitor virtual server activity statistics, substitute <virtualServerStats> for <pageStats>.
 - ▶ To monitor server connection status statistics, substitute <connectionStats> for <pageStats>.
 - ▶ To monitor server DNS statistics for iPlanet 6.0 servers, substitute <dnsStats> for <pageStats>.
 - ▶ To monitor Keep-Alive statistics, substitute <keepAliveStats> for <pageStats>.
-

Scheduling This Monitor

Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Update value of several minutes to enable the server to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.

For details on configuring this monitor, see “iPlanet Server Monitor Settings” on page 653.

Microsoft Exchange 2003 Mailbox Monitor Overview

Use the Microsoft Exchange 2003 Mailbox Monitor to display important statistics about mailboxes handled by a Microsoft Exchange 2003 server, including mailboxes that are over a certain size, and mailboxes that have not been accessed in some number of days.

Note:

- ▶ The Microsoft Exchange 2003 Mailbox Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. For details on using the template, see “Microsoft Exchange Solution Templates” on page 1305.
- ▶ This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only.

Note: SiteScope must be configured to log on as a user account within the domain when running as a service, and not as "Local System account".

For details on configuring this monitor, see “Microsoft Exchange 2003 Mailbox Monitor Settings” on page 656.

Microsoft Exchange 2003 Public Folder Monitor Overview

Use the Microsoft Exchange 2003 Public Folder Monitor to display important statistics about public folders handled by a Microsoft Exchange 2000/2003 server, such as access times, empty folders, folder sizes, and folders not accessed within some time period.

Note:

- ▶ The Microsoft Exchange 2003 Public Folder Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. For details on using the template, see “Microsoft Exchange Solution Templates” on page 1305.
- ▶ This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only.

Note: SiteScope must be configured to log on as a user account within the domain when running as a service, and not as "Local System account".

For details on configuring this monitor, see “Microsoft Exchange 2003 Public Folder Monitor Settings” on page 659.

Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Overview

Use the Microsoft Exchange 2000/2003/2007 Message Traffic Monitor to display important statistics about messages handled by a Microsoft Exchange 2000/2003/2007 server, such as a count of messages sent that are larger than a certain size, or sent to a large number of recipients.

Note:

- ▶ The Microsoft Exchange 2000/2003/2007 Message Traffic Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
 - ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. For details on using the template, see “Microsoft Exchange Solution Templates” on page 1305.
 - ▶ This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).
-

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only.

Note: SiteScope must be configured to log on as a user account within the domain when running as a service, and not as "Local System account".

For details on configuring this monitor, see “Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Settings” on page 662.

Microsoft Exchange 2007 Monitor Overview

Use the Microsoft Exchange 2007 Monitor to display important statistics about the messaging system handled by a Microsoft Exchange Server 2007. The statistics are gathered through Exchange Management Shell, a command-line interface (built on Microsoft Windows PowerShell technology) that is used for managing and testing Microsoft Exchange Server 2007 servers and objects.

By default, the Microsoft Exchange 2007 Monitor can run command-lets (cmdlets) to provide health information about MAPI logons, Mail flow, and Search. You can also retrieve health information for Outlook Web Access and Web Services by configuring a test mailbox in the Exchange Server 2007. For details, see “Configuring Additional Microsoft Exchange Server Counters” on page 573.

Create a separate Microsoft Exchange 2007 monitor instance for each Microsoft Exchange server in your environment. The Microsoft Exchange 2007 Monitor is supported on Windows versions of SiteScope only.

System Requirements

- ▶ To configure Microsoft Exchange 2007 Monitor, Exchange Management Shell must be installed on SiteScope server. Windows PowerShell 1.0 must be installed on the computer that runs the Exchange Management Shell.
- ▶ To run each cmdlet mentioned above, the following requirements must be followed:
 - ▶ Server roles that correspond to the cmdlets you want to run must be installed on the Microsoft Exchange Server 2007. When monitoring Microsoft Exchange Server 2007, the available counters are determined according to the server roles installed. For example, if the Hub Transport and Mailbox roles are installed, the Test-MailFlow cmdlet runs. The following table shows the server roles required to run the cmdlets.

Server Role	Cmdlet
Mailbox	<ul style="list-style-type: none"> ▶ Test-MAPICConnectivity ▶ Test-ExchangeSearch
Hub Transport, Mailbox	Test-MailFlow
Client Access	<ul style="list-style-type: none"> ▶ Test-OWAConnectivity ▶ Test-WebServicesConnectivity

- ▶ You must log on to the SiteScope server using a domain account that has the permissions assigned to the Exchange Server Administrators group. The account must also be a member of the local Administrators group on that computer. For details, see “Preparing the System for Using the Microsoft Exchange 2007 Monitor” on page 571.

Preparing the System for Using the Microsoft Exchange 2007 Monitor

There are several important configuration requirements that must be performed or verified before the Microsoft Exchange 2007 Monitor can be used. This section describes the steps you use to configure your environment for this monitor. The following are several definitions that are used in the steps listed below.

- ▶ **Local Administrator.** An account that has administrative privileges on the local machine. An account can have this privilege either implicitly by having Domain Admin privileges or explicitly by adding as a member of the Administrators group on the local machine. Consult your system administrator, if necessary, for help with creating accounts.
- ▶ **MailBox Owner.** This is an "owner" account for which an Exchange mailbox has been set up. To use the Microsoft Exchange 2007 Monitor, this account must be a Local Administrator (see definition above) on the SiteScope server.
- ▶ **SiteScope User.** This is the account that is used to run the SiteScope service. This account must also be a Local Administrator (see definition above).

Before creating an Microsoft Exchange 2007 Monitor, perform the following setup steps:

1 Create mailbox accounts on each Exchange Server to be monitored with the Microsoft Exchange 2007 monitor.

Exchange mailbox accounts are used by Microsoft Exchange 2007 monitor to measure the performance counters on the Exchange server. Consult your Exchange system administrator if you need help setting up mailbox accounts for use with the SiteScope Microsoft Exchange 2007 monitor.

2 Add each Exchange Mailbox Owner to the Administrators users group on the SiteScope server.

The Mailbox Owner accounts setup in step 1, which are by definition domain logons, must be added as to the Administrators group on the SiteScope server.

- ▶ Click **Start > Settings > Control Panel > Users and Passwords > Advanced tab** or open the Computer Management utility and expand the **Local Users and Groups** folder in the left pane and click the **Groups** folder.

- ▶ Double-click the **Administrators** group icon to open the Administrators Properties window.
- ▶ Click the **Add** button to add each Mailbox Owner you expect to use with the Exchange 2007 Monitor.

Note: Make sure that the domain logon description is of the form domain\logon.

3 Verify that the SiteScope user logon is a member of Administrators group or a domain administrator account.

Important: The SiteScope user account must be a Local Administrator or a member of the domain admins group.

To change the logon account for the SiteScope user:

- ▶ Open the **Services** control utility on the SiteScope server.
- ▶ Right-click the **SiteScope** service entry and click **Properties**. The SiteScope Properties settings page opens.
- ▶ Click the **Log On** tab.
- ▶ Verify that the SiteScope user is run as a member of Administrators group or a domain logon account. To change the logon properties, click the **This account** radio button and type the SiteScope user logon.
- ▶ Restart the SiteScope server after making changes to the SiteScope service logon account.

Configuring Additional Microsoft Exchange Server Counters

You must configure a test mailbox in the Microsoft Exchange Server 2007 to retrieve health information for the Outlook Web Access and Web Services cmdlets.

To configure a test mailbox in the Microsoft Exchange Server 2007:

- 1** Run the script **New-TestCasConnectivityUser.ps1** in the Exchange Server to create a test mailbox. The script can be found under **<Exchange 2007 installation directory>\Scripts**.
- 2** After running the command, define an initial password for this account, and press ENTER to confirm the process. A new user is created with a name similar to **CAS_<16 digits>**.

You can run the **Get-Mailbox** cmdlet to verify that the test mailbox was created. This cmdlet retrieves a list of mailboxes, which you can use to check for the new test mailbox.

- 3** Repeat this process for each Exchange Mailbox Server that is to be tested.

Scheduling This Monitor

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only. It is not recommended to set monitor run frequency to less than 10 minutes.

For details on configuring this monitor, see “Microsoft Exchange 2007 Monitor Settings” on page 664.

Microsoft Exchange 5.5 Message Traffic Monitor Overview

Use the Microsoft Exchange 5.5 Message Traffic Monitor to display important statistics about messages handled by a Microsoft Exchange 5.5 server, such as a count of messages sent that are larger than a certain size, or sent to a large number of recipients.

Note:

- ▶ The Microsoft Exchange 5.5 Message Traffic Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. For details on using the template, see “Microsoft Exchange Solution Templates” on page 1305.

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only.

For details on configuring this monitor, see “Microsoft Exchange 5.5 Message Traffic Monitor” on page 666.

News Monitor Overview

Use the News Monitor to regularly monitor news groups on News servers. This enables you to manage the number of articles that are allowed to queue up, and delete them before they cause disk space problems.

Status

Each time the News Monitor runs, it returns a status message and writes it in the monitoring log file. It also writes the total time it takes to receive a response from the news server, and the number of articles available for each of the specified news groups.

The reading is the current value of the monitor. The possible values for the News Monitor are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- <news group> not found - the given news group was not found on the news server
- permission denied for connection - the connection could not be made, probably because the news server was configured to enable connections from a limited range of addresses
- login expected - the news server expected a user name and password, but none were provided. In this case, type a user name and password under the Advanced Settings section of the monitor.
- login failed, unauthorized - the user name and password were not accepted by the news server

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

For details on configuring this monitor, see “News Monitor Settings” on page 668.

Oracle 9i Application Server Monitor Overview

Use the Oracle 9i Application Server Monitor to monitor the server performance data for Oracle 9i servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Oracle 9i Application server in your environment.

Note: You must enable Web caching on the Oracle 9i Application Server to use the Oracle 9i Application Server Monitor.

For details on configuring this monitor, see “Oracle 9i Application Server Monitor Settings” on page 670.

Oracle 10g Application Server Monitor Overview

Use the Oracle 10g Application Server Monitor to monitor the server performance data for Oracle 10g servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Oracle 10g Application server in your environment.

Note: By default, the Oracle 10g metrics servlet is visible only to the local host. To enable monitoring the Oracle 10g application server, the servlet must be accessible from other IP addresses. You must edit the **dms.conf** file in the **<Oracle 10g installation path>infra/Apache/Apache/conf** directory. For details on editing the file and making this change, refer to the Oracle 10g application server documentation. Once configured properly, you should be able to see the following URL: **http://<Oracle 10g machine URL>:7201/dmsoc4j/Spy?format=xml**.

For details on configuring this monitor, see “Oracle 10g Application Server Monitor Settings” on page 672.

Radius Monitor Overview

Use the Radius Monitor to test that the RADIUS server correctly handles authentication requests. If the RADIUS server fails, any users that try to use it are unable to login and access any services. Create a separate monitor instance for each server you are running. You may want to setup multiple monitors per server if you want to test different kinds of login accounts.

Setup Requirements

- ▶ For SiteScope to monitor your RADIUS server, you must first add the IP address of your SiteScope server to the list of Clients that the RADIUS server is allowed to communicate with. This must be done in order for the Radius Server to take requests from SiteScope. Failure to do this results in Unknown Client errors on the RADIUS server.
- ▶ The Radius Monitor currently supports Password Authentication Procedure (PAP) authentication but not the Challenge Handshake Authentication Protocol (CHAP) or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). Your RADIUS server must be configured to accept PAP requests to use this monitor.

Status

Each time the Radius Monitor runs, it returns a status message and writes it in the monitoring log file. It also writes the total time it takes to receive a authentication response. The reading is the current value of the monitor. The possible values for the Radius Monitor are:

- ▶ OK
- ▶ unknown host name
- ▶ timed out reading
- ▶ match error

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

For details on configuring this monitor, see “Radius Monitor Settings” on page 674.

SAP CCMS Monitor Overview

Use the SAP CCMS Monitor to retrieve and report metrics using SAP's centralized monitoring architecture, CCMS (Computer Center Management System). With CCMS, a SAP administrator can monitor all servers, components and resources in the R/3 landscape from a single centralized server, greatly facilitating not only problem discovery but also problem diagnosis.

Note:

- ▶ The SAP CCMS Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a SAP CCMS environment. For details, see “SAP Solution Templates” on page 1347.
- ▶ This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

Using the SAP CCMS Monitor, you can also enable reporting of the host topology to Business Availability Center. If enabled, Business Availability Center automatically populates the CMDB with CIs based on the monitored hosts in SiteScope.

Using SAP's advanced CCMS interface BC-XAL 1.0, the SiteScope SAP CCMS Monitor exposes hundreds of performance and availability metrics. The error and warning thresholds for the monitor can be set for one or more of the nearly 120 SAP server performance statistics available by using the CCMS interface.

Note: Due to the large amount of metrics that are retrieved when displaying the entire SAP metrics browse tree during monitor definition, there could be a delay in opening the Choose Counters page. However, after a browse tree has been successfully retrieved, it is cached to file automatically, so that the next time you retrieve metrics from the same server/user name, the wait time is greatly reduced.

This monitor only retrieves and displays numeric metrics (Performance attributes). Status, Log and Information attributes are not supported. Also, presentation and management of SAP CCMS Alerts in SiteScope are not supported at this time.

Setup Requirements

- ▶ The SAP CCMS Monitor requires that the SAP Java Connector (SAP JCo 2.0.6 and above) component be downloaded from the SAP Service Marketplace Software Distribution Center, and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

To download SAP Java Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>), click **SAP Java Connector**, and then click **Tools and Services**. You need a valid Service Marketplace login to access the SAP Web site.

For details on installing the SAP Java Connector, see “SAP Java Connector Installation” on page 586.

- ▶ The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and above only.
- ▶ Consult your SAP documentation to determine if your R/3 landscape components may need additional software installed to run or work with CCMS.

User Authorization

A SAP user requires certain privileges to read CCMS metrics. When defining a SAP CCMS Monitor in SiteScope you must specify a user who has XMI authorization to be able to login to the CCMS server and retrieve metrics. The user should have one or more of the profiles listed below assigned to it. Authorizations are collected in SAP profiles, and the following profiles include XMI authorization:

- S_A.SYSTEM
- PD_CHICAGO
- S_WF_RWTEST
- SAP_ALL

One test to see if a user has such authorization is to try and issue transaction RZ20 in the SAP GUI and see if the CCMS monitor sets can be displayed.

SAP Java Connector Installation

The SAP CCMS monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

To enable the SAP CCMS monitor on a Windows environment:

- 1** Download the following .jar file and .dll files from the SAP support Web site (<http://www.service.sap.com/connectors>):
 - **sapjco.jar**
 - **librfc32.dll**
 - **sapjcorfc.dll**
- 2** Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.

- 3 Copy the two .dll files into the <SiteScope root directory>\bin directory.

Note: Check if the .dll files already exist in the <Windows installation directory>/system32 directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

- 4 Restart SiteScope.

To enable the SAP CCMS monitor on a UNIX environment:

- 1 Download the following .jar file and .so files from the SAP support Web site:

- sapjco.jar
- librfccm.so
- libsapjcorfc.so

- 2 Copy the sapjco.jar file into the <SiteScope root directory>\WEB-INF\lib directory.

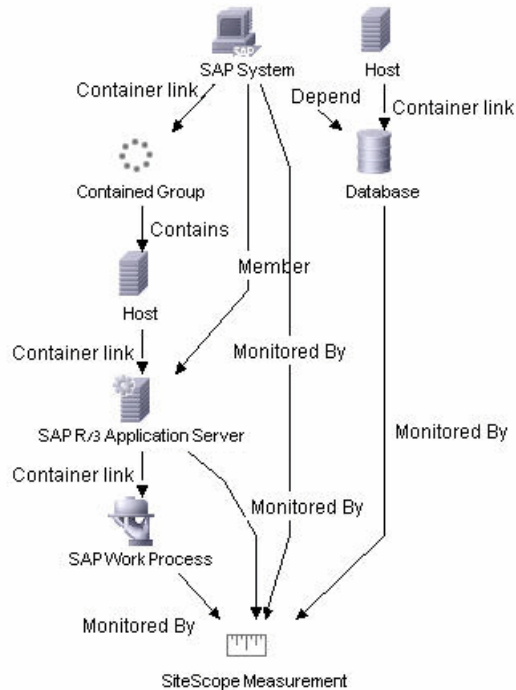
- 3 Copy the two .so files as follows:

- For Sun installations, copy into the <SiteScope root directory>\java\bin\sparc directory.
- For Linux installation, copy into the <SiteScope root directory>\java\bin\i386 directory.

- 4 Restart SiteScope.

SAP CCMS Topology Settings

The SAP CCMS monitor can identify the topology of the SAP System being monitored. If **Report SAP Topology to HP Business Availability Center** is selected in the Topology Settings (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the Universal CMDB as SiteScope Measurement Groups and SiteScope Measurement CIs.

Note:

- ▶ This direct integration between SiteScope and Business Availability Center is available only when the Business Availability Center for SAP Applications license is installed.
 - ▶ When you add a new application server to the SAP System, you must clear the **Report SAP Topology to HP Business Availability Center** option, save the Monitor definition, and then select the option again and save the monitor definition, in order for the monitor to recognize the new application server.
-

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 50.

For information about the SAP topology, see “SAP Systems View” in *Solutions and Integrations*.

For details on configuring this monitor, see “SAP CCMS Monitor Settings” on page 676.

SAP CCMS Alerts Monitor Overview

Use the SAP CCMS Alerts Monitor to retrieve and report alerts from the SAP CCMS monitors using SAP's centralized monitoring architecture, CCMS (Computer Center Management System). The SAP CCMS Alerts Monitor retrieves alerts using SAP's advanced CCMS interface BC-XAL 1.0.

The SAP CCMS Alerts Monitor allows you to monitor alerts for various components of your R/3 landscape.

Note: The SAP CCMS Alerts Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

Setup Requirements

- ▶ The SAP CCMS Alerts Monitor requires that the SAP Java Connector (SAP JCo 2.0.6 and above) component be downloaded from the SAP Service Marketplace Software Distribution Center, and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

To download SAP Java Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>), click **SAP Java Connector**, and then click **Tools and Services**. You need a valid Service Marketplace login to access the SAP Web site.

For details on installing the SAP Java Connector, see “SAP Java Connector Installation” on page 593.

- ▶ The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and above only.
- ▶ Consult your SAP documentation to determine if your R/3 landscape components may need additional software installed to run or work with CCMS.

User Authorization

A SAP user requires certain privileges to read CCMS metrics. When defining a SAP CCMS Alerts Monitor in SiteScope you must specify a user who has XMI authorization to be able to login to the CCMS server and retrieve metrics. The user should have one or more of the profiles listed below assigned to it. Authorizations are collected in SAP profiles, and the following profiles include XMI authorization:

- S_A.SYSTEM
- PD_CHICAGO
- S_WF_RWTEST
- SAP_ALL

One test to see if a user has such authorization is to try and issue transaction RZ20 in the SAP GUI and see if the CCMS monitor sets can be displayed.

SAP Java Connector Installation

The SAP CCMS Alerts monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

To enable the SAP CCMS Alerts monitor on a Windows environment:

- 1** Download the following .jar file and .dll files from the SAP support Web site:
 - **sapjco.jar**
 - **librfc32.dll**
 - **sapjcorfc.dll**
- 2** Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.
- 3** Copy the two .dll files into the **<SiteScope root directory>\bin** directory.

Note: Check if the .dll files already exist in your **<Windows installation directory>\system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

4 Restart SiteScope.

To enable the SAP CCMS Alerts monitor on a UNIX environment:

1 Download the following .jar file and .so files from the SAP support Web site:

- **sapjco.jar**
- **librfccm.so**
- **libsapjcorfc.so**

2 Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.

3 Copy the two .so files as follows:

- For Sun installations, copy into the **<SiteScope root directory>\java\bin\sparc** directory.
- For Linux installation, copy into the **<SiteScope root directory>\java\bin\i386** directory.

4 Restart SiteScope.

Scheduling This Monitor

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Update every** setting. Note, however, that CCMS metrics are generally only updated once every 5 minutes.

For details on configuring this monitor, see “SAP CCMS Alerts Monitor Settings” on page 679.

SAP Java Web Application Server Monitor Overview

Use the SiteScope SAP Java Web Application Server monitor to monitor the availability and server statistics for SAP Java Web Application server cluster. A Java cluster consists of one instance of Dispatcher per host, and one or more Servers. The monitor displays a counter tree for each dispatcher and server in the cluster.

Note:

- ▶ The SAP Java Web Application Alerts Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a SAP Java Web Application server. For details on using the template, see “SAP Solution Templates” on page 1347.

To enable the SAP Java Web Application Server monitor, you must install the SAP JMX Connector. For details, see below.

SAP JMX Connector Installation

The SAP Java Web Application Server monitor uses SAP JMX Connector libraries to connect to SAP J2EE cluster. A user must have the required license granted by SAP to receive and use these libraries.

To enable the SAP Java Web Application Server monitor:

- 1** Rename the **logging.jar** file from the SAP Java Web Application server to **sap_logging.jar** so as not to overwrite the SiteScope **logging.jar** file.
- 2** Copy the following .jar files from the SAP Java Web Application server installation:
 - **admin.jar**
 - **com_sap_pj_jmx.jar**
 - **exception.jar**
 - **sap_logging.jar** (renamed from **logging.jar** in SAP library)
 - **jmx.jar**into the **<SiteScope root directory>\WEB-INF\lib** directory.
- 3** Restart SiteScope.

For details on configuring this monitor, see “SAP Java Web Application Server Monitor Settings” on page 681.

SAP Performance Monitor Overview

Use the SAP Performance Monitor to monitor the server and database performance data for SAP application servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server and database loading for performance, availability, and capacity planning. Create a separate monitor instance for each SAP server in your environment.

Note:

- ▶ The SAP Performance Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a SAP server. For details, see “SAP Solution Templates” on page 1347.

To enable the SAP Performance monitor, you must install the SAP Java Connector. For details, see below.

SAP Java Connector Installation

The SAP Performance monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

To enable the SAP Performance monitor on a Windows environment:

- 1 Download the following .jar file and .dll files from the SAP support Web site:
 - ▶ `sapjco.jar`
 - ▶ `librfc32.dll`
 - ▶ `sapjcorfc.dll`

- 2 Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.
- 3 Copy the two .dll files into the **<SiteScope root directory>\bin** directory.

Note: Check if the .dll files already exist in your **<Windows installation directory>/system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

- 4 Restart SiteScope.

To enable the SAP Performance monitor on a UNIX environment:

- 1 Download the following .jar file and .so files from the SAP support Web site:
 - **sapjco.jar**
 - **librfccm.so**
 - **libsapjcorfc.so**
- 2 Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.
- 3 Copy the two .so files as follows:
 - For Sun installations, copy into the **<SiteScope root directory>\java\bin\sparc** directory.
 - For Linux installation, copy into the **<SiteScope root directory>\java\bin\i386** directory.
- 4 Restart SiteScope.

For details on configuring this monitor, see “SAP Performance Monitor Settings” on page 683.

SAP Work Processes Monitor Overview

Use the SAP Work Processes Monitor to monitor the effectiveness of your SAP R/3 server configurations. The monitor provides statistical information on work process performance. This information allows you to estimate whether the SAP R/3 Server is efficiently using its resources.

Note: The SAP Work Processes Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

Using the SAP Work Processes Monitor, you can also enable reporting of the host topology to Business Availability Center. If enabled, Business Availability Center automatically populates the CMDB with CIs based on the monitored hosts in SiteScope.

To enable the SAP Work Processes monitor, you must install the SAP Java Connector. For details, see below.

Understanding the SAP Work Processes Monitor

A SAP work process is a program that runs the R/3 application tasks. Each work process acts as a specialized system service. In terms of the operating system, a group of parallel work processes makes up the R/3 runtime system.

Every work process specializes in a particular task type: dialog, batch, update, enqueue, spool, message, or gateway. In client/server terms, a work process is a service, and the computing system running the particular service is known as a server. For example, if the system is providing only dialog services, this is a dialog server, although commonly referred to as an application server.

The dispatcher assigns tasks to the free work processes, making optimal use of system resources and balancing the system load. The dispatcher knows and distributes pending tasks according to the type of the defined processes. The difference among the various work processes affects only those tasks or special services that have been assigned to the work processes through the dispatching strategy.

SAP Java Connector Installation

The SAP Work Processes monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

To enable the SAP Work Processes monitor on a Windows environment:

- 1** Download the following .jar file and .dll files from the SAP support Web site:
 - **sapjco.jar**
 - **librfc32.dll**
 - **sapjcorfc.dll**
- 2** Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.
- 3** Copy the two .dll files into the **<SiteScope root directory>\bin** directory.

Note: Check if the .dll files already exist in the **<Windows installation directory>\system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

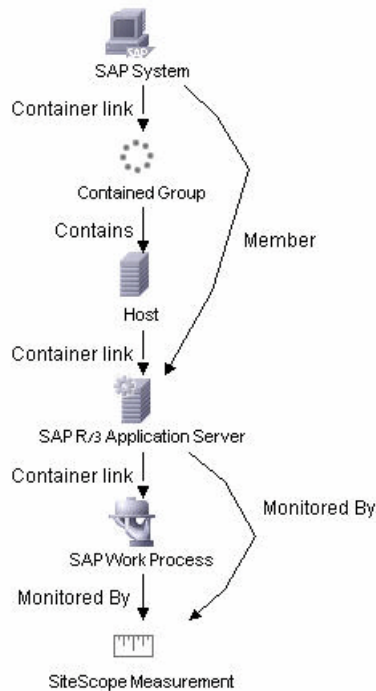
- 4** Restart SiteScope.

To enable the SAP Work Processes monitor on a UNIX environment:

- 1** Download the following .jar file and .so files from the SAP support Web site:
 - **sapjco.jar**
 - **librfccm.so**
 - **libsapjcorfc.so**
- 2** Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.
- 3** Copy the two .so files as follows:
 - For Sun installations, copy into the **<SiteScope root directory>\java\bin\sparc** directory.
 - For Linux installation, copy into the **<SiteScope root directory>\java\bin\i386** directory.
- 4** Restart SiteScope.

SAP Work Processes Topology Settings

The SAP Work Processes monitor can identify the work processes of the server being monitored. If **Report SAP Topology to HP Business Availability Center** is selected in the Topology Settings (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the Universal CMDB as SiteScope Measurement Groups and SiteScope Measurement CIs.

Note: This direct integration between SiteScope and Business Availability Center is available only when the Business Availability Center for SAP Applications license is installed.

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 50.

For information about the SAP topology, see “SAP Systems View” in *Solutions and Integrations*.

For details on configuring this monitor, see “SAP Work Processes Monitor Settings” on page 685.

Siebel Application Server Monitor Overview

The Siebel Application Server Monitor (previously know as the Siebel Server Manager Monitor) uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel application servers.

Note:

- ▶ The Siebel Application Server Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
 - ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a Siebel application server. For details, see “Siebel Solution Templates” on page 1353.
-

System Requirements

The following are requirements for using the Siebel Application Server Monitor:

- ▶ The Siebel Server Manager client must be installed only on a Windows machine where SiteScope is running or that is accessible to the SiteScope machine (even if the Siebel application server is installed on UNIX). There are several options for how you can do this:
 - ▶ Copy the necessary client libraries from the Siebel server and install them on the machine where SiteScope is running (recommended option).
 - ▶ Enable the client on the Siebel server itself and create a remote server profile in SiteScope to access that server and the Siebel client on that server.

- ▶ Install and enable the client on a third remote server and create a remote server profile in SiteScope to access that server and the Siebel client on that server.
- ▶ For Windows networks, map the network drive where the Siebel client is installed to the SiteScope machine and use this in the Script Path.
- ▶ You must know the install path for the Server Manager client to be able to setup Siebel Server Manager monitors in SiteScope. If the client is installed on the machine where SiteScope is running, this is the path on that machine. If the client is installed on a remote machine, you must know the fully qualified path to the client executable relative to that machine.
- ▶ You must know the name of the Siebel applications that are available in your network. For example, call center, sales, and so on.
- ▶ You must know the name or address of the Siebel Gateway server used by the Siebel applications you want to monitor. Ask your Siebel system administrator or consult the Siebel documentation for more information about the Gateway server name.
- ▶ You must know the name or address of the Siebel Enterprise server used by the Siebel applications you want to monitor. Ask your Siebel system administrator or consult the Siebel documentation for more information.
- ▶ You must know the user and password that Server Manager uses for logging into the Siebel server. This user must be granted Siebel Administrator responsibility on the Siebel server.
- ▶ For monitoring Siebel processes, SiteScope needs credentials/authorization to access the target Siebel machine. You may need to define a Remote host in SiteScope for the target Siebel machine, unless the SiteScope server is already implicitly authenticated by the Siebel machine.

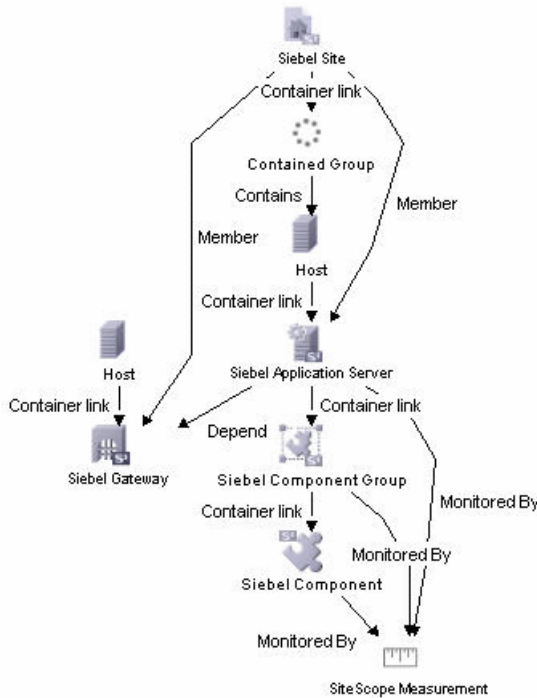
Note: Process monitoring remote Siebel machines incurs a noticeable delay (to get process metrics) hence the monitor runs slower than if the target Siebel machine is in close proximity to the SiteScope server. If your process counters are returning with no values during a run, it may be that the process metrics read operation is taking too long and SiteScope is timing out. In this case you may want to specify a required timeout value for **perfix** in the Infrastructure Settings Preferences page; for example, change the **Perfix timeout** value to 120 seconds. To access the Infrastructure Settings Preferences, expand **Preferences** in the left menu tree, choose **Infrastructure Settings Preferences**, and select the **General Settings** section.

- ▶ You must know the full path to the executable directory of the Siebel Server Manager Client relative to the machine it is installed on.
- ▶ You must make sure that the Siebel Server Manager Client's libraries are available to the Client. This varies according to the platform on which SiteScope is running:
 - ▶ **For SiteScope on Solaris/Linux.** If you are accessing the Siebel Server Manager Client on a remote server, you must have a remote UNIX server profile to connect to that server. Set the `LD_LIBRARY_PATH` on that machine by using the Initialize Shell Environment field for the remote server configuration created in SiteScope. An example shell initialization command is
`LD_LIBRARY_PATH=/var/siebel/client/lib;export LD_LIBRARY_PATH.`
 - ▶ **For SiteScope on Windows.** If the client libraries are installed locally, you must add a system variable called `LD_LIBRARY_PATH` that includes the path to the bin directory of the Siebel Client Manager.

If you are accessing the Siebel Server Manager Client on a remote server, you must have a remote NT server profile to connect to that server (NetBIOS connections only). Type the full path to the Siebel Server Manager executable directory relative to the server chosen in the **Script Path** box on the Choose Server page.

Siebel Application Server Topology Settings

The Siebel Application Server monitor can identify the topology of the Siebel Application Servers being monitored. If **Report Siebel Topology to HP Business Availability Center** is selected in the Topology Settings (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the Universal CMDB as SiteScope Measurement Groups and SiteScope Measurement CIs.

Note: This direct integration between SiteScope and Business Availability Center is available only when the Business Availability Center for Siebel Applications license is installed.

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 50.

For information about the Siebel topology, see “Siebel Views” in *Solutions and Integrations*.

For details on configuring this monitor, see “Siebel Application Server Monitor Settings” on page 687.

Siebel Log File Monitor Overview

Use the Siebel Log File Monitor to automatically scan multiple log files for detailed data and error information. By having SiteScope scan the log files at set intervals, you can eliminate the need to scan the logs manually. In addition, you can be notified of warning conditions that you may have otherwise been unaware of until something more serious happened.

Note: The Siebel Log File Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

Each time that SiteScope runs this monitor, it starts from the point in the file where it stopped reading last time it ran. This insures that you are only notified of new entries and speeds the rate at which the monitor runs. While this behavior can be overridden, is not recommended, and should be done for troubleshooting purposes only.

You can schedule your Siebel Log File Monitors to run as often as every 15 seconds. However, depending on the size of the log files, the total number of monitors you have running, and whether the **Search from Start** option is selected, the monitor may take a considerable amount of time to run.

For details on configuring this monitor, see “Siebel Log File Monitor Settings” on page 691.

Siebel Web Server Monitor Overview

Use the Siebel Web Server Monitor to monitor statistical and operational information about a Siebel server by way of the Siebel Web server plug-in. You can use this monitor to watch Siebel server login session statistics and gauge the performance of the Siebel server Object Managers and database.

Note:

- ▶ The Siebel Web Server Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a Siebel Web server. For details, see “Siebel Solution Templates” on page 1353.

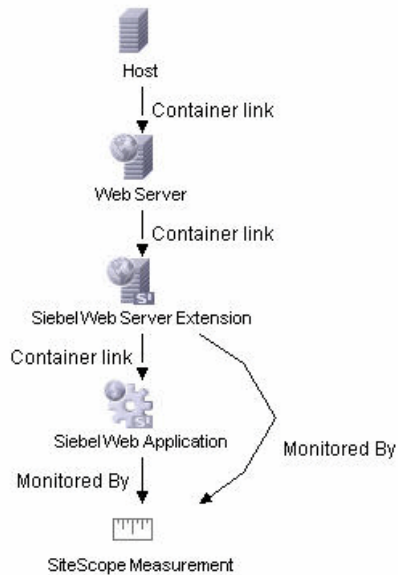
System Requirements

The following are several key requirements for using the Siebel Web Server Monitor:

- ▶ The Siebel Web server plug-in must be installed.
- ▶ The Siebel Web server plug-in should be configured to enable the display of the statistics you want to monitor. This may require that stats page sections be enabled by editing the **eapps.cfg** file for the Siebel server. Consult the Siebel documentation for more information.

Siebel Web Server Topology Settings

The Siebel Web Server monitor can identify the topology of the Siebel Web Server being monitored. If **Report Siebel Topology to HP Business Availability Center** is selected in the Topology Settings (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the Universal CMDB as SiteScope Measurement Groups and SiteScope Measurement CIs.

Note: This direct integration between SiteScope and Business Availability Center is available only when the Business Availability Center for Siebel Applications license is installed.

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 50.

For information about the Siebel topology, see “Siebel Views” in *Solutions and Integrations*.

For details on configuring this monitor, see “Siebel Web Server Monitor Settings” on page 695.

SilverStream Server Monitor Overview

Use the SilverStream Server Monitor to monitor the server performance metrics pages for SilverStream servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SilverStream server you are running.

You must know the server statistics URL for the SilverStream server you want to monitor. For some server configurations, you must use the server name rather than the IP address for the server.

Note: The monitor supports SilverStream versions 4.x. There is limited support for versions 5.0 and higher (includes only hits and bytes in the available counters).

For details on configuring this monitor, see “SilverStream Server Monitor Settings” on page 699.

SunONE Server Monitor Overview

Use the SunONE Server Monitor to monitor performance metrics reported in the stats-xml file of SunONE servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SunONE server you are running.

Setup Requirements

Before you can use the SunONE Server Monitor, the **stats-xml** service option must be enabled on each Web server you want to monitor. This normally requires that you manually edit the **obj.conf** configuration file for each server instance. For iPlanet 6.0 servers, the entry has the following syntax:

```
<Object name="stats-xml">  
ObjectType fn="force-type" type="text/xml"  
Service fn="stats-xml"  
</Object>
```

Each server instance must be restarted for the changes to become effective.

For details on configuring this monitor, see “SunONE Server Monitor Settings” on page 701.

Tuxedo Monitor Overview

Use the Tuxedo Monitor to monitor the server performance data for BEA Tuxedo servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Tuxedo server in your environment.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

System Requirements

The following are several key configuration requirements for using the Tuxedo Monitor:

- ▶ If SiteScope is running as a machine in the same domain as the Tuxedo server then SiteScope can connect to the Tuxedo server as a native client. If SiteScope is outside the domain of the Tuxedo server, you must install, configure, and enable the Tuxedo Workstation component to enable SiteScope to make requests of the Tuxedo server.
- ▶ The client and server side workstation component software versions should be the same. Some versions of the client software can work with multiple versions of Tuxedo servers but support information is limited.
- ▶ If Tuxedo 7.1 or later is installed on both the server you want to monitor and the SiteScope server, more than one Tuxedo server can be monitored at a time. If Tuxedo 6.5 or earlier is used, only one Tuxedo server can be monitored at a time.
- ▶ If SiteScope is outside the domain of the Tuxedo server, the Tuxedo Workstation client software needs to be installed on the server where SiteScope is running. This is usually in a DLL called libwsc.dll. The address to the application server needs to be specified in the WSNADDR environment variable.

- On the server where the Tuxedo application server is running, set the TUXDIR variable to be the TUXEDO installation directory and add the TUXEDO bin directory to the PATH variable.

The following environment variables must be added to the SiteScope environment:

- %TUXDIR% should be set on the monitoring machine to the <Tuxedo_root_folder>
- <Tuxedo_root_folder>\bin should be added to %PATH% variable

Note: Any environment variables (for example, TUXDIR) should be defined as system variables, not user variables.

For details on configuring this monitor, see “Tuxedo Monitor Settings” on page 703.

UDDI Monitor Overview

Use the UDDI Monitor to check the availability and round-trip response time of the UDDI server. Each time that the monitor is run, SiteScope checks if the UDDI Server can find a business entity.

Setup Requirements

The following are requirements for using the UDDI Monitor:

- The UDDI server must use UDDI Version 2.
- The administrator of the UDDI server can limit or disable this monitor.

For details on configuring this monitor, see “UDDI Monitor Settings” on page 705.

VMware Performance Monitor Overview

Use the VMware monitor to monitor VMware-based servers. VMware supplies much of the virtualization software available for x86-compatible computers. The VMware monitor supports monitoring:

- ▶ Single VMware ESX server installations.
- ▶ ESX server clusters managed by VMware Virtual Center.
- ▶ VMotion of virtual machines.

During initial monitor creation, the new monitor uses the connection URL configured to access the software and dynamically discover the object hierarchy and available performance counters. You can select from these performance counters to determine which measurements SiteScope should retrieve for reporting server status.

For details describing all the available counters, refer to the VMware documentation available at

<http://www.vmware.com/pdf/ProgrammingGuide201.pdf>

VMotion Support

VMotion is a technology from VMware which allows transparent transferring of virtual machines between physical hosts in a virtual infrastructure cluster. It allows you to move your virtual machines from one server to another without having to turn those virtual machines off. This process can be done both manually and automatically as part of cluster load-balancing.

The VMware monitor is browseable and the counters tree is designed so that virtual machine nodes are not children of physical host nodes. This means that the structure of the tree does not change during VMotion and if counters from a virtual machine are selected for this monitor, they will not change as a result of VMotion. This is regardless of where the virtual machine belonged at any particular moment.

SSL Connectivity

VMware servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The `https://` prefix means that it is a secure, encrypted connection. Monitoring a VMware server which uses an encrypted connection, requires importing the server certificate.

To import a server certificate:

- 1 Export the certificate by going to the VMware administration URL and performing the export procedure described in the document.
- 2 Import the certificate, from the `<SiteScope root directory>\java\lib\security`, by entering:

```
../../../../bin/keytool -import -file myCert.cer -alias myalias -keystore cacerts
```

Make sure to specify a unique alias for every certificate you add. If you do not, the keytool uses an automatic alias and once you attempt to add more than one custom certificate, the new certificate overwrites the old one and keeps only the default alias.

The word `changeit` is the default password for the `jssecacerts` file.

- 3 Make a copy of `<SiteScope root directory>\java\lib\security\cacerts` and rename it `<SiteScope root directory>\java\lib\security\jssecacerts`. After doing this, manually check to make sure the `jssecacerts` file is located in the `<SiteScope root directory>\java\lib\security` directory. The reason for creating the `jssecacerts` file is that the default `cacerts` file is overwritten every time SiteScope is upgraded or re-installed. Creating a copy with a different name allows new certificates to be imported and not be overwritten with future installations or upgrades.

Note: This step is not necessary if you already have a `jssecacerts` file.

For details on configuring this monitor, see “VMware Performance Monitor Settings” on page 706.

WebLogic Application Server Monitor Overview

Use the WebLogic Application Server Monitor to monitor performance statistics data from WebLogic 6.x, 7.x, and 8.x servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate WebLogic Application Server Monitor instance for each WebLogic server in your environment.

The BEA WebLogic Application Server monitor uses the Java JMX interface to access Runtime MBeans on the WebLogic server. An MBean is a container that holds the performance data. You must set certain permissions on the WebLogic server for SiteScope to be able to monitor MBeans.

Important: WebLogic Application Server Monitors cannot be used to monitor WebLogic 9.x or 10.x servers.

- ▶ To monitor these servers, use a JMX monitor as described in “JMX Monitor Settings” on page 801.
- ▶ For further details, see “Creating a JMX Monitor for a WebLogic 9.x or 10.x Server” on page 778.

If you are using a WebLogic 9.x or 10.x server, the rest of this chapter is not relevant.

Note: SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a WebLogic application server. For details, see “WebLogic Solution Template” on page 1369.

Configuration Requirements for WebLogic 6.x Servers

To set permissions for monitoring WebLogic 6.x servers, create a new ACL on the WebLogic server with the name **weblogic.admin.mbean**. Set the permission type to **access** and set the Users and Groups to be the user or group account that SiteScope uses to monitor the WebLogic server.

Configuration Requirements for WebLogic 7.x Servers

WebLogic 7.x and later servers use Security Policies instead of ACL's to control access to the server resources. To monitor WebLogic 7.x servers with SiteScope, the WebLogic administrator needs to add the user account that is running SiteScope to a WebLogic user group. The WebLogic group containing the SiteScope user must then be associated with a role statement that grants the necessary security role for accessing the desired WebLogic resources. The same security role must also be associated with the applicable policy statement that grants SiteScope access to the WebLogic resources. See the WebLogic server documentation for more information.

Configuring SiteScope to Use T3 Over SSL Against a WebLogic Server

You use the following steps to configure a WebLogic Monitor with the **Secure Server** option to monitor a WebLogic 7 or 8 server.

To configure SiteScope to use SSL for WebLogic server monitoring:

- 1** Obtain and install a JRE version 1.4.1 on the machine where SiteScope is running. Make a note of the full path to this JRE installation, as you must enter this information in the WebLogic Monitor setup.
- 2** Import the WebLogic Server's certificate, signed by a certificate authority, into the `<jre_path>\lib\security\cacerts` file for the JRE 1.4.1 installation on the SiteScope machine. If it is not, then you have to import the signer's certificate into the cacerts file using the keytool program. For instance, using the default WebLogic cert setup, you must import the **CertGenCA.der** certificate using the following command (this must all be entered on a single command line):

```
C:\j2sdk1.4.1\jre\bin>keytool.exe -import -alias weblogic81CA -keystore
..\lib\security\cacerts -trustcacerts -file
C:\BEA\weblogic81\server\lib\CertGenCA.der
```

- 3 Obtain a valid BEA license file and put it somewhere on the SiteScope machine. This is the file named **license.bea** in the BEA installation directory.
- 4 Obtain the **weblogic.jar** file from the WebLogic server or from a WebLogic server of the same version that you are monitoring. For WebLogic version 8.x, you must also obtain a copy of the **wlcipher.jar** file. Copy this or these files to the SiteScope server.

Note: Do not install the **weblogic.jar** file in the SiteScope directory tree. In other words, do not install it in the **<SiteScope root directory>\java\lib\ext** directory as this causes the Weblogic monitor to fail. You must install it in a separate directory on the server where SiteScope is running.

- 5 Open SiteScope and add a WebLogic Application Server Monitor.
- 6 Complete the boxes in the form as indicated and as described in the following steps.
- 7 Select the **Secure Server** option.
- 8 Type the full path to the **wlcipher.jar** and **weblogic.jar** files in the **WLCipher Jar File** and the **WebLogic Jar File** boxes, respectively.
- 9 A valid WebLogic license file must be copied to the SiteScope server. Type the full path to the BEA license file in the **WebLogic License File** box.
- 10 Type the full path to the **javaw.exe** (for Windows platforms) or the **java** (Solaris/Linux) executable for the JRE version 1.4.1 installation in the **Location of JVM** box.
- 11 With the other applicable boxes completed, you should be able to browse the counters on the WebLogic server over SSL when you click the **Get Counters** button.

For details on configuring this monitor, see “WebLogic Application Server Monitor Settings” on page 709.

WebSphere Application Server Monitor Overview

Use the WebSphere Application Server Monitor to monitor the server performance statistics from IBM WebSphere servers using the performance monitoring interfaces provided with WebSphere. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate WebSphere Application Server Monitor instance for each WebSphere Application Server in your environment.

Note: SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of a WebSphere Application server. For details, see “WebSphere Solution Template” on page 1377.

System Requirements

Before you can use the WebSphere Application Server Monitor, there are a number of configuration requirements involving the server environment. The following is an overview of the configuration steps:

For WebSphere 3.5.x and 4.x

Perform the following to prepare the WebSphere environment for SiteScope monitoring of WebSphere versions 3.5.x and 4.x:

- Install the IBM WebSphere Administrator's Console on the SiteScope server if you are monitoring WebSphere versions 3.5.x or 4.x.

If installing the Administrator's Console:

- Select **Custom Installation** option during installation.
- Select **Administrator's Console** and **IBM JDK 1.2.2.** in the **Choose Application Server Components** dialog box.
- Specify the machine you want to monitor during the installation.

- ▶ Enable the WebSphere servers to be monitored.
 - ▶ For WebSphere 3.5.x, enable EPM Counters on the WebSphere server.
 - ▶ For WebSphere 4.x, enable PMI Counters or enable the Performance Monitoring Service on the WebSphere server. You can enable the counters for the application you want to monitor by using the WebSphere Administrator's Console.
 - ▶ For WebSphere 4.x, select **Resources** and then select the **Performance** option. In the dialog box that opens, expand the **Performance Modules** tree. To manage different levels of performance data, select the performance modules, choose a performance level, and then click the **Set** button.
- ▶ Alternatively, on WebSphere 3.5.x, you can set the EPM Specification to:
`epm=high:epm.beanMethodData=none`
by using the WebSphere Administrator's Console.
- ▶ If security has been enabled on the WebSphere server, the server security ring must be copied to the admin client.

For WebSphere 5.x

To monitor WebSphere version 5.x, the necessary WebSphere libraries must be available on the SiteScope server. Generally, this means that a WebSphere 5.x client install must exist on the SiteScope server.

To install the correct client software on a SiteScope server:

- 1** Install the **Administration (or admin console) Performance Analysis** option from the custom options menu in the WebSphere 5.x install.

Important: Certain trial versions of IBM WebSphere do not include the Performance Analysis option required by the SiteScope WebSphere Application Server Monitor. The SiteScope monitor can only work when a complete WebSphere production installation is available.

- 2** Copy all of the files from the **lib** folder of a WebSphere 5.x Application Server installation to the **lib** folder on the client install from step 1.

- 3 The WebSphere 5.x server and client settings have to match. This means that the SiteScope WebSphere Application Server Monitor is not able to monitor a WebSphere 5.1 application server if the client libraries are from a WebSphere 5.0 and vice versa. Client libraries should be installed in separate folders with clearly distinct directory names (for example, Websphere50 and Websphere51) to avoid confusion and SiteScope setup errors.

Note: For WebSphere 5.x SiteScope uses the WebSphere JMX interface so the port number used to communicate with the application server is the SOAP port number. The default SOAP port number is 8880.

- 4 You must enable the WebSphere servers to be monitored. For WebSphere 4.x and 5.x, enable PMI Counters or enable the Performance Monitoring Service on the WebSphere server. You can enable the counters for the application you want to monitor by using the WebSphere Administrator's Console.

For WebSphere 5.x, Click on **Servers > Application Servers**. Select the server to be monitored from the Application Server list. From the Configuration tab, click on the Performance Monitoring Service in the Additional Properties list. Click the **Start Up** check box and select the **Initial specification** level as Standard or Custom. Then click the Apply button.

- 5 If security has been enabled on the WebSphere server, the server security ring must be copied to the admin client.

Note: If security has been enabled on the WebSphere 5.x server, you must copy the security keyring from the WebSphere server to SiteScope. A keyring is a certification used by the server to identify the client.

For WebSphere 6.x

To enable monitoring WebSphere version 6.x, you must have the following directories copied onto the SiteScope machine:

- AppServer/Java
- AppServer/lib

These directories can be copied into any directory on the SiteScope machine but must be stored exactly as they appear under the **AppServer** directory.

You can use one of the following options:

- Create a directory on the machine running SiteScope called **AppServer** and copy the two directories, **Java** and **lib**, directly into the newly created **AppServer** directory. This is the recommended option because it occupies the least amount of disk space on your SiteScope machine.
- Copy the entire WebSphere AppServer directory from the machine being monitored onto the machine running SiteScope.
- Copy all the WebSphere application server files onto the machine running SiteScope. This is the least recommended option because of the size of the application server files.

Once you have the **AppServer/Java** and **Appserver/lib** files on the SiteScope machine, use the following procedure to prepare the WebSphere environment for monitoring WebSphere 6.x.

To set up monitoring WebSphere 6.x:

- 1** On the WebSphere server, select **Servers > Application Servers > <server name> > Performance Monitoring Infrastructure (PMI)** and ensure that the counters are set to **Extended**.
- 2** From the SiteScope machine, make sure that you can access the SOAP from a browser. For example, open a browser and type the following sample address: `http://jberantlab:8880`. If an XML page is returned, the monitor is ready to be added to SiteScope and configured.

- 3 Open SiteScope, add the WebSphere Application Server Monitor, and configure the settings. For details, see “WebSphere Application Server Monitor Settings” on page 712.

Note: For WebSphere 6.x and later, SiteScope uses the WebSphere JMX interface so the port number used to communicate with the application server is the SOAP port number. The default SOAP port number is 8880.

WebSphere version 6.x supports global security. Global security is set up and maintained through the WebSphere administrative console. To enable this functionality in SiteScope, you must configure the WebSphere 6.x monitor in the Advanced Settings pane.

For details on configuring this monitor, see “WebSphere Application Server Monitor Settings” on page 712.

WebSphere MQ Status Monitor Overview

Use the WebSphere MQ Status Monitor to monitor the performance attributes of MQ Objects: channels and queues, on MQ Servers v5.2 and above (formerly known as MQSeries). You can monitor both performance attributes and events for channels and queues.

Note: The WebSphere MQ Status Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

You can set the error and warning thresholds for the WebSphere MQ Status Monitor on as many as fifteen function measurements.

System Requirements

This monitor requires two IBM MQ SupportPacs to be downloaded from the IBM Web site and installed on the same machine where the SiteScope server is running:

- ▶ **MA88.** MQSeries classes for Java, version 5.2.2 (5648-C60) or later. Go to the IBM Web site for this support package. Note that in some cases this component may already be bundled with the IBM MQ Server installation. Check your IBM MQ install documentation for details.
- ▶ **MS0B.** WebSphere MQ Java classes for PCF. Go to the IBM Web site for this support package.

Follow the instructions for installing both support packs. Copy the following files from these installations to the

<SiteScope root directory>\java\lib\ext directory:

- ▶ **com.ibm.mq.jar**
- ▶ **com.ibm.mq.pcf.jar**
- ▶ **connector.jar**

After installing the required libraries, stop and restart SiteScope.

Channel Status Codes

You can choose from two different reporting schemes for Channel Status Code values:

- ▶ **IBM MQ Native Coding Scheme.** Report the actual or original channel status codes as documented in the IBM MQ literature.
- ▶ **HP Coding Scheme.** Report channel status codes in ascending values that are directly proportional to the health of the channel. That is, SiteScope reports a channel status value from 0 (least healthy) to 6 (healthiest). This scheme is consistent with how other HP products report MQ channel status codes. However this scheme provides less gradients than the IBM scheme, as shown in the table below:

MQ Channel Status	MQ Coding Scheme	HP Coding Scheme
Stopped	6	0
Paused	8	0
Inactive	-1	0
Initializing	4	1
Stopping	13	1
Starting	2	2
Retrying	5	3
Requesting	7	4
Binding	1	5
Running	3	6
Stopped	6	0

You can select the required coding scheme in the **Channel Status Code Scheme** box under the Advanced Settings section.

Monitoring MQ Events

For events, two system queues are regularly polled for the presence of relevant events:

- SYSTEM.ADMIN.PERFM.EVENT - for queue performance events
- SYSTEM.ADMIN.CHANNEL.EVENT - for channel events

On each scheduled run of the MQ monitor (which contain event counters), one or both of these system queues are queried for the presence of events that match the chosen event type, the source queue or channel that generated the event, and its queue manager. Events found are only browsed and not removed from the queue, so such events can continue to be consumed by other applications, if necessary. On each run the MQ monitor reports the number of event occurrences found since the last run of the monitor.

The monitor strives not to report the same event occurrence more than once. This is accomplished by recording the timestamp of the most recent event browsed, so that in the next monitor run any events encountered that were generated prior to this recorded timestamp are ignored.

Enabling Queue Events on the MQ Server

By default, queue performance events are unavailable in the MQ server. For SiteScope to monitor these events, enable the MQ server to create these events. A MQSC command must be issued on each queue and for each event to be enabled. In addition, required threshold values must be set on each queue and for each event that specify the conditions for generating the event. Consult the IBM MQ MQSC Command Reference for more information.

Channel events are always enabled and require no further action for them to operate.

Specifying Alternate Queue Managers

It is possible to set up an MQSeries environment such that events from remote queue managers are routed to a central queue manager for monitoring. If the event configured for monitoring by the user is from a remote queue manager (a queue manager other than the one identified in **Queue Manager** of the MQ Monitor definition page), it must be specified in the **Alternate Queue Manager** text box.

Authentication

Your MQ server may require SiteScope to authenticate itself when connecting to retrieve metrics. A function has been built into this monitor to run a user-developed, client-side security exit written in Java.

To use this function, specify the fully-qualified class name of the security exit component in file **<SiteScope root directory>\groups\master.config**. For example,

```
_mqMonitorSecurityExit=com.mycompany.mq.MyExit
```

where the security exit class is called `com.mycompany.mq.MyExit`.

Make sure this class is in the classpath of the running SiteScope JVM by copying your security exit class into **<SiteScope root directory>\java\lib\ext**. You can only deploy one security exit class for a SiteScope instance, and every MQ monitor running on that instance runs that security exit.

In the case of a Windows-based SiteScope instance monitoring a Windows-based MQ server, the default authentication scheme requires that SiteScope be running under a user account that is recognized by the target server's Windows security group. Specifically, the SiteScope user must be added to the server's `mqm` group.

For information about MQ security exits and other authentication schemes, consult the IBM WebSphere MQ documentation.

For details on configuring this monitor, see “WebSphere MQ Status Monitor Settings” on page 716.

WebSphere Performance Servlet Monitor Overview

Use the WebSphere Performance Servlet Monitor to monitor the server performance statistics for IBM WebSphere servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate WebSphere Performance Servlet Monitor instance for each WebSphere Application Server in your environment.

System Requirements

The following are several key requirements for using the WebSphere Performance Servlet Monitor:

- ▶ The WebSphere Performance Servlet is an optional component for WebSphere 3.0x and 3.5x versions. The performance servlet must be installed on WebSphere servers to use this monitor. A patch needs to be applied according to which WebSphere 3.x version you are monitoring.
- ▶ The WebSphere Performance Servlet must be installed on each WebSphere 3.x server you want to monitor. The files should be copied to the **hosts\default_host\default_app\servlets** subdirectory on each WebSphere server machine. The files needed per version are as follows:

Version	Files
3.02	xml4j.jar performance.dtd perf.jar
3.5	perf35.jar
3.5.2, 3.5.3	perf35x.jar

- ▶ The WebSphere Performance Servlet should be included as part of WebSphere 4.0 although it needs to be deployed. If you are running WebSphere 4.0 servers, only one instance of the servlet needs to be deployed to monitor one or more WebSphere 4.0 servers.

- ▶ Verify that the servlet is running properly and that the performance data is generated. One way to do this is to try to display it through an XML enabled browser. The servlet URL should be in the following format:

`http://<server:port>/<dir_alias>/com.ibm.ivb.epm.servlet.PerformanceServlet`

For example,

`http://wbs.company.com:81/servlet/com.ibm.ivb.epm.servlet.PerformanceServlet`

For details on configuring this monitor, see “WebSphere Performance Monitor Settings” on page 718.

Application Monitors User Interface

This section describes:

- ▶ Active Directory Replication Monitor Settings on page 625
- ▶ ASP Server Monitor Settings on page 627
- ▶ Apache Server Monitor Settings on page 629
- ▶ BroadVision Application Server Monitor Settings on page 631
- ▶ Check Point Firewall-1 Monitor Settings on page 632
- ▶ Cisco Works Monitor Settings on page 634
- ▶ Citrix Server Monitor Settings on page 638
- ▶ ColdFusion Server Monitor Settings on page 640
- ▶ COM+ Server Monitor Settings on page 642
- ▶ Dynamo Application Server Monitor Settings on page 644
- ▶ Disk Space Monitor Settings on page 646
- ▶ F5 Big-IP Monitor Settings on page 648
- ▶ IIS Server Monitor Settings on page 651
- ▶ iPlanet Server Monitor Settings on page 653
- ▶ Microsoft Exchange 2003 Mailbox Monitor Settings on page 656

- ▶ Microsoft Exchange 2003 Public Folder Monitor Settings on page 659
- ▶ Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Settings on page 662
- ▶ Microsoft Exchange 2007 Monitor Settings on page 664
- ▶ Microsoft Exchange 5.5 Message Traffic Monitor on page 666
- ▶ News Monitor Settings on page 668
- ▶ Oracle 9i Application Server Monitor Settings on page 670
- ▶ Oracle 10g Application Server Monitor Settings on page 672
- ▶ Radius Monitor Settings on page 674
- ▶ SAP CCMS Monitor Settings on page 676
- ▶ SAP CCMS Alerts Monitor Settings on page 679
- ▶ SAP Java Web Application Server Monitor Settings on page 681
- ▶ SAP Performance Monitor Settings on page 683
- ▶ SAP Work Processes Monitor Settings on page 685
- ▶ Siebel Application Server Monitor Settings on page 687
- ▶ Siebel Log File Monitor Settings on page 691
- ▶ Siebel Web Server Monitor Settings on page 695
- ▶ SilverStream Server Monitor Settings on page 699
- ▶ SunONE Server Monitor Settings on page 701
- ▶ Tuxedo Monitor Settings on page 703
- ▶ UDDI Monitor Settings on page 705
- ▶ VMware Performance Monitor Settings on page 706
- ▶ WebLogic Application Server Monitor Settings on page 709
- ▶ WebSphere Application Server Monitor Settings on page 712
- ▶ WebSphere MQ Status Monitor Settings on page 716
- ▶ WebSphere Performance Monitor Settings on page 718

Active Directory Replication Monitor Settings

Description	<p>The Active Directory Replication Monitor allows you to monitor the time that it takes replication to occur between up to ten Domain Controllers. The error and warning thresholds for the monitor can be set on each of the monitored Domain Controllers.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ Monitors must be created in a group in the monitor tree.
Useful Links	<p>"Active Directory Replication Monitor Overview" on page 551.</p>

The Add/Edit Active Directory Replication Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Domain Controller	Select the Domain Controller that contains the replicated data.
Replicating Domain Controllers	Type a comma separated list of Domain Controllers that replicate data from the Domain Controller entered above.

GUI Element	Description
Username	Type either the user name or the entire Security Principal of a Domain Admin account. If a user name is given, the default security principal is created from the root context of the Domain Controller. For example, if you type in Administrator for a domain controller in the domain yourcompany.com, then the entire Security Principal would be CN=Administrator,CN=Users,DC=yourcompany,DC=com.
Password	Type the password for the Domain Admin account.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Maximum Replication Time	Type the maximum amount of time for replication to occur. The monitor goes into error if any of the Replicating Domain Controllers exceed this replication time.
Polling Interval	The amount of time this monitor should wait between queries of the Replicating Domain Controllers. A higher number reduces the number of LDAP queries against the servers.
Path to Directory	The path to a Directory in the Active Directory that you want to monitor. This is in the form of an LDAP query. Default value: Based on the default Directory for this server. For example, the default for a Domain Controller for sub.yourcompany.com is DC=sub,DC=yourcompany,DC=com.
Trace	This activates detailed tracing of the LDAP queries being run. This is used to debug problems.

ASP Server Monitor Settings

Description	<p>Monitor the availability of a Microsoft ASP server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more ASP server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"ASP Server Monitor Overview" on page 552

The Add/Edit ASP Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the ASP Server you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Apache Server Monitor Settings

Description	<p>Use to monitor the administrative and performance statistics for an Apache server.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Apache Server Monitor Overview" on page 553

The Add/Edit Apache Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.
URL	Choose the server URL you want to verify with this monitor. This should be the Apache server statistics URL which usually has the form of <code>http://<servername>:<port>/server-status?auto</code> .

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Authorization User Name	If the server you want to monitor requires a name and password for access, type the name in this box.
Authorization Password	If the server you want to monitor requires a name and password for access, type the password in this box.
HTTP Proxy	(Optional) A proxy server can be used to access the server. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, type the name here. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, type the password here. Note: your proxy server must support Proxy-Authenticate for these options to function.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.
Server OS	The operating system that the Apache server is running on. This is used to correctly read server statistics from Apache based on the operating system platform. Default value: UNIX

BroadVision Application Server Monitor Settings

Description	<p>Monitor the availability and performance statistics of a BroadVision server. The error and warning thresholds for the monitor can be set on one or more BroadVision server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"BroadVision Application Server Monitor Overview" on page 554

The Add/Edit BroadVision Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Type the BroadVision root server name of the BroadVision server you want to monitor. For example, 199.123.45.678.
Port	Type the ORB port number to the BroadVision server you want to monitor. Example: 1221

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Check Point Firewall-1 Monitor Settings

Description	<p>Monitor the statistics of a Check Point Firewall-1 server using SNMP. The error and warning thresholds for the monitor can be set on one or more firewall statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Check Point Firewall-1 Monitor Overview" on page 554

The Add/Edit Check Point Firewall-1 Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.
Index	Type the index of the SNMP object you want to check with this monitor. Non-table object IDs have an index of 0 (zero).
Community	Type the community name of the Check Point Firewall-1 you want to monitor. You may need to consult with your network administrators about what community names are active in your network environment. Default value: public
Host Name	Type the host name or IP address of the Check Point Firewall-1 server you want to monitor. If the Check Point Firewall is configured to respond to SNMP on a port number other than the default port, type the port number as part of the server address. Default value: 161

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Retry Delay	The number of seconds that the monitor should wait for a response from the server before retrying the request.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing out. Once this time period passes, the monitor logs an error and reports an error status.

Cisco Works Monitor Settings

Description	<p>Monitor the statistics of a Cisco Works Server using SNMP. The error and warning thresholds for the monitor can be set on one or more Cisco Works server statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Cisco Works Monitor Overview" on page 555

The Add/Edit Cisco Works Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Type the name of the server you want to monitor.
SNMP Version	Select the version of SNMP to use when connecting.
Community	Type the community name of the Cisco Works Server you want to monitor (valid only for version 1 or 2 connections). You may need to consult with your network administrators about what community names are active in your network environment. Default value: public
SNMP V3 Authentication Type	Select the type of authentication to use for version 3 connections.
SNMP V3 Username	Type the user name for version 3 connections.
SNMP V3 Authentication Password	Type the authentication password to use for version 3 connections.
SNMP V3 Privacy Password	Type the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.
SNMP V3 Context Engine ID	Type a hexadecimal string representing the Context Engine ID to use for this connection. Note: This is applicable for SNMP V3 only.
SNMP V3 Context Name	Type the Context Name to use for this connection. Note: This is applicable for SNMP V3 only.
Timeout	Type the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.

GUI Element	Description
Retries	Type the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.
Port	Type the port to use when requesting data from the SNMP agent. Default value: 161
Starting OID	Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered in this box. Default value: 1 Edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value of 1 did not enable retrieving any counters, then you may have to type a different value in this box.
MIB File	Select either the Cisco Works MIB file or All MIBs . Selecting the Cisco Works MIB file causes only those objects that are described within that MIB file to be displayed. Selecting All MIBs causes all objects discovered on the given Cisco Works server to be displayed when browsing counters. If no MIB information is available for an object, it is still displayed, but with no textual name or description.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Counter Calculation Mode	<p>Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are:</p> <ul style="list-style-type: none"> ➤ a simple delta of the current value from the previous value ➤ a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements <p>Note: This option only applies to the aforementioned object types. A Cisco Works Monitor that monitors Counter objects as well as DisplayString objects only performs this calculation on the Counter objects.</p>

Citrix Server Monitor Settings

<p>Description</p>	<p>Monitor the availability of the following Citrix servers:</p> <ul style="list-style-type: none"> ▶ MetaFrame 1.8 Service Pack 3 ▶ MetaFrame XP(s,a,e) Feature Release 1/Service Pack 1 ▶ MetaFrame XP(s,a,e) Feature Release 2/Service Pack 2 ▶ Presentation Server 3.5 ▶ Presentation Server 4.x <p>The error and warning thresholds for the monitor can be set on one or more Citrix Server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p>Useful Links</p>	<p>"Citrix Server Monitor Overview" on page 555</p>

The Add/Edit Citrix Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Choose the server where the Citrix Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters. For information about the Citrix performance counters, see Appendix C of the MetaFrame Presentation Server 4.0 Administrator's Guide (http://support.citrix.com/article/CTX106319).
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.



ColdFusion Server Monitor Settings

Description	<p>Monitor the availability of an Allaire ColdFusion server (versions 4.5x) on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more ColdFusion server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"ColdFusion Server Monitor Overview" on page 558

The Add/Edit ColdFusion Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the ColdFusion Server you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

COM+ Server Monitor Settings

Description	<p>The Com+ Server Monitor monitors the performance of software components registered and running on Microsoft COM+ servers. When you specify the host and port number of this probe instance, SiteScope retrieves all the functions running on the COM+ server, for your monitoring selection. Error and warning thresholds for the monitor can be set on one or more function measurements.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<p>This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</p> <p>Monitors must be created in a group in the monitor tree.</p>
Useful Links	"COM+ Server Monitor Overview" on page 559

The Add/Edit Com+ Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
COM+ Probe Host Name	Type the host name of the COM+ Probe.
COM+ Probe Port Number	Specify the port number of the COM+ Probe. The installation default for the probe is at port 8008.
Authorization User Name	(Optional) User name for authorization to the probe.

GUI Element	Description
Authorization Password	(Optional) Password for authorization to the probe.
HTTP Proxy	(Optional) A proxy server can be used to access the probe. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the probe, type the name here. Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the probe, type the password here.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	<p>The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p>Note: Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with a Timeout value of more than 60 seconds to enable the server to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.</p>

Dynamo Application Server Monitor Settings

Description	<p>Allows you to monitor the availability of an ATG Dynamo platform. The error and warning thresholds for the monitor can be set on one or more Dynamo Application Server Monitor performance statistics by using SNMP.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Dynamo Application Server Monitor Overview" on page 561

The Add/Edit Dynamo Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.
Index	Type the index of the SNMP object you want to check with this monitor. Non-table object IDs have an index of 0 (zero).

GUI Element	Description
Community	Type the community that the above SNMP object belongs to. You may need to consult with your network administrators about what community names are active in your network environment. Default value: public
Host Name	Type the IP address or host name of the Dynamo Server to be monitored along with the port that server is answering on. If the SNMP agent for the Dynamo server is answering on a port other than the default port, you must include the port number as part of the host name address. Default value: 8870

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Retry Delay	Type the time, in seconds, for SiteScope to wait before retrying a request.
Timeout	Type the total time, in seconds, that SiteScope should wait for a successful reply from the Dynamo server. If a reply is not received in the time indicated, the monitor returns a timeout error.

Disk Space Monitor Settings

Description	Track how much disk space is currently in use on your server. Use this page to add the monitor or edit the monitor's properties. To access: <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Disk Space Monitor Overview" on page 894

The Add/Edit Disk Space Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the disk space you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to select a server name.

GUI Element	Description
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	<p>Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.</p>
Disk	<p>Select the disk drive that you want to monitor from the list.</p> <p>Note: Disk performance counters are unavailable by default in standard Windows 2000 installations. In order for you to monitor disk drives using the SiteScope Disk Monitor on servers running Windows 2000, you must enable these disk counters. Use the <code>diskperf -y</code> command line on each Win2000 machine you want to monitor disk space and then reboot each server. You should then be able to select the disk drives for those servers in the SiteScope Disk Monitor form.</p>

F5 Big-IP Monitor Settings

Description	<p>Use to monitor the administrative and performance statistics for an Apache server.</p> <p>Allows you to monitor the statistics of a F5 Big-IP load balancing device using SNMP. The error and warning thresholds for the monitor can be set on one or more load balancer statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"F5 Big-IP Monitor Overview" on page 561

The Add/Edit F5 Big-IP Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Type the name of the server you want to monitor.
SNMP Version	Select the version of SNMP to use when connecting.
Community	Type the community string (valid only for version 1 or 2 connections).
SNMP V3 Authentication Type	Select the type of authentication to use for version 3 connections.
SNMP V3 Username	Type the user name for version 3 connections.

GUI Element	Description
SNMP V3 Authentication Password	Type the authentication password to use for version 3 connections.
SNMP V3 Privacy Password	Type the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.
SNMP V3 Context Engine ID	Type a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.
SNMP V3 Context Name	Type the Context Name to use for this connection. This is applicable for SNMP V3 only.
Timeout	Type the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.
Retries	Type the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.
Port	Type the port to use when requesting data from the SNMP agent. The default of 161 is the port on which an SNMP agent is typically listening.
Starting OID	Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered in this box. The default value is 1, which is commonly used and applicable to most applications. You should edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value of 1 did not enable retrieving any counters, then you may have to type a different value in this box.

GUI Element	Description
MIB File	Select either the F5 MIB file or All MIBs . Selecting the F5 MIB file displays only those objects that are described within that MIB file. Selecting All MIBs displays all objects discovered on the given F5 Big-IP when browsing counters. If no MIB information is available for an object, it is still displayed, but with no textual name or description.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Counter Calculation Mode	<p>Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are:</p> <ul style="list-style-type: none"> ▶ a simple delta of the current value from the previous value, OR ▶ a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements <p>Note: This option only applies to the aforementioned object types. An SNMP by MIB Monitor that monitors Counter objects as well as DisplayString objects only performs this calculation on the Counter objects.</p>

IIS Server Monitor Settings

Description	<p>Allows you to monitor the availability and server statistics of a Microsoft IIS server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more IIS server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"IIS Server Monitor Overview" on page 562

The IIS Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the F5 Big-IP Server you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

iPlanet Server Monitor Settings

Description	<p>Allows you to monitor the availability of SunONE/iPlanet and Netscape servers. The error and warning thresholds for the monitor can be set on one or more Netscape server performance statistics or HTTP response codes.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"iPlanet Server Monitor Overview" on page 563

The iPlanet Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Counters	<p>Choose the server performance parameters and counters you want to check with this monitor. The list to the right of this item displays the available parameters and counters and those currently selected for this monitor.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ Select only those counters that are applicable to the server version you want to monitor. ▶ Do not edit the order of the counters in the selected counter text box. The counters must be maintained in the order they appear in the choose counter selection page.

GUI Element	Description
URL	<p>Select the URL you want to verify with this monitor. This URL should be the URL to the applicable server monitor statistics Web page for the server version you want to monitor. For iPlanet 4.1 servers this usually has the format <code>http://servername:adminport/https-serveraddress/bin/sitemon?doit.</code></p> <p>For iPlanet 6.0 servers, the URL of the monitor statistics Web page has the format <code>http://servername:adminport/https-instanceserveraddress/bin/instance-app/pageStats.jsp?pollInterval=15&vsname=All</code> where <code><pageStats.jsp></code> is replaced with the file reference for the specific statistics page you want to monitor (see the list of counters).</p> <p>Note: The servername:port and serveraddress are not necessarily identical depending on if you access the administrator server pages locally or remotely. The SiteScope iPlanet Server Monitor generally needs to be configured using the full serveraddress and not the <code>https-admserv</code> syntax. Normally you can find the serveraddress in the Select a Server box on the main administration Web page.</p> <p>Note: (For Advanced Users Only) The iPlanet Server Monitor can be used to monitor other server products in the SunONE product line that make their performance statistics available by using a server monitor statistics Web page.</p> <p>To monitor other products, you must know the URL of the access log or administration Web page for that product version.</p> <p>You must modify the regular expression in the <code>_netscapeRegExp=</code> entry of the SiteScope master.config file and add any additional counter strings to the SiteScope/templates.applications/counters.iplanet file to extract the applicable values from the administration logs.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Authorization User Name	If the server you want to monitor requires a name and password for access, type the name in this box.
Authorization Password	If the server you want to monitor requires a name and password for access, type the password in this box.
HTTP Proxy	Optionally, a proxy server can be used to access the server. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, type the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, type the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Timeout	<p>The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p>Note: Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Timeout value of more than 60 seconds to enable the server to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.</p>

Microsoft Exchange 2003 Mailbox Monitor Settings

<p>Description</p>	<p>The Microsoft Exchange 2003 Mailbox Monitor monitors mailbox statistics of Microsoft Exchange Server 2003.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click the Microsoft Exchange 2003 solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
<p>Important Information</p>	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information about using templates to deploy monitors, see "SiteScope Templates" on page 1189. ▶ Monitors must be created in a group in the monitor tree.
<p>Useful Links</p>	<p>"Microsoft Exchange 2003 Mailbox Monitor Overview" on page 566</p>

The Add/Edit Microsoft Exchange 2003 Mailbox Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Choose the server running Microsoft Exchange Server 2003 that you want to monitor.
Username	Type the user name to use when querying the server for mailbox statistics. The statistics are gathered by using WMI (Windows Management Instrumentation), so the user name entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2. Default value: If this box is left blank, the user that SiteScope is running is used.
Password	Type the password for the user name entered above, or blank if user name is blank.
N largest mailboxes	Type the number (N) of mailboxes to display when reporting the N largest mailboxes.
Days since access	Type the number of days (N) to use when reporting the number of mailboxes that have not been accessed in N days.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Reporting directory	Type a location for SiteScope to save the results of each execution of this monitor. A default location is chosen if this box is left blank.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.

Microsoft Exchange 2003 Public Folder Monitor Settings

Description	<p>The Microsoft Exchange 2003 Public Folder Monitor monitors public folder statistics of Microsoft Exchange Server 2003.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click the Microsoft Exchange 2003 solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Important Information	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information about using templates to deploy monitors, see “SiteScope Templates” on page 1189. ▶ Monitors must be created in a group in the monitor tree.
Useful Links	<p>“Microsoft Exchange 2003 Public Folder Monitor Overview” on page 567</p>

The Add/Edit Microsoft Exchange 2003 Public Folder Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Choose the server running Microsoft Exchange Server 2003 that you want to monitor.
Username	Type the user name to use when querying the server for mailbox statistics. The statistics are gathered by using WMI (Windows Management Instrumentation), so the user name entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2. Default value: If this box is left blank, the user that SiteScope is running as is used.
Password	Type the password for the user name entered above, or blank if user name is blank.
Days since access	Type the number of days (N) to use when reporting the number of public folders that have not been accessed in N days.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Reporting directory	Type a location for SiteScope to save the results of each execution of this monitor. Default value: A default location is chosen if this box is left blank.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.

Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Settings

Description	<p>The Microsoft Exchange 2000/2003/2007 Message Traffic Monitor monitors message statistics of Microsoft Exchange Server 2000/2003/2007.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click the Microsoft Exchange 2000, Microsoft Exchange 2003, or Microsoft Exchange 2007 solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Important Information	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ This monitor can only be added by deploying an Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information about using templates to deploy monitors, see "SiteScope Templates" on page 1189. ▶ Monitors must be created in a group in the monitor tree.
Useful Links	<p>"Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Overview" on page 568</p>

The Add/Edit Microsoft Exchange 2000/2003/2007 Message Traffic Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Recipient limit	Type the number (N) of recipients to use when computing the number of messages sent to more than N recipients.
Log directory	The UNC path of the messaging tracking log file directory.
Query interval	Type the number of minutes to look back for messages when computing statistics. This affects how long it takes to run the monitor as a large interval could result in a large number of messages to be processed.
Number of outgoing users	Type the number (N) of users to use for reporting the top N outgoing users.
Message size limit	Type the number (N) of bytes to use when computing the number of messages sent larger than N bytes.
Number of domains	Type the number (N) of domains to use for reporting the top N sending domains.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Reporting directory	Type a location for SiteScope to save the results of each execution of this monitor. Default value: A default location is chosen if this box is left blank.

Microsoft Exchange 2007 Monitor Settings

Description	<p>The Microsoft Exchange 2007 Monitor monitors statistics of Microsoft Exchange Server 2007 on Windows platforms only.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<ul style="list-style-type: none"> ▶ Monitors must be created in a group in the monitor tree. ▶ You can create or update the Microsoft Exchange 2007 Monitor even if you input the incorrect Exchange Domain or Mailbox. This is because these properties are counter specific. As a result, some counter values may not be retrieved.
Useful Links	<p>"Microsoft Exchange 2007 Monitor Overview" on page 569</p>

The Add/Edit Microsoft Exchange 2007 Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element	Description
Exchange Server	Type the name of the server running Microsoft Exchange Server 2007 that you want to monitor.
Exchange Domain	Type the domain name and the mailbox of the server running Microsoft Exchange Server 2007 that you want to monitor.

GUI Element	Description
Mailbox	Type the name (alias) of the mailbox to be used for this monitor. This is often the e-mail account name but it may be a different name. It is recommended that you copy the mailbox name as it appears in the E-Mail Account properties for the e-mail account you are using with this monitor.
Exchange PS Console File Path	Type the full path to the Microsoft Exchange 2007 Server Management Shell console file. Example: C:\Program Files\Microsoft\Exchange Server\Bin\ExShell.psc
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters. Each performance counter contains information in the following categories: <ul style="list-style-type: none"> ▶ Unit\Type. The statistic's units. Some examples of possible types of units include percent, millisecond, or KB. ▶ Component. Components from which the performance counter is collected. ▶ Server Role. Indicates the required server role for running the cmdlet.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	Enables you to customize the time to wait, in seconds, for getting a response. You can set the timeout to no less than 1 second and no more than 10 minutes.

 **Microsoft Exchange 5.5 Message Traffic Monitor**

Description	<p>The Microsoft Exchange 5.5 Message Traffic Monitor monitors message statistics of Microsoft Exchange Server 5.5.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click the Microsoft Exchange 5.5 solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Important Information	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information about using templates to deploy monitors, see "SiteScope Templates" on page 1189. ▶ Monitors must be created in a group in the monitor tree.
Useful Links	<p>"Microsoft Exchange 5.5 Message Traffic Monitor Overview" on page 574</p>

The Add/Edit Exchange 5.5 Message Traffic Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Recipient limit	Type the number (N) of recipients to use when computing the number of messages sent to more than N recipients.
Log directory	Type a UNC path to the directory where message tracking logs are stored for the Exchange 5.5 server. Generally, this path is \\<server name>\tracking.log.
Query interval	Type the number of minutes to look back for messages when computing statistics. This affects how long it takes to run the monitor as a large interval could result in a large number of messages to be processed.
Number of outgoing users	Type the number (N) of users to use for reporting the top N outgoing users.
Message size limit	Type the number (N) of bytes to use when computing the number of messages sent larger than N bytes.
Number of domains	Type the number (N) of domains to use for reporting the top N sending domains.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Reporting directory	Type a location for SiteScope to save the results of each execution of this monitor. Default value: A default location is chosen if this box is left blank.

News Monitor Settings

Description	<p>The News Monitor verifies that a news server can be connected to, and is responding. It also measures how long it takes to make a connection, and how many articles are currently in the specified news groups.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"News Monitor Overview" on page 575

The News Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
News Server	<p>Type the IP address or the name of the news server that you want to monitor.</p> <p>Example: 206.168.191.21 or news.thiscompany.com.</p> <p>If the port is not the standard news port, add the port after the server with a colon.</p> <p>Example: news.thiscompany.com:7777</p>
News Groups	<p>Optionally type one or more news groups to be checked, separated by commas. Each of these news groups are checked for the current number of articles available in that news group. The reading of the monitor is the sum of articles available for each of the specified news groups.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	The number of seconds that the News monitor should wait for all of news transactions to complete before timing-out. Once this time period passes, the News monitor logs an error and reports an error status.
User Name	If your News server requires authorization, type a valid user name here.
Password	If your News server requires authorization, type a valid password here.
Connect From	The name or IP address of the server that connects to the News monitor.

Oracle 9i Application Server Monitor Settings

Description	<p>The Oracle 9i Application Server Monitor allows you to monitor the availability and performance statistics of a Oracle 9i Application Server. The error and warning thresholds for the monitor can be set on one or more Oracle 9i server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Oracle 9i Application Server Monitor Overview" on page 576

The Oracle 9i Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
URL	Type the server administration URL for the server you want to monitor. The URL is usually in the format: <code>http://server:port/webcacheadmin?SCREEN_ID=CGA.Site.Stats&ACTION=Show</code> .
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Authorization User Name	If the server you want to monitor requires a name and password for access, type the name in this box.
Authorization Password	If the server you want to monitor requires a name and password for access, type the password in this box.
HTTP Proxy	Optionally, a proxy server can be used to access the server. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, type the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, type the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.

Oracle 10g Application Server Monitor Settings

Description	<p>The Oracle 10g Application Server Monitor allows you to monitor the availability and performance statistics of an Oracle 10g Application Server. The error and warning thresholds for the monitor can be set on one or more Oracle 10g server performance statistics. Monitor allows you to monitor the availability and performance statistics of an Oracle 10g Application Server. The error and warning thresholds for the monitor can be set on one or more Oracle 10g server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Oracle 10g Application Server Monitor Overview" on page 577

The Oracle 10g Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Authorization User Name	If the server you want to monitor requires a name and password for accessing, type the name in this box.
Password	If the server you want to monitor requires a name and password for accessing, type the password in this box.

GUI Element	Description
Proxy Server	Optionally, a proxy server can be used to access the server. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, type the name here. Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, type the password here. Your proxy server must support Proxy-Authenticate for these options to function.
Host Name	Type the server administration URL for the server you want to monitor.
Metric Type	Type the type of metrics to monitor. Options are App Server (OC4J) and Web Server (DMS).
Port	Type the server port for the server you want to monitor. Default value: 7201 (configured in the dms.conf file)
Secure Server	Select this option to use a secure server.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.

Radius Monitor Settings

Description	<p>The Radius (Remote Authentication Dial In User Service) Monitor checks that a RADIUS server is working correctly by sending an authentication request and checking the result.</p> <p>A RADIUS server is used to authenticate users, often connecting through a remote connection such as a dialup modem or a DSL line.</p> <p>Use this page to add a monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Radius Monitor Overview" on page 578

The Add/Edit Radius Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
RADIUS Server	Type the IP address or the name of the RADIUS server that you want to monitor. Example: 206.168.191.21 or radius.thiscompany.com
Secret Phrase	Type the secret used to encrypt all requests to this RADIUS server.
User Name	Type the user name to authenticate.
Password	Type the password to authenticate.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Timeout	The number of seconds that the Radius monitor should wait for the connection to the port, and for any sending and receiving to complete. Once this time period passes, the Radius monitor logs an error and reports an error status.

GUI Element	Description
Port	Choose the TCP port used by the RADIUS server. Default value: 1645
Match Content	Type a string of text to check for in the response. If the text is not contained in the response, the monitor displays the message no match on content . You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching. Example: <code>/\d\d/</code> or <code>/size \d\d/i</code> Note: The search is case sensitive.

SAP CCMS Monitor Settings

Description	The SAP CCMS Monitor allows you to monitor the performance of your SAP R/3 System landscape in a centralized manner using SAP CCMS interface. Use this page to add the monitor or edit the monitor's properties. To access: <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ Monitors must be created in a group in the monitor tree.
Useful Links	"SAP CCMS Monitor Overview" on page 579

The Add/Edit SAP CCMS Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Application Server	Type the address of the SAP server you want to monitor.
SAP Client	Type the Client to use for connecting to SAP.
System Number	Type the System number for the SAP server.
Authorization User Name	Type the user name required to connect to the SAP server.
Authorization Password	Type the password required to connect to the SAP server.
Authorization Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.</p>
SAP Router String	<p>If your connection is being made through a router, type a router address string, otherwise leave it blank.</p> <p>You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select Properties to view the router address.</p>

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor. This tree more or less matches the hierarchy of Monitoring Tree Elements displayed in the Monitoring Tree that is shown in the SAP GUI with transaction RZ20. However, the SiteScope browse tree may show more or less information than RZ20 depending on the authorization level of the user name you specified for this monitor.

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Report SAP Topology to HP Business Availability Center	This monitor can identify the topology of the server being monitored. If this option is selected, the monitor creates a SAP topology in Business Availability Center's CMDB. For information about the topology, see "SAP CCMS Topology Settings" on page 583.

SAP CCMS Alerts Monitor Settings

Description	<p>The SAP CCMS Alerts Monitor allows you to read and complete alerts from the SAP CCMS Alerts monitors.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<p>This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</p> <p>Monitors must be created in a group in the monitor tree.</p>
Useful Links	"SAP CCMS Alerts Monitor Overview" on page 585

The Add/Edit SAP CCMS Alerts Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Application Server	Type the host name/IP address of the SAP server you want to monitor.
SAP Client	Type the Client to use for connecting to SAP.
System Number	Type the System number for the SAP server.
Authorization User Name	Type the user name required to connect to the SAP server. This user must have authorization to access CCMS metrics.
Authorization Password	Type the Password required to connect to the SAP server.

GUI Element	Description
Authorization Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.</p>
SAP Router String	<p>If your connection is being made through a router, type a router address string, otherwise leave it blank.</p> <p>You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select Properties to view the router address.</p>
Counters	<p>The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p>
Get Counters	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p>

SAP Java Web Application Server Monitor Settings

Description	<p>The SAP Java Web Application Server Monitor allows you to monitor the availability and server statistics for SAP Java Web Application server cluster.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<p>This monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running.</p> <p>Monitors must be created in a group in the monitor tree.</p>
Useful Links	<p>"SAP Java Web Application Server Monitor Overview" on page 588</p>

The Add/Edit SAP Java Web Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Application Server	Type the address of the SAP Java Web Application Server you want to monitor.
Port	Type the port number of the SAP Java Web Application Server you want to monitor. Default value: 50004
Authorization User Name	Type the user name required to connect to the SAP server.

GUI Element	Description
Authorization Password	Type the Password required to connect to the SAP server.
Authorization Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.</p>
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor. These counters are received dynamically from the JMX.

SAP Performance Monitor Settings

Description	<p>The SAP Performance Monitor allows you to monitor the availability and performance statistics of a SAP Application Server. The error and warning thresholds for the monitor can be set on SAP server and database performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<p>This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</p> <p>Monitors must be created in a group in the monitor tree.</p>
Useful Links	"SAP Performance Monitor Overview" on page 590

The Add/Edit SAP Performance Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Application Server	Type the address of the SAP server you want to monitor.
SAP Client	Type the Client to use for connecting to SAP.
System Number	Type the System number for the SAP server.

GUI Element	Description
SAP Router String	<p>If your connection is being made through a router, type a router address string, otherwise, leave it blank.</p> <p>You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select Properties to view the router address.</p>
Authorization User Name	Type the user name required to connect to the SAP server.
Authorization Password	Type the password required to connect to the SAP server.
Authorization Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.</p>
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

SAP Work Processes Monitor Settings

Description	<p>The SAP Work Processes Monitor allows you to monitor the effectiveness of your SAP R/3 server configurations. The monitor provides statistical information on work process performance to estimate whether the SAP R/3 Server is efficiently using its resources.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ Monitors must be created in a group in the monitor tree.
Useful Links	"SAP Work Processes Monitor Overview" on page 592

The Add/Edit SAP Work Processes Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Application Server	Type the address of the SAP server you want to monitor.
SAP Client	Type the Client to use for connecting to SAP.
System Number	Type the System number for the SAP server.
Authorization User Name	Type the user name required to connect to the SAP server.

GUI Element	Description
Authorization Password	Type the password required to connect to the SAP server.
Authorization Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.</p>
SAP Router String	<p>If your connection is being made through a router, type a router address string, otherwise, leave it blank.</p> <p>You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select Properties to view the router address.</p>
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Report SAP Topology to HP Business Availability Center	This monitor can identify the topology of the server being monitored. If this option is selected, the monitor creates a SAP topology in Business Availability Center's CMDB. For information about the topology, see "SAP Work Processes Topology Settings" on page 595.

Siebel Application Server Monitor Settings

Description	<p>The Siebel Application Server Monitor (previously know as the Siebel Server Manager Monitor) uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel application servers.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ Monitors must be created in a group in the monitor tree.
Useful Links	"Siebel Application Server Monitor Overview" on page 597

The Add/Edit Siebel Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Script Server	Select or type the remote Windows or UNIX machine where the Server Manager (svrvmgr) script is installed. The method of connection is either SSH or Telnet (but not Microsoft NetBios). For NetBios, choose this server and map the drive.
Siebel Host Name	This box is required if you are doing either of the following: <ul style="list-style-type: none"> ▶ Doing process monitoring. In this case you must define a Remote Definition to the target Siebel machine whose Siebel processes are to be monitored. Specify in this box the Host Server Name of the Siebel Remote definition (not the Title). This is the NT Server Address box for NT Remotes or Server Address box for UNIX Remotes. ▶ Reporting monitor data to an installation of HP Business Availability Center. In this case the value entered is used as a text identifier describing the target Siebel server that this monitor is monitoring. This text descriptor is used to identify the Siebel server when the monitor data is viewed in an HP Business Availability Center report. The box is optional only if the Script Server box is already specified to be the target Siebel server.
Application Server	Type the Siebel server name or address.
Gateway Server	Type the Gateway server name or address.
Enterprise Server	Type the Enterprise server name or address.
User	Type the user name for the Siebel Server Manager client.

GUI Element	Description
Password	Type the password for the Siebel Server Manager client.
Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.</p>
Script Path	<p>The full path to the Siebel Server Manager executable directory relative to the machine chosen above.</p> <p>Example: E:\sea704\client\BIN</p>
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Siebel Tasks Time Window	<p>Specify a time window in which tasks are monitored on the Siebel application server. If the task start time is within the time window (for example, 20 minutes), the task is monitored. The time window is calculated according to the formula: time window = (current time – property value).</p> <p>Type 0 to monitor every task on the Siebel application server, regardless of its start time.</p> <p>Default value: 60 minutes</p>

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Report Siebel Topology to HP Business Availability Center	<p>This monitor can identify the topology of the server being monitored. If this option is selected, the monitor creates a Siebel topology in Business Availability Center's CMDB. For information about the topology, see "Siebel Application Server Topology Settings" on page 600.</p>

Siebel Log File Monitor Settings

Description	<p>The Siebel Log File Monitor watches for log file entries added to a group of log files by looking for entries containing a specific event type or subtype.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<p>This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</p> <p>Monitors must be created in a group in the monitor tree.</p>
Useful Links	<p>"Siebel Log File Monitor Overview" on page 601</p>

The Add/Edit Siebel Log File Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The Siebel server where the log files you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.

GUI Element	Description
Log File Directory	<p>Type the path to the log directory you want to monitor.</p> <p>To monitor log files on a remote Windows NT/2000 server through NetBIOS, specify a UNC path to the remote directory.</p> <p>Example: \\remoteserver\logFileDirectory</p> <p>If you are using SSH as a connection method to the remote NT server, you must select the java library and ssh1 options for that remote.</p>
File Name	<p>Select the log files that you want to monitor. A regular expression must be used to specify multiple files. The search is not recursive and only matches files listed within the log file directory.</p> <p>Note: Selecting too many log files to monitor can significantly degrade SiteScope performance.</p>
Severity	<p>Select the severity level of entries to consider for matching. Entries that have the correct event type/subtype and have an equal or greater severity are matched. Those entries with lesser severity are ignored.</p>
Event Type	<p>Select the matching event type or subtype. The monitor reports how many log entries were found of the specified type.</p>

GUI Element	Description
Log-Entry Content Match	<p>(Optional) You may specify an additional text string or regular expression to further narrow down the matched log entries. This match expression is run against the content returned from the initial Severity and Event Type match.</p> <p>You use this option to find only those log entries with the selected severity an event type that meet this additional match criteria.</p>
Search from Start	<p>Select file checking option for this monitor instance. This setting controls what SiteScope looks for and how much of the target file is checked each time that the monitor is run. The following table describes the options for this setting:</p> <ul style="list-style-type: none"> ▶ Off. Check only newly-added records, starting at the time that the monitor was created (not when the file was created). ▶ On. Always check the contents of the whole file. <p>Note: Monitoring large numbers of log files with this option enabled may use large amounts of memory and CPU time. This can degrade SiteScope server performance.</p> <p>Default value: Off</p>

Siebel Web Server Monitor Settings

Description	<p>The Siebel Web Server Monitor allows you to use SiteScope to monitor statistical and operational information about a Siebel server by way of the Siebel Web server plug-in. You can use this monitor to watch Siebel server login session statistics and gauge the performance of the Siebel server Object Managers and database.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ Monitors must be created in a group in the monitor tree.
Useful Links	<p>“Siebel Web Server Monitor Overview” on page 602</p>

The Add/Edit Siebel Web Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Application URL	Type the URL of the Web plug-in server stats page for the application you want to monitor. Example: http://siebelsrv/service/_stats.swe If the Siebel Web server is configured to support verbose mode, you can also use http://siebelsrv/service/_stats.swe?verbose=high to include information on Locks and Current Operations Processing for the Siebel server.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Authorization User Name	Type the user name to access the Web server stats page.
Authorization Password	Type the password for accessing the Web server stats page.
HTTP Proxy	If you are using a proxy to access the Siebel server, type the proxy server and port to use. Example: proxy.SiteScope.com:8080

GUI Element	Description
Proxy Server User Name	Type the proxy user name if the proxy server requires authorization.
Proxy Server Password	<p>Type the proxy password if the proxy server requires authorization.</p> <p>If access to the Siebel Web Server site is controlled by a centralized authorization and authentication access control system, the following fields are used to submit information to a HTML/CGI enabled authentication system.</p> <p>You can determine if authentication is required by trying to access the Web plug-in server stats page using a Web browser outside of SiteScope. If an HTML-based authentication form opens before you see the Siebel service statistics page, you must use the following fields to access the Siebel Web server plug-in.</p>
HTML Form-based Authentication Required	Check this option to have SiteScope submit HTML form-based authentication when accessing the Siebel Web server plug-in.
Authorization Form Name	<p>When using HTML Form-based Authentication, this is the identifier of the authentication form within the Web page. The identifier is a number representing the place or order of the forms on an HTML page.</p> <p>Example: [1] is the first HTML <FORM> set, [2] is the second, and so on. The default is [1] because it assumes that the authentication information is entered into the first HTML <FORM> tag set on the page.</p>
Authorization Username Form Field	When using HTML Form-based Authentication, type the user name that should be submitted to the access control system. This must be the user name that would be entered in the authentication form the same as if you were accessing the Siebel Web server plug-in manually using a Web browser.

GUI Element	Description
Authorization Password Form Field	Type the password that should be submitted to the access control system. This must be the password that would be entered in the authentication form when accessing the Siebel Web server plug-in manually using a Web browser.
Authorization Form Button	<p>When using HTML Form-based Authentication, this is the identifier of the Submit button on the authentication form.</p> <p>The identifier is a number representing the place or order of the buttons on an HTML page.</p> <p>Example: [1] is the first HTML <INPUT TYPE=SUBMIT> button, [2] is the second, and so on.</p> <p>Default value: [1]</p>

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Report Siebel Topology to HP Business Availability Center	This monitor can identify the topology of the server being monitored. If this option is selected, the monitor creates a Siebel topology in Business Availability Center's CMDB. For information about the topology, see "Siebel Web Server Topology Settings" on page 603.

SilverStream Server Monitor Settings

Description	<p>The SilverStream Server Monitor allows you to monitor the availability of an SilverStream server. The error and warning thresholds for the monitor can be set on one or more SilverStream server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<p>The monitor supports SilverStream versions 4.x. There is limited support for versions 5.0 and higher (includes only hits and bytes in the available counters).</p> <p>Monitors must be created in a group in the monitor tree.</p>
Useful Links	<p>“SilverStream Server Monitor Overview” on page 604</p>

The Add/Edit SilverStream Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Counters	<p>Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.</p>
URL	<p>Choose the URL you want to verify with this monitor. This URL should be the URL to the applicable server administration Web page.</p> <p>Example: <code>http://<servername>:<port>/SilverStream/Statistics</code></p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Authorization User Name	If the server you want to monitor requires a name and password for access, type the name in this box.
Authorization Password	If the server you want to monitor requires a name and password for access, type the password in this box.
HTTP Proxy	(Optional) A proxy server can be used to access the server. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, type the name here. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, type the password here. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.

 **SunONE Server Monitor Settings**

Description	<p>The SunONE Server Monitor allows you to monitor the availability of SunONE or iPlanet 6.x servers using the stats-xml performance metrics file (iwsstats.xml or nesstats.xml) facility.</p> <p>By providing the URL of this stats-xml file, SiteScope can parse and display all metrics reported in this file and enable you to choose those metrics you need to be monitored as counters. In addition, several derived counters are provided for your selection which measure percent utilization of certain system resources. Error and warning thresholds for the monitor can be set on one or more SunONE server performance statistics or HTTP response codes.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"SunONE Server Monitor Overview" on page 605

The Add/Edit SunONE Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Stats-XML URL	Specify the URL to the stats-xml file on the SunONE server you want to monitor. This is usually in the form <code>http://server_id:port/stats-xml/<stats-xml-file></code> where <code><stats-xml-file></code> is <code>nesstats.xml</code> or <code>iwsstats.xml</code> .
Authorization User Name	Type the user name of the SunONE server you want to monitor.
Authorization Password	Type the password of the SunONE server you want to monitor.
HTTP Proxy	(Optional) A proxy server can be used to access the server. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, type the name here. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, type the password here.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	<p>The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p>Note: Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Timeout value of more than 60 seconds to enable the server time to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.</p>

Tuxedo Monitor Settings

Description	<p>The Tuxedo Monitor allows you to monitor the availability of an BEA Tuxedo server. The error and warning thresholds for the monitor can be set on one or more Tuxedo Monitor performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Tuxedo Monitor Overview" on page 606

The Add/Edit Tuxedo Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Type the name or IP address of the server. The address should match that dedicated to the Tuxedo Workstation component (the WSL process). On UNIX servers, type the full path of the applicable server.
Port	Type the port number for the Tuxedo server. The port number should match the port dedicated to the Tuxedo Workstation component (the WSL process). Default value: 65535
User	Type the user name if required to access the Tuxedo server.
Password	Type the Password if required to access the Tuxedo server.
Client Name	Type an optional client name for the Tuxedo server.
Connection Data	Type any extra or optional Connection Data to be used for connecting to the Tuxedo server. In some cases, this may be a hexadecimal number.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

UDDI Monitor Settings

Description	<p>The UDDI Monitor checks the availability and round-trip response time of the UDDI server.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"UDDI Monitor Overview" on page 607

The Add/Edit UDDI Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Inquiry URL	Type the UDDI server inquiry URL. Example: <code>http://uddi.company.com/inquiry/</code>
Business Name	Type the business entity to search for in the UDDI server.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Max Businesses Number	The maximum allowed business entities to receive from the UDDI server (1–200). Default value: 10

VMware Performance Monitor Settings

<p>Description</p>	<p>The VMware Performance Monitor enables you to monitor performance statistics of the VMware infrastructure for various server applications. The supported applications include VirtualCenter 2.0.x, ESX Server 3.0.x, and others.</p> <p>The monitor supports monitoring both single VMware ESX server installations and ESX server clusters managed by VMware Virtual Centers.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<p>The following are the requirements for monitoring:</p> <ul style="list-style-type: none"> ▶ The monitored VI server or ESX server cluster must be directly accessible by the SiteScope server (no proxy involved). ▶ The VI server or ESX server cluster provides connection either by http or by https (depending on the VI server configuration). If https is used, server certificate must be imported to the SiteScope. <p>Monitors must be created in a group in the monitor tree.</p>
<p>Useful Links</p>	<p>"VMware Performance Monitor Overview" on page 608</p>

The Add/Edit VMware Performance Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Connection URL	<p>Select the VMware infrastructure for the server you want to monitor.</p> <p>The format of the URL is: <protocol>://<server_name>/sdk</p> <ul style="list-style-type: none"> ▶ <protocol> is either http or https. ▶ <server_name> is the name of the VI server.
User Name	The user name of the VMware web service's administrator.
Password	The password of the VMware web service's administrator.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Socket timeout	<p>Type the number in milliseconds that the VMware monitor should wait for data from a server during a single data request. Once the socket timeout period elapses, the monitor logs an error and reports the error status.</p> <p>Note:</p> <ul style="list-style-type: none">▶ The socket timeout value must be larger than 0.▶ The value of zero is interpreted as an infinite timeout. <p>Default value: 600000</p>

WebLogic Application Server Monitor Settings

Description	<p>The WebLogic Application Server Monitor allows you to monitor the statistics of a WebLogic version 6 through 8 servers.</p> <p>For WebLogic Application Server version 9, a JMX monitor should be used. The error and warning thresholds for the monitor can be set on one or more Application Server statistics.</p> <p>WebLogic Application Server Monitors cannot be used to monitor WebLogic 9.x servers. To monitor these servers, use a JMX monitor.</p> <p>For further details, see “Creating a JMX Monitor for a WebLogic 9.x or 10.x Server” on page 778.</p> <p>If you are using a WebLogic 9.x server, this chapter is not relevant.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“WebLogic Application Server Monitor Overview” on page 610

The Add/Edit WebLogic Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Target	Type the name of the server where WebLogic is running.
Server	Type the address of the server where WebLogic is running.
Port Number	Type the port number that the WebLogic server is responding on. Default value: 7001
User Name	Type the user name required to log into the WebLogic server.
Password	Type the password required to log into the WebLogic server.
Secure Server	Select this box if you are using a secure server connection option. If you select this option, you must type the applicable port number used by the WebLogic server for secure connections. Default value: 7002
WLCipher Jar File	For some versions of WebLogic Server, you must install a copy of the <code>wlcipher.jar</code> file from the WebLogic server onto the SiteScope server to enable monitoring over SSL. Type the absolute path to the file on the SiteScope machine in this box. Example: <code>C:\bea\weblogic81\server\lib\wlcipher.jar</code> Note: This option is for use only with the Secure Server (SSL) option.

GUI Element	Description
WebLogic License File	<p>You use this box only when you want to enable the Secure Server (SSL) option. Type the absolute path to the BEA license file that was copied to the SiteScope machine.</p> <p>Example: C:\bea\license.bea</p>
Location of JVM	<p>Type the full path to the Java Virtual Machine (JVM) in which the WebLogic monitoring process should be run. For monitors that do not use the Secure Server option, this is not required.</p> <p>For monitors which do use the Secure Server option, a separate JVM must be installed on the server where SiteScope is running. This other JVM must be version 1.4.1 or earlier. This is not the same JVM version used by SiteScope.</p> <p>Example: C:\j2sdk1.4.1\jre\bin\javaw.exe</p>
Timeout	<p>The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p>Default value: 180</p> <p>It is recommended not to change the default value so that performance is not adversely affected.</p>
WebLogic Jar File	<p>Type the absolute path to the weblogic.jar file on the SiteScope machine. This file must be installed on the SiteScope server and can be downloaded from the WebLogic server.</p> <p>Example: c:\bea\weblogic7\ebcc\lib\ext\weblogic.jar</p> <p>This file is not strictly required for monitoring some earlier versions of WebLogic 6. In this case, leaving this box blank normally causes any necessary classes to be downloaded directly from the WebLogic server. Note that this is not as efficient as loading the classes from the *.jar file on the server where SiteScope is running.</p>

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

WebSphere Application Server Monitor Settings

Description	<p>The WebSphere Application Server Monitor allows you to monitor the availability and server statistics of an IBM WebSphere Application Server 3.5.x, 4.x, 5.x, and 6.x. The error and warning thresholds for the monitor can be set on one or more WebSphere Application Server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"WebSphere Application Server Monitor Overview" on page 613

The Add/Edit WebSphere Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Target	Type the logical name of the server you want to monitor. If this box is left empty, the hostname entered above is used.
Server	Choose the server where the WebSphere Application Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.
Port Number	Type the port number for the SOAP.
User Name	Type the user name to access the WebSphere Application Server if one has been configured.
Password	Type the password to access the WebSphere Application Server if one has been configured.
Credentials	Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243. Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.
Security Realm	Only relevant for WebSphere 3.5 users. Specify the security realm of the WebSphere application server.
Version	Type the version of the WebSphere application you are monitoring.

GUI Element	Description
WebSphere Directory	<ul style="list-style-type: none"> ▶ For 3.x: Type the path to a WebSphere 3.5x Directory. The directory you type here should contain at least a valid Admin Client installation. ▶ For 6.x: Type the path to the AppServer directory.
Client Properties File	For version 6.x, type SOAP.client.props .
Classpath	(Optional) Type additional classpath variables that are to be used by the WebSphere JVM running on the SiteScope machine.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

In WebSphere Application Server version 6.x, you can enable global security by configuring the properties below:

GUI Element	Description
Trust Store	This is the full directory path of file DummyClientTrustFile.jks . This file is in the client monitor directory on the SiteScope machine. The default path is C:\WebSphere\AppServer\profiles\default\etc .
Trust Store Password	This is the password for the SSL trust store file. Default value: WebAS
Key Store	This is the full directory path of file DummyClientKeyFile.jks . This file is in the client monitor directory on the SiteScope machine. Default value: C:\WebSphere\AppServer\profiles\default\etc

GUI Element	Description
Key Store Password	<p>This is the password for the SSL key store file.</p> <p>Default value: WebAS</p> <p>The values for Trust Store, Trust Store Password, Key Store, and Key Store Password are automatically configured and can be found in the following directories:</p> <ul style="list-style-type: none"> ➤ on Windows platform, in <drive>:\WebSphere\AppServer\etc\ ➤ on Solaris platform, in /opt/WebSphere/AppServer/etc/ ➤ on Linux platform, in /opt/IBMWebAS/etc/ <p>For more information about Key Store passwords, refer to the IBM Information Center (http://publib.boulder.ibm.com/infocenter/wasinfo/v4r0/index.jsp?topic=/com.ibm.websphere.v4.doc/wasa_content/050703.html) and search for SSL configuration.</p>

WebSphere MQ Status Monitor Settings

Description	<p>The WebSphere MQ Status Monitor allows you to monitor the performance attributes of MQ Objects (channels and queues) on MQ Servers v5.2 and later. Both performance attributes and events for channels and queues can be monitored.</p> <p>This monitor was formerly known as MQSeries.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<p>This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</p> <p>Monitors must be created in a group in the monitor tree.</p>
Useful Links	<p>"WebSphere MQ Status Monitor Overview" on page 617</p>

The Add/Edit WebSphere MQ Status Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
MQ Server Name	<p>Specify the host name of the MQ Server you want to monitor. Type the network name of the server or the IP address of the server.</p> <p>Example: mqmachinename</p>
MQ Server Port	<p>Specify the port number of the target MQ Server.</p> <p>Default value: 1414</p>

GUI Element	Description
Server Connection Channel	Type the name of the server connection channel of the target MQ server. Check with the MQ Server administrator for the name syntax of the server connection channel.
Queue Manager	Type the name of the queue manager whose queues or channels are to be monitored.
Alternate Queue Manager	(Optional) You can type an alternate queue manager name that has been set up to forward its events to the primary queue manager specified above if you are also interested in monitoring those events.
Selected Measurements	<p>The Get Measurements button allows you to add or delete counters for the monitor. Click this button after you have specified all the server information above.</p> <p>There are two primary window panes on the Measurement Selection page:</p> <ul style="list-style-type: none"> ▶ Available Measurements. A browse window which displays available MQ queue instances and channel instances, and counters to choose from. You must first select either Queue or Channel Objects to work with in the Objects drop-down list. Once an object is selected, a connection to the MQ server is made, using the server information provided in the previous page. A list of available queues or channels is displayed, both system and user instances, depending on the object type selected. After pressing the Add button, any number of instances and counters you select using check boxes are combined into individual monitoring counters and listed in the Selected Measurements window. ▶ Selected Measurements. Lists the counters you have selected to be monitored from pressing the Add button. The X check box preceding each counter allows you to delete the counter.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Channel Status Code Scheme	<p>Select a reporting schemes for Channel Status Code values:</p> <ul style="list-style-type: none"> ▶ Use HP coding scheme. Report the actual or original channel status codes as documented in the IBM MQ literature. ▶ Use IBM MQ coding scheme. Report channel status codes in ascending values that are directly proportional to the health of the channel. SiteScope reports a channel status value from 0 (least healthy) to 6 (healthiest). For details, see “Channel Status Codes” on page 619.

WebSphere Performance Monitor Settings

Description	<p>The WebSphere Performance Monitor to monitor the server statistics of IBM WebSphere Server (versions 3.0x, 3.5, 3.5.x, and 4.0) by using a WebSphere Performance Servlet. The error and warning thresholds for the monitor can be set on one or more performance statistics.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“WebSphere Performance Servlet Monitor Overview” on page 622

The Add/Edit WebSphere Performance Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Server	<p>Type the server you want to monitor. On UNIX servers, type the full path of the server. You are also asked to type the URL to the performance servlet as installed on the WebSphere server and the port number that is to be used to access the server.</p> <p>For WebSphere versions 3.x.x, the URL can be viewed by using the Servlet Properties page in the WebSphere Admin Console.</p> <p>For WebSphere version 4.0, the URL normally has the form: <code>http://<server:port_number:>/wasPerfTool/servlet/perfservlet</code>.</p>
Secure Server	Type the secure server you want to monitor.
Target	Type the logical name of the server that is the target of this monitor instance. If you leave this box empty, the hostname is used. Depending on the deployment of the WebSphere application in your infrastructure, this may be the same as the Server selected above.
Port	<p>Type the port number to the WebSphere server you want to monitor.</p> <p>Default value: 80 for non-secure server and 443 for secure server.</p>

GUI Element	Description
Servlet URL	<p>URL of the performance servlet.</p> <p>For WebSphere 4.0, the default URL is /wasPerfTool/servlet/perfservlet. In earlier versions, the URL is chosen during the installation of the servlet.</p> <p>For WebSphere 6.0 and later, use the URL: /wasPerfTool/servlet/perfservlet?version=5. In either case, the URL can be found in the Servlet properties page of the Admin Console.</p>
Authorization User Name	<p>If the URL requires authorization, type the user name here.</p>
Password	<p>If the URL requires authorization, type the password here.</p>
Proxy Server User Name	<p>If the proxy server requires a name and password to access the server, type the name here.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Proxy Server Password	<p>If the proxy server requires a name and password to access the server, type the password here.</p>
Counters	<p>The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p>
Get Counters	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	Type the time, in seconds, that the monitor should wait for a response from the Performance Servlet. If a response is not received within the interval of the timeout, the monitor reports a timeout error.
Refresh Selected Metrics Frequency	Select a time interval at which the WebSphere server should update the metrics that are requested by this monitor. This value should be equal to or less than the Frequency time interval for the monitor.

16

Database Monitors

This chapter includes the main concepts and reference information for monitoring different types of database applications.

This chapter includes:

Concepts

- ▶ DB2 Monitor Overview on page 723
- ▶ DB2 8.x Monitor Overview on page 725
- ▶ Database Counter Monitor Overview on page 726
- ▶ Database Query Monitor Overview on page 729
- ▶ LDAP Monitor Overview on page 738
- ▶ Microsoft SQL Server Monitor Overview on page 739
- ▶ Oracle Database Monitor Overview on page 740
- ▶ Sybase Monitor Overview on page 742

Reference

- ▶ Database Monitors User Interface Settings on page 743

DB2 Monitor Overview

Use the DB2 Monitor to monitor DB2 servers for availability and proper function. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate DB2 Monitor instance for each IBM DB2 server in your environment.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

Setup Requirements

The following are several key requirements for using the DB2 Monitor:

- ▶ The DB2 client files and libraries must be copied to the machine where SiteScope is running. The DB2 client Control Center must be installed on the SiteScope server.
- ▶ In the DB2 Control Center console, the system you want to monitor must be added to the **Systems** list. In the Add System dialog box, type the information required:
 - ▶ **System Name:** <db2_server_name>
 - ▶ **Remote Instance:**DB2
 - ▶ **Host Name:** <db2_server_name>
 - ▶ **Service Name:** <db2_server_port> (the default is port 50000)

Click **Retrieve** and then click **OK**.

- ▶ A remote DB2 instance needs to be added to the <db2_server_name> node in the Control Center Console. Select the <db2_server_name> node and select to add and Instance. Type the information required in the dialog box:
 - ▶ **Remote Instance:** DB2
 - ▶ **Instance Name:**<database_name_used_for_DB2_monitor>
 - ▶ **Host Name:** <db2_server_name>
 - ▶ **Service Name:** <db2_server_port> (the default is port 50000)

and then click **OK**.

For details on configuring this monitor, see “DB2 Monitor Settings” on page 743.

DB2 8.x Monitor Overview

Use the DB2 Monitor to monitor DB2 servers for availability and proper functioning. You can monitor multiple parameters or counters with a single monitor instance. This allows you to monitor server loading for performance, availability, and capacity planning. Create a separate DB2 Monitor instance for each Database in your IBM DB2 environment.

Setup Requirements

The following are several key requirements for using the DB2 8.x Monitor:

- ▶ JDBC drivers for connecting to the DB2 Database server. These can be found in your DB2 server installation directories. You must use the following files: `db2jcc_license_cu.jar`, `db2jcc_license_cisuz.jar`, `db2jcc.jar`.
- ▶ This monitor uses the Snapshot mirroring functionality supported by DB2. You must enable the Snapshot Mirror on your DB2 instance to retrieve counters. See the following information from the IBM DB2 documentation <http://www-128.ibm.com/developerworks/db2/library/techarticle/dm-0408hubel/>.

For details on configuring this monitor, see “DB2 8.x Monitor Settings” on page 745.

Database Counter Monitor Overview

Use the Database Counter Monitor to make SQL queries for performance metrics from any JDBC-accessible database. This monitor provides optional support for calculating deltas and rates for metrics between monitor runs. You can monitor multiple counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning.

Note: The Database Counter Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

Setup Requirements

The following are several key requirements for using the Database Counter Monitor:

- ▶ You must have a copy of the applicable JDBC database driver file (for example, the Oracle thin driver is packaged in a file called `classes12.zip`) on the SiteScope server. Copy the downloaded driver file into the `<SiteScope root directory>\WEB-INF\lib` subdirectory. If the file is in zip format, do not unzip the file. Stop and restart the SiteScope service after copying the driver file to the SiteScope machine.
- ▶ You must know the syntax for accessing the database driver. Examples of common database driver strings are:
 - ▶ **sun.jdbc.odbc.JdbcOdbcDriver.** JDBC-ODBC Bridge Driver from Sun Microsystems.
 - ▶ **com.inet.tds.TdsDriver.** TDS driver from i-net Software for Microsoft SQL databases. This driver is deployed with SiteScope.
 - ▶ **com.inet.ora.OraDriver.** A driver from Oracle for Oracle databases. This driver is deployed with SiteScope.

- ▶ **com.mercury.jdbc.sqlserver.SQLServerDriver.** DataDirect driver from DataDirect Technologies. It is an alternative to the TDS driver for those Microsoft SQL databases that use Windows NT authentication. This driver is deployed with SiteScope.
- ▶ **oracle.jdbc.driver.OracleDriver.** JDBC thin driver for Oracle 7 and 8 databases. This driver is an Oracle product and is supplied by Oracle.
- ▶ **org.postgresql.Driver.** The database driver for the Postgresql database.
- ▶ You must know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers.

Examples of common database connection URLs are:

- ▶ **jdbc:odbc:<dsname>**
where <dsname> is the data source name in the system environment or configuration.
- ▶ **jdbc:inetdae:<hostname>:<port>**
where <hostname> is the name of the host where the database is running and <port> is the port on which the database interfaces with the driver.
- ▶ **jdbc:mercury:sqlserver://<hostname>:1433;DatabaseName=master;AuthenticationMethod=type2**
where <hostname> is the name of the host where the database is running.
- ▶ **jdbc:oracle:thin:@<hostname>:<port>:<dbname>**
where <hostname> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <dbname> is the SID of the Oracle database instance.
- ▶ **jdbc:postgresql://<hostname>:<port>/<dbname>**
where <hostname> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <dbname> is the name of the Postgresql database.

- ▶ Generally, you should only have one instance of each type of JDBC driver client installed on the SiteScope machine. If there is more than one instance installed, SiteScope may report an error and be unable to connect to the database. For example, installing two **classes12.zip** files from two different versions of Oracle is unlikely to work.
- ▶ You must have a database user login that SiteScope can use to access the database with **CREATE SESSION** system privileges. SiteScope is only able to run the SQL queries that this user has permission to run on the database.

Note: When Windows authentication is used to connect to the database, configure SiteScope using the following settings:

- ▶ Database Connection URL: **jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>;AuthenticationMethod=type2.**
- ▶ Database driver: **com.mercury.jdbc.sqlserver.SQLServerDriver.**
- ▶ Leave the **Database User name** and **Database Password** boxes empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.

For details on configuring this monitor, see “Database Counter Monitor Settings” on page 749.

Database Query Monitor Overview

Use the Database Query Monitor to monitor the availability and proper functioning of your database application. If your database application is not working properly, the user may not be able to access Web content and forms that depend on the database. Most importantly, the user cannot complete e-commerce transactions that are supported by databases. You can also use the Database Query Monitor to isolate performance bottlenecks. If the database interaction time and the associated user URL retrieval times are both increasing at about the same amount, the database is probably the bottleneck.

Usually the most important thing to monitor in databases are the queries used by your most frequently used and most important Web applications. If more than one database is used, you must monitor each of the databases.

Each time the Database Query Monitor runs, it returns a status, the time it takes to perform the query, the number of rows in the query result, and the first two fields in the first row of the result and writes them in the monitoring log file.

You can also monitor internal database statistics. The statistics provided by each database are different but may include items such as database free space, transaction log free space, transactions/second, and average transaction duration.

Setup Requirements

The steps for setting up a Database Query Monitor vary according to what database software you are trying to monitor. The following is an overview of the requirements for using the Database Query Monitor:

- You must install or copy a compatible JDBC database driver or database access API into the required SiteScope directory location.

Many database driver packages are available as compressed (zipped) archive files or .jar files. Copy the downloaded driver file into the `<SiteScope root directory>\WEB-INF\lib` subdirectory. Do not unzip the file.

- ▶ You must know the syntax for accessing the database driver. Examples of common database driver strings are:
 - ▶ **sun.jdbc.odbc.JdbcOdbcDriver**. JDBC-ODBC Bridge Driver from Sun Microsystems.
 - ▶ **com.inet.tds.TdsDriver**. TDS driver from i-net Software for Microsoft SQL databases. This driver is deployed with SiteScope.
 - ▶ **com.inet.ora.OraDriver**. A driver from Oracle for Oracle databases. This driver is deployed with SiteScope.
 - ▶ **com.mercury.jdbc.sqlserver.SQLServerDriver**. DataDirect driver from DataDirect Technologies. It is an alternative to the TDS driver for those Microsoft SQL databases that use Windows NT authentication. This driver is deployed with SiteScope.
 - ▶ **oracle.jdbc.driver.OracleDriver**. JDBC thin driver for Oracle 7 and 8 databases. This driver is an Oracle product and is supplied by Oracle.
- ▶ You must know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers.

Examples of common database connection URLs are:

- ▶ **jdbc:odbc:<dsname>**
where <dsname> is the data source name in the system environment or configuration.
- ▶ **jdbc:inetdae:<hostname>:<port>**
where <hostname> is the name of the host where the database is running and <port> is the port on which the database interfaces with the driver.
- ▶ **jdbc:mercury:sqlserver://<hosthost>:1433;DatabaseName=master;AuthenticationMethod=type2**
where <hostname> is the name of the host where the database is running.
- ▶ **jdbc:oracle:thin:@<hostname>:<port>:<dbname>**
where <hostname> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <dbname> is the name of the Oracle database instance.

- ▶ The database you want to monitor needs to be running, have a database name defined, and have at least one named table created in the database. In some cases, the database management software needs to be configured to enable connections by using the middleware or database driver.
- ▶ You need a valid user name and password to access and perform a query on the database. In some cases, the machine and user account that SiteScope is running on must be given permissions to access the database.
- ▶ You must know a valid SQL query string for the database instance and database tables in the database you want to monitor. Consult your database administrator to work out required queries to test.

Note: When Windows authentication is used to connect to the database, configure SiteScope using the following settings:

- ▶ Database Connection URL: **`jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>;AuthenticationMethod=type2.`**
 - ▶ Database driver: **`com.mercury.jdbc.sqlserver.SQLServerDriver.`**
 - ▶ Leave the **Database User name** and **Database Password** boxes empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.
-

Accessing Oracle Databases Without Using ODBC

If you want to monitor an Oracle database without using ODBC, a good alternative is to use the Oracle Thin JDBC Drivers.

To set up SiteScope to use the JDBC Thin Drivers:

- 1 Download the Oracle Thin JDBC drivers from the Oracle Web site (may require service/support agreement with Oracle).
- 2 Copy the downloaded driver package into the `<SiteScope root directory>\WEB-INF\lib` subdirectory.

Note: Do not extract the files from the archive file.

- 3 Stop and restart the SiteScope service.
- 4 Add a Database Query Monitor within SiteScope.

The **Database Connection URL** format for the Oracle JDBC driver is:

`jdbc:oracle:thin:@<tcp address>:<tcp port>:<database SID>`

For example to connect to the ORCL database on a machine using port 1521 you would use:

`jdbc:oracle:thin:@206.168.191.19:1521:ORCL`

Note: After the word thin is a colon (:) and an at (@) symbol.

The **Database Driver** for the Oracle thin JDBC driver is:

`oracle.jdbc.driver.OracleDriver`

Type this string into the **Database Driver** text box under the Advanced Settings section of the Add Database Query Monitor form.

Possible Errors Using the Oracle Thin Driver

- **"error, connect error, No suitable driver"**: check for syntax errors in "Database Connection URL", such as dots instead of colons.
- **"error, connect error, Io exception: The Network Adapter could not establish the connection"**: in "Database Connection URL", check `jdbc:oracle:thin:@206.168.191.19:1521:ORCL`.
- **"error, connect error, Io exception: Invalid connection string format, a valid format is: 'host:port:sid'"**: in "Database Connection URL", check `jdbc:oracle:thin:@206.168.191.19:1521:ORCL`.
- **"error, connect error, Invalid Oracle URL specified: OracleDriver.connect"**: in "Database Connection URL", check for a colon before the "@"
`jdbc:oracle:thin@206.168.191.19:1521:ORCL`.
- **"Refused:OR=(CODE=12505)(EMFI=4))"**: in "Database Connection URL", check the database SID is probably incorrect (ORCL part). This error can also occur when the tcp address, or tcp port is incorrect. If this is the case, verify the tcp port and check with the your database administrator to verify the proper SID.
- **"String Index out of range: -1"**: in "Database Connection URL", check for the database server address, port, and the database SID.
- **"error, driver connect error, oracle.jdbc.driver.OracleDriver"**: check syntax in item "Database Driver".
- **"error, driver connect error, oracle.jdbc.driver.OracleDriver"**: check that driver is loaded in correct place.
- **"error, connect error, No suitable driver"**: check driver specified in item "Database Driver".
- **"error, connect error, No suitable driver"**: check for syntax errors in "Database Connection URL", such as dots instead of colons.

Monitoring Informix Databases

Monitoring a Informix database requires the use of a JDBC driver.

To enable SiteScope to monitor an Informix database:

- 1** Download the Informix JDBC driver from Informix. See the Informix Web site for details.
- 2** Uncompress the distribution file.
- 3** Open a DOS window and go to the **jdbc140jc2** directory.
- 4** Unpack the driver by running the following command:
`c:\SiteScope\java\bin\java -cp . setup`
- 5** Copy **ifxjdbc.jar** to the **<SiteScope root directory>\WEB-INF\lib** subdirectory.
- 6** Stop and restart SiteScope.
- 7** Use your browser to add a Database Query Monitor within SiteScope.

The **Database Connection URL** format for the Informix JDBC driver is:

```
jdbc:informix-sqli://<database hostname>:<tcp port><database server>:INFORMIXSERVER=<database>
```

If you require a username and password the Database Connection URL format for the Informix JDBC driver is:

```
jdbc:informix-sqli://<database hostname>:<tcp port><database server>:INFORMIXSERVER=<database>;user=myuser;password=mypassword
```

For example, to connect to the Database Server **sysmaster** running on the machine called **pond.thiscompany.com** and the Database called **maindbase**, type:

```
jdbc:informix-sqli://pond.thiscompany.com:1526/sysmaster:INFORMIXSERVER=maindbase;
```

The **Database Driver** for the Informix JDBC driver is:

```
com.informix.jdbc.IfxDriver
```

Type this string into the **Database Driver** box under the Main Settings section of the Add Database Query Monitor form.

Monitoring MySQL Databases

Monitoring a MySQL database requires the use of a JDBC driver.

To enable SiteScope to monitor a MySQL database:

- 1** Download the MySQL JDBC driver from the MySQL web site (<http://www.mysql.com>).
- 2** Uncompress the distribution file.
- 3** Among all the other files, you should find a file with a .jar extension.
- 4** Copy the .jar file into the <SiteScope root directory>\WEB-INF\lib directory.
- 5** Stop and restart SiteScope.
- 6** Use your browser to add a Database Query Monitor within SiteScope.

The Database Connection URL format for the MySQL JDBC driver is:

```
jdbc:mysql://<database hostname>[:<tcp port>]/<database>
```

For example to connect to the MySQL database "aBigDatabase" on a machine using the standard MySQL port number 3306 you would use:

```
jdbc:mysql://206.168.191.19/aBigDatabase
```

If you are using a different port to connect to the database, include that port number as part of the IP address.

The specification for the MySQL JDBC driver is: org.gjt.mm.mysql.Driver

Type this string into the **Database Driver** box under the Main Settings section of the Add Database Query Monitor form.

Possible Errors Using the MySQL Driver

If, after setting this up, you get an authorization error in the Database Query Monitor, then you may have to grant rights for the SiteScope machine to access the MySQL database. Consult the MySQL Database administrator for setting up privileges for the SiteScope machine to access the MySQL server.

Monitoring Sybase Databases

To use JDBC drivers with your Sybase SQL server, perform the following steps:

- 1 Obtain the driver for the version of Sybase that you are using. For example, for version 5.X databases you need **jconn2.jar**. If you have Jconnect, you should be able to find a driver in the Jconnect directory.
- 2 Place the zip file in the **<SiteScope root directory>\WEB-INF\lib** directory.

Note: Do not extract the zip file.

- 3 Stop and restart the SiteScope service.
- 4 Add a Database Query Monitor in SiteScope.
- 5 For the **Database Connection URL**, use the syntax of:

`jdbc:sybase:Tds:hostname:port`

For example to connect to SQL server named **bgsu97** listening on port **2408**, you would type:

`jdbc:sybase:Tds:bgsu97:2408`

- 6 You can specify a database by using the syntax:

`jdbc:sybase:Tds:hostname:port#/database`

For example to connect to SQL server named **bgsu97** listening on port **2408** and to the database of **quincy**, you would type:

`jdbc:sybase:Tds:bgsu97:2408/quincy`

- 7 For the **Database Driver**, type:
 - `com.sybase.jdbc.SybDriver` (for Sybase version 4.x)
 - `com.sybase.jdbc2.jdbc.SybDriver` (for Sybase version 5.x)
- 8 Type the database user name and password.

9 Type a query string for a database instance and table in the Sybase database you want to monitor.

- For example, Sp_help should work and return something similar to:
good, 0.06 sec, 27 rows, KIRK1, dbo, user table
- Alternately, the query string select * from spt_ijdbc_mda should return something similar to:
Monitor: good, 0.06 sec, 175 rows, CLASSFORNAME, 1, create table #tmp_class_for_name (xtbinaryoffrow image null),
sp_ijdbc_class_for_name(?), select * from #tmp_class_for_name, 1, 7,
12000, -1

10 Click OK.

Possible Errors with Sybase Database Monitoring

- Verify you are using the correct driver for the version of Sybase you are monitoring. Type com.sybase.jdbc.SybDriver for Sybase version 4.x. and com.sybase.jdbc2.jdbc.SybDriver for Sybase version 5.x.
- If you get the error: "**error, driver connect error, com/sybase/jdbc/SybDriver**", click **Edit** for the monitor and verify that there are no spaces at the end of the driver name. Save the changes and try the monitor again.
- If you get the error: "**connect error, JZ006: Caught IOException: java.net.UnknownHostException: dbservername**", verify the name of the database server in the **Database Connection URL** box is correct.

Scheduling This Monitor

You may want to monitor your most critical and most common queries frequently, every 2-5 minutes. Database statistics that change less frequently can be monitored every 30 or 60 minutes.

For details on configuring this monitor, see "Database Query Monitor Settings" on page 754.

LDAP Monitor Overview

If your LDAP server is not working properly, the user is not able to access and update information in the directory. Most importantly, the user is not able to perform any authentication using the LDAP server. Use the LDAP Monitor to monitor the availability and proper functioning of your LDAP server. Another reason to monitor the LDAP server is so that you can find performance bottlenecks. If your end user and LDAP times are both increasing at about the same amount, the LDAP server is probably the bottleneck.

The most important thing to monitor is the authentication of a specific user on the LDAP server. If more than one LDAP server is used, you should monitor each of the servers. You may also want to monitor round trip time of the authentication process.

Status

Each time the LDAP Monitor runs, it returns a status based on the time it takes to perform the connection.

The possible values for the LDAP status are:

- OK
- warning
- error

An error status or warning status is returned if the current value of the monitor is anything other than OK. Errors occur if SiteScope is unable to connect, receives an unknown hostname error, or the IP address does not match the hostname.

For details on configuring this monitor, see “LDAP Monitor Settings” on page 760.

Microsoft SQL Server Monitor Overview

Use the Microsoft SQL Server Monitor to monitor the server performance metrics pages for SQL Servers versions 6.5, 7.1, 2000, and 2005 on Windows NT systems. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Microsoft SQL Server you are running.

Note:

- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of a Microsoft SQL 2005 server. For details, see “Microsoft SQL Server Solution Template” on page 1319.
 - ▶ This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).
-

Setup Requirements

- ▶ The Microsoft SQL Server Monitor uses performance counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you must define the connection to these servers under the Microsoft Windows Remote Preferences option in the SiteScope Preferences container. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.
- ▶ The Remote Registry service must be running on the machine where the SQL Server is running if the SQL Server is running on Windows 2000.

For details on configuring this monitor, see “Microsoft SQL Server Monitor Settings” on page 764.

Oracle Database Monitor Overview

Use the Oracle Database Monitor to monitor the server performance statistics from Oracle Database servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate Oracle Database Monitor instance for each Oracle database server in your environment.

Note: SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of an Oracle Database server. For details, see “Oracle Database Solution Template” on page 1337.

Setup Requirements

The following are several key requirements for using the Oracle Database Monitor:

- ▶ You must have a copy of the applicable Oracle JDBC database driver file (for example, `classes12.zip`) on the SiteScope server. Copy the downloaded driver file into the `<SiteScope root directory>\WEB-INF\lib` subdirectory. Do not unzip the file. Stop and restart the SiteScope service after copying the driver file to the SiteScope machine.

Note: More than one driver file is available for download. Some drivers support more than one version of Oracle database (for example, the `classes12.zip` Oracle JDBC thin driver) while others only support a particular version. If you are monitoring a recent version of Oracle database, download the latest version of the database driver.

- ▶ You must supply the correct **Database Connection URL**, a database user name and password when setting up the monitor. When using the Oracle thin driver, the database connection URL has the form of:
jdbc:oracle:thin:@<tcp address>:<server name or IP address>:<database sid>.

For example, to connect to the ORCL database on a machine using port 1521 you would use:

```
jdbc:oracle:thin:@206.168.191.19:1521:ORCL.
```

Note: The colon (:) and the at (@) symbols must be included as shown.

- ▶ You must specify the Oracle **Database Driver** that was installed on the SiteScope server when setting up the monitor. The Database Driver for the Oracle thin JDBC driver is `oracle.jdbc.driver.OracleDriver`.
- ▶ You should have only one version of each driver installed on the SiteScope machine. If there is more than one version installed, SiteScope may report an error and be unable to connect to the database.
- ▶ The user specified in **username** must be granted the permission to access System tablespace.

For details on configuring this monitor, see “Oracle Database Monitor Settings” on page 766.

Sybase Monitor Overview

Use the Sybase Monitor to monitor the server performance data for Sybase database servers. You can monitor multiple parameters or counters with a single monitor instance. Create a separate monitor instance for each Sybase server in your environment.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

Setup Requirements

- ▶ Before you can use the Sybase Monitor, you have to configure the Sybase server environment. The Sybase Monitor connects to the Sybase ASE server by using the Adaptive Server Enterprise Monitor Server and retrieves metrics from the server using Sybase-provided libraries. When connecting to the monitored server, you connect to the Adaptive Server Enterprise Monitor Server, not the Sybase server. The Adaptive Server Enterprise Monitor Server is an application that runs on the same machine as Sybase server and retrieves performance information from the Sybase server. The Adaptive Server Enterprise Monitor Server usually has the same server name as the Sybase server, but with the suffix `_ms`. For example, if the name of the Sybase database application server is `back-endddb`, the name of the Adaptive Server Enterprise Monitor Server for that server would be `back-endddb_ms`.
- ▶ You also have to install the Sybase Central client on the machine where SiteScope is running to connect to the Adaptive Server Enterprise Monitor Server. The version of the client software that you install must be at least as recent or more recent than the version of the server you are trying to monitor. For example, if you have Sybase version 11.0 servers, you must use the Sybase Central client version 11.0 or later. You also must know the port number used to connect to the Sybase server. You can use the `dsedit` tool in the Sybase client console to test connectivity with the Adaptive Server Enterprise Monitor Server.

For details on configuring this monitor, see “Sybase Monitor Settings” on page 770.

Database Monitors User Interface Settings

This section describes:

- DB2 Monitor Settings on page 743
- DB2 8.x Monitor Settings on page 745
- Database Counter Monitor Settings on page 749
- Database Query Monitor Settings on page 754
- LDAP Monitor Settings on page 760
- Microsoft SQL Server Monitor Settings on page 764
- Oracle Database Monitor Settings on page 766
- Sybase Monitor Settings on page 770

DB2 Monitor Settings

Description	<p>Monitors the availability and performance statistics of an IBM DB2 database versions 6.x and 7.x. The 8.x versions of DB2 are not currently supported. The error and warning thresholds for the monitor can be set on one or more DB2 server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ➤ In the monitor tree, right-click a group and select Add Monitor. ➤ In the Contents tab for the group, click Add Monitor.
Important Information	<p>Monitors must be created in a group in the monitor tree.</p>
Useful Links	<p>"DB2 Monitor Overview" on page 723</p>

The Add/Edit DB2 Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Type the address or name of the server where the DB2 database is running.
Node Name	Type the DB2 database node name that you want to monitor. Example: DB2 is a default node created by DB2 installation.
User Name	Type the DB2 database user name to be used to access the DB2 server. This is usually a DB2 administrator user name.
Password	Type the password for the user specified above.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

DB2 8.x Monitor Settings

Description	<p>Monitors the availability and performance statistics of an IBM DB2 database for versions 8.x. The error and warning thresholds for the monitor can be set on up to ten DB2 server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"DB2 8.x Monitor Overview" on page 725

The Add/Edit DB2 8.x Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
DB2 Server	Type the address or name of the server where the DB2 8.x database is running.
Port	The port on which the DB2 8.x database accepts connections. Default value: 5000
Database	Type the DB2 database node name that you want to monitor. Example: DB2 is the default node name created by DB2 installation.

GUI Element	Description
Database User Name	Type the DB2 database user name to be used to access the DB2 server. This is usually a DB2 administrator user name.
Database Password	Type the password for the user specified above.
Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the database user name and password. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a database user name and password. A credential profile takes priority over database user name and password entries.</p>
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Partition	Partition to monitor. Example: -1 is the current partition; -2 is all partitions.
Calculate Rate	Select to calculate rates for counter values rather than the actual values returned from the monitored server. Example: If a counter counts logins and every second an average of two users log in to the database, the counter keeps growing. Selecting this option, the monitor displays the value 2, which means 2 user logins per second.

Database Connection Settings

Description	<p>The Database Connection Settings enable you to retrieve, share, and reuse database connections for database monitors that use any JDBC-compliant driver. When multiple database monitors use the same database, using a connection pool instead of an open connection for each monitor improves monitor performance and optimizes database server resource utilization.</p> <p>Connections can be shared regardless of monitor type. For example, SiteScope database logger, database tools (Database Connection, Database Information), database alerts, and database monitors (Oracle database, Database Counter, Database Query, DB2 8.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>
Important Information	You can set additional database options that affect all resources that connect to the database in the JDBC Global Options in the General Preferences container.
Useful Links	"JDBC Global Options" on page 255

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Use Connection Pool	<p>If this check box is selected, SQL connection sharing is enabled. This means that you use a connection pool rather than open and close a new connection for each monitor query.</p> <p>Default value: Selected</p>
Physically Close if idle connection count exceeds	<p>This is the maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool.</p> <p>Default value: 10</p>
Idle Connection Timeout	<p>The maximum amount of time, in seconds/minutes/hours/days, that a SQL connection remains unused after it has been returned to the SQL connection pool. When the time is exceeded, the connection is automatically closed.</p> <p>Default value: 5 minutes</p>
Query Timeout	<p>The amount of time, in seconds/minutes/hours/days, to wait for execution of a SQL statement. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored.</p> <p>Default value: 1 minute</p>

Database Counter Monitor Settings

<p>Description</p>	<p>The Database Counter Monitor allows you to monitor the availability of any database through a JDBC driver. The error and warning thresholds for the monitor can be set on one or more database server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ Monitors must be created in a group in the monitor tree.
<p>Useful Links</p>	<p>"Database Counter Monitor Overview" on page 726</p>

The Add/Edit Database Counter Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Database Connection URL	<p>Type the connection URL to the database you want to connect to. The syntax is <code>jdbc:oracle:thin:@<server name or IP address>:<database server port>:<sid></code>.</p> <p>Example: To connect to the ORCL database on a machine using port 1521 use: <code>jdbc:oracle:thin:@206.168.191.19:1521:ORCL</code>. The colon (:) and @ symbols must be included as shown.</p> <p>Note for using Windows Authentication: If you want to access the database using Windows authentication, type <code>jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>;AuthenticationMethod=type2</code> as the connection URL, and <code>com.mercury.jdbc.sqlserver.SQLServerDriver</code> as your database driver. Leave the Database User Name and Database Password boxes empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.</p>
Query	<p>Type a SQL query that returns at least two columns of data. The values in the first column of data are interpreted as the labels for the entries in the each row. The values in the first row are treated as labels for each entry in the column.</p>
Database User Name	Type the user name that SiteScope should use to connect to the database.
Database Password	Type the password for the user name that SiteScope should use to connect to the database.

GUI Element	Description
Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the database user name and password. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a database user name and password. A credential profile takes priority over database user name and password entries.</p>
Database Driver	<p>Type the driver used to connect to the database.</p> <p>Example: org.postgresql.Driver</p>
Counters	<p>The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p>
Get Counters	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
DB Machine Name	<p>The identifier for the target database server, as it should be reported to HP Business Availability Center.</p>
Divisor Query	<p>A SQL query that returns a single numeric value. The value of each counter is calculated by dividing the counter value as retrieved from the database divided by the Divisor Query value.</p>

GUI Element	Description
No Cumulative Counters	Selecting this check box turns off the default behavior of calculating the value of a counter as the difference between that counter's cumulative values (as retrieved from the database on consecutive monitor runs).
No Divide Counters	Selecting this check box turns off the default behavior of calculating the value of a counter as the value retrieved from the database (or the delta of two values retrieved from the database over consecutive monitor runs) divided by some number. The divisor is either taken from the Divisor Query, or it is the elapsed time in seconds since the previous monitor run.

Database Connection Settings

Description	<p>The Database Connection Settings enable you to retrieve, share, and reuse database connections for database monitors that use any JDBC-compliant driver. When multiple database monitors use the same database, using a connection pool instead of an open connection for each monitor improves monitor performance and optimizes database server resource utilization.</p> <p>Connections can be shared regardless of monitor type. For example, SiteScope database logger, database tools (Database Connection, Database Information), database alerts, and database monitors (Oracle database, Database Counter, Database Query, DB2 8.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>
Important Information	You can set additional database options that affect all resources that connect to the database in the JDBC Global Options in the General Preferences container.
Useful Links	"JDBC Global Options" on page 255

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Use Connection Pool	<p>If this check box is selected, SQL connection sharing is enabled. This means that you use a connection pool rather than open and close a new connection for each monitor query.</p> <p>This option is selected by default.</p>
Physically Close if idle connection count exceeds	<p>This is the maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool.</p> <p>Default value: 10</p>
Idle Connection Timeout	<p>The maximum amount of time, in seconds/minutes/hours/days, that a SQL connection remains unused after it has been returned to the SQL connection pool. When the time is exceeded, the connection is automatically closed.</p> <p>Default value: 5 minutes</p>
Query Timeout	<p>The amount of time, in seconds/minutes/hours/days, to wait for execution of a SQL statement. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored.</p> <p>Default value: 1 minute</p>

Database Query Monitor Settings

<p>Description</p>	<p>Checks that a database is working correctly by connecting to it and performing a query. Optionally, it can check the results of a database query for expected content.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p>Useful Links</p>	<p>"Database Query Monitor Overview" on page 729</p>

The Add/Edit Database Query Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Database Connection URL	<p>Type a URL to a Database Connection. One way to create a database connection is to use ODBC to create a named connection to a database.</p> <p>Example: First use the ODBC control panel to create a connection called <code>test</code>. Then, type <code>jdbc:odbc:test</code> in this box as the connection URL.</p> <p>Note for using Windows Authentication: If you want to access the database using Windows authentication, type <code>jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>;AuthenticationMethod=type2</code> as the connection URL, and <code>com.mercury.jdbc.sqlserver.SQLServerDriver</code> as your database driver. Leave the Database User Name and Database Password boxes empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.</p>
Database Driver	<p>Type the java class name of the JDBC database driver.</p> <p>The default driver uses ODBC to make database connections. SiteScope uses the same database driver for both primary and backup database connections.</p> <p>If a custom driver is used, the driver must also be installed in the <code><SiteScope root directory>\WEB-INF\lib</code> directory.</p> <p>Default value: <code>sun.jdbc.odbc.JdbcOdbcDriver</code></p>

GUI Element	Description
Database User Name	<p>Type the user name used to log in to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystems JDBC-ODBC bridge driver, sun.jdbc.odbc.JdbcOdbcDriver), you can leave this blank and choose NT Authentication when you setup the ODBC connection.</p> <p>With NT Authentication, SiteScope connects using the login account of the SiteScope service.</p> <p>Note: The specified user name must have privileges to run the query specified for the monitor.</p>
Database Password	<p>Type a password used to login to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystems JDBC ODBC bridge driver (sun.jdbc.odbc.JdbcOdbcDriver), you can leave this blank and choose NT Authentication when you create the ODBC connection.</p> <p>With NT Authentication, SiteScope connects using the login account of the SiteScope service.</p>
Query	<p>Type the SQL query to test.</p> <p>Example: select * from sysobjects</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Match Content	<p>Type a string of text to check for in the query result. If the text is not contained in the result, the monitor displays no match on content. This works for XML tags as well.</p> <p>You may also perform a Perl regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p>Example: <code>/href=Doc\d+\.\html/</code> or <code>/href=doc\d+\.\html/i</code></p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression.</p> <p>Example: <code>/Temperature: (d+)/</code> would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</p> <p>Note: The search is case sensitive.</p>
File Path	<p>Type the name of the file that contains the query you want to run. The file should be in a simple text format.</p> <p>Use this function as an alternative to the Query text box in the Main Settings pane for complex queries or queries that change and are updated by an external application.</p>

GUI Element	Description
<p>Column Labels</p>	<p>Type the field labels for the two columns returned by the query, separated by a comma (","). These column labels are used as data labels in SiteScope reports for Database Query Monitors.</p> <p>Note: The field labels should be two of the labels that are returned by the Query string entered above.</p>
<p>DB Machine Name</p>	<p>If you are reporting monitor data to an installation of HP Business Availability Center, type a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in an HP Business Availability Center report.</p> <p>Syntax exceptions: Use only alphanumeric characters for this entry. You can type the name of the monitored server or a description of the database.</p>

Database Connection Settings

Description	<p>The Database Connection Settings enable you to retrieve, share, and reuse database connections for database monitors that use any JDBC-compliant driver. When multiple database monitors use the same database, using a connection pool instead of an open connection for each monitor improves monitor performance and optimizes database server resource utilization.</p> <p>Connections can be shared regardless of monitor type. For example, SiteScope database logger, database tools (Database Connection, Database Information), database alerts, and database monitors (Oracle database, Database Counter, Database Query, DB2 8.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>
Important Information	<p>You can set additional database options that affect all resources that connect to the database in the JDBC Global Options in the General Preferences container.</p>
Useful Links	<p>“JDBC Global Options” on page 255</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Use Connection Pool	<p>If this check box is checked, SQL connection sharing is enabled. This means that you use a connection pool rather than open and close a new connection for each monitor query.</p> <p>This option is checked by default.</p>
Physically Close if idle connection count exceeds	<p>This is the maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool.</p> <p>Default value: 10</p>

GUI Element	Description
Idle Connection Timeout	<p>The maximum amount of time, in seconds/minutes/hours/days, that a SQL connection remains unused after it has been returned to the SQL connection pool. When the time is exceeded, the connection is automatically closed.</p> <p>Default value: 5 minutes</p>
Query Timeout	<p>The amount of time, in seconds/minutes/hours/days, to wait for execution of a SQL statement. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored.</p> <p>Default value: 1 minute</p>

LDAP Monitor Settings

Description	<p>Verifies that a Lightweight Directory Access Protocol (LDAP) server is working correctly by connecting to it and performing a simple authentication. Optionally, it can check the result for expected content.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"LDAP Monitor Overview" on page 738

The LDAP Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
LDAP Service Provider	Type the constant that holds the name of the environment property for specifying configuration information for the service provider to use. The value of the property should contain a URL string (for example, <code>ldap://somehost:389</code>). This property may be specified in the environment, an applet parameter, a system property, or a resource file. If it is not specified in any of these sources, the default configuration is determined by the service provider.
Security Principal	Type the constant that holds the name of the environment property for specifying the identity of the principal for authenticating the caller to the service. The format of the principal depends on the authentication scheme. If this property is unspecified, the behavior is determined by the service provider. This should be of the form <code>uid=testuser,ou=TEST,o=mydomain.com</code> .
Security Credential	Type the constant that holds the name of the environment property for specifying the credentials of the principal for authenticating the caller to the service. The value of the property depends on the authentication scheme. For example, it could be a hashed password, clear-text password, key, certificate, and so on. If this property is unspecified, the behavior is determined by the service provider.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Content Match	<p>Type a string of text to check for in the query result. If the text is not contained in the result, the monitor displays no match on content. The search is case sensitive. This works for XML tags as well.</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p>Example: <code>/href=Doc\d+\.\html/</code> or <code>/href=doc\d+\.\html/i</code></p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression.</p> <p>Example: <code>/Temperature: (\d+)</code>. This would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</p>

GUI Element	Description
Object Query	<p>Use this box to type an object query to look at a LDAP object other than the default user dn object. For example, type the mail object to check for an e-mail address associated with the dn object entered above. You must type a valid object query in this text box if you are using a LDAP filter (see the description below).</p> <p>Note: To use LDAP version 3 for a particular monitor, type [LDAP-3] before the query. If you want to use version 2 and version 3, type [LDAP-ANY].</p>
LDAP Filter	<p>Type an LDAP filter in this text box to perform a search using a filter criteria.</p> <p>The LDAP filter syntax is a logical expression in prefix notation meaning that logical operator appears before its arguments. For example, the item <code>sn=Freddie</code> means that the <code>sn</code> attribute must exist with the attribute value equal to <code>Freddie</code>.</p> <p>Multiple items can be included in the filter string by enclosing them in parentheses (such as <code>sn=Freddie</code>) and combined using logical operators such as the <code>&</code> (the ampersand conjunction operator) to create logical expressions.</p> <p>Example: The filter syntax <code>(& (sn=Freddie) (mail=*))</code> requests LDAP entries that have both a <code>sn</code> attribute of <code>Freddie</code> and a <code>mail</code> attribute.</p> <p>More information about LDAP filter syntax can be found at http://www.ietf.org/rfc/rfc2254.txt and also at http://java.sun.com/products/jndi/tutorial/basics/directory/filter.html.</p>

 **Microsoft SQL Server Monitor Settings**

Description	<p>The Microsoft SQL Server Monitor allows you to monitor the availability and performance of a Microsoft SQL Server (versions 6.5, 7.1, 2000, 2005) on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more SQL Server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Microsoft SQL Server Monitor Overview" on page 739

The Add/Edit Microsoft SQL Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the Microsoft SQL Server you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to type a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.
Counters	The server performance counters you want to check with this monitor. All non-default instances are dynamically loaded and displayed in the drop-down box. Use the Get Counters button to select counters.

GUI Element	Description
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.
SQL Instance Name	Select the Microsoft SQL server instance you want to monitor from the list of SQL instances running on the selected server. Default value: SQLServer (this value is displayed even if SiteScope is unable to get the instance list).

Oracle Database Monitor Settings

Description	<p>The Oracle Database Monitor allows you to monitor the availability of an Oracle database server (versions 9i plus some earlier versions). The error and warning thresholds for the monitor can be set on one or more Oracle server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ► In the monitor tree, right-click a group and select Add Monitor. <p>In the Contents tab for the group, click Add Monitor.</p>
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Oracle Database Monitor Overview" on page 740

The Oracle Database Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Database Connection URL	Type the connection URL to the database you want to connect to. The syntax is <code>jdbc:oracle:thin:@<server name or IP address>:<database server port>:<sid></code> . Example: To connect to the ORCL database on a machine using port 1521, use: <code>jdbc:oracle:thin:@206.168.191.19:1521:ORCL</code> . Note: The colon (:) and @ symbols must be included as shown.
Database Driver	Type the driver used to connect to the database. Example: <code>oracle.jdbc.driver.OracleDriver</code>
Database User Name	Type the user name that SiteScope should use to connect to the database. The specified user must be granted the permissions of a DBA.
Database Password	Type the password for the user name that SiteScope should use to connect to the database.
Credentials	Select a credential profile from the drop-down list to have SiteScope automatically supply the database user name and password. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243. Note: If you select or type a credential profile, you do not need to type a database user name and password. A credential profile takes priority over database user name and password entries.

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
DB Machine Name	Type the name of the target database server.

Database Connection Settings

Description	<p>The Database Connection Settings enable you to retrieve, share, and reuse database connections for database monitors that use any JDBC-compliant driver. When multiple database monitors use the same database, using a connection pool instead of an open connection for each monitor improves monitor performance and optimizes database server resource utilization.</p> <p>Connections can be shared regardless of monitor type. For example, SiteScope database logger, database tools (Database Connection, Database Information), database alerts, and database monitors (Oracle database, Database Counter, Database Query, DB2 8.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>
Important Information	You can set additional database options that affect all resources that connect to the database in the JDBC Global Options in the General Preferences container.
Useful Links	“JDBC Global Options” on page 255

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Use Connection Pool	<p>If this check box is checked, SQL connection sharing is enabled. This means that you use a connection pool rather than open and close a new connection for each monitor query.</p> <p>This option is checked by default.</p>
Physically Close if idle connection count exceeds	<p>This is the maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool.</p> <p>Default value: 10</p>
Idle Connection Timeout	<p>The maximum amount of time, in seconds/minutes/hours/days, that a SQL connection remains unused after it has been returned to the SQL connection pool. When the time is exceeded, the connection is automatically closed.</p> <p>Default value: 5 minutes</p>
Query Timeout	<p>The amount of time, in seconds/minutes/hours/days, to wait for execution of a SQL statement. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored.</p> <p>Default value: 1 minute</p>

Sybase Monitor Settings

Description	<p>The Sybase Monitor allows you to monitor the availability and performance statistics of a Sybase Server. The error and warning thresholds for the monitor can be set on one or more Sybase server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Sybase Monitor Overview" on page 742

The Add/Edit Sybase Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Choose the server where the Sybase server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.
User Name	Type the user name to access the Sybase database.
Password	Type the password of the user name to access the Sybase database.

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

17

Generic Monitors

This chapter includes the main concepts and reference information for monitoring various type of environment. These monitors can monitor networks, applications, and databases depending on how they are configured.

This chapter includes:

Concepts

- ▶ Composite Monitor Overview on page 774
- ▶ Directory Monitor Overview on page 774
- ▶ File Monitor Overview on page 775
- ▶ JMX Monitor Overview on page 776
- ▶ Log File Monitor Overview on page 779
- ▶ Script Monitor Overview on page 781
- ▶ Web Service Monitor Overview on page 787
- ▶ XML Metrics Monitor Overview on page 791

Reference

- ▶ Generic Monitors User Interface on page 792

Composite Monitor Overview

Each time the Composite Monitor runs, it returns a status based on the number and percentage of items in the specified monitors and/or groups currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

Use this monitor if you want to create complex monitor alert logic. For example, if you want to trigger an alert when:

- ▶ Five or more monitors in a group of eight are in error
- ▶ Three or more groups have monitors with errors in them
- ▶ You have two monitors, and exactly one is in error

then you could create a Composite Monitor that went into error on these conditions, and then add alerts on the Composite Monitor to take the desired actions.

If you need alert logic that is more complex than SiteScope's standard alerts allow, you can use the Composite Monitor to create a customized alert behavior.

For details on configuring this monitor, see “Composite Monitor Settings” on page 793.

Directory Monitor Overview

Use the Directory Monitor to monitor directories that contain log files or other files that tend to grow and multiply unpredictably. You can instruct SiteScope to notify you if either the number of files or total disk space used gets out of hand. You can also use this to monitor directories in which new files are added and deleted frequently. For example, in the case of an FTP directory, you probably want to watch both the number of files in the directory and the files contained in the directory.

You can set up thresholds for this monitor based on the time in minutes since the latest time a file in the directory has been modified, as well as the time in minutes since the first time a file in the directory has been modified.

Because the uses for the Directory Monitor vary so greatly, there is no one interval that works best. Keep in mind that if you are watching a directory that contains a lot of files and sub directories, this monitor may take longer to run.

For details on configuring this monitor, see “Directory Monitor Settings” on page 795.

File Monitor Overview

The File Monitor is useful for watching files that can grow too large and use up disk space, such as log files. Other files that you may want to watch are Web pages that have important content that does not change often.

You can set up your File Monitors to monitor file size, age, or content, and set a threshold at which you should be notified. SiteScope can alert you to unauthorized content changes so that you can correct them immediately. You can write scripts for SiteScope to run that automatically roll log files when they reach a certain size.

Reading and Status

Each time the File Monitor runs, it returns a reading and a status and writes them in the monitoring log file. It also writes the file size and age into the log file.

The reading is the current value of the monitor. Possible values are:

- OK
- content match error
- file not found
- contents changed

An error status is returned if the current value of the monitor is anything other than OK.

For details on configuring this monitor, see “File Monitor Settings” on page 797.

JMX Monitor Overview

Use the JMX Monitor to monitor performance statistics of Java-based applications that provide access to their statistics by using the standard JMX remoting technology defined by JSR 160.

You can monitor multiple parameters or counters with a single monitor instance. The counters available vary from application to application, but normally include both basic JVM performance counters as well as counters specific to the application. You may create one JMX Monitor instance for each application you are monitoring, or several monitors for the same application that analyze different counters.

Note: WebLogic 9.x and 10.x servers can only be monitored using a JMX monitor. For details on how to monitor a WebLogic 9.x or 10.x server, see “Creating a JMX Monitor for a WebLogic 9.x or 10.x Server” on page 778.

Applications Supporting JSR 160

Here are some applications that currently support JSR 160 and information about how to monitor them:

- ▶ BEA WebLogic 9.x and 10.x supports JSR 160, which can be enabled on the WebLogic application server by following instructions found on the BEA Web site (<http://e-docs.bea.com/wls/docs90/ConsoleHelp/taskhelp/channels/EnableAndConfigureIOP.html>).

Once enabled, the JMX URL for monitoring the server follows the following form:

```
service:jmx:rmi:///jndi/iiop://<localhost>:7001/weblogic.management.mbeanservers.runtime
```

where the <localhost> is the server name or IP address that is running your WebLogic application.

For instructions to create a JMX monitor for WebLogic 9.x and 10.x servers, see “Creating a JMX Monitor for a WebLogic 9.x or 10.x Server” on page 778.

- ▶ Tomcat 5.x supports JSR 160, by defining the following properties to the JVM on startup:
 - ▶ `Dcom.sun.management.jmxremote`
 - ▶ `Dcom.sun.management.jmxremote.port=9999`
 - ▶ `Dcom.sun.management.jmxremote.ssl=false`
 - ▶ `Dcom.sun.management.jmxremote.authenticate=false`

The above properties specify the port as 9999. This value can be changed to any available port. Also, it specifies no authentication. If authentication is necessary, see the Java Sun Web site for more details (<http://java.sun.com/j2se/1.5.0/docs/guide/jmx/tutorial/security.html>). If the above properties are defined when starting Tomcat 5.x on `<localhost>`, the following would be the JMX URL for monitoring it:

```
service:jmx:rmi:///jndi/rmi://<localhost>:9999/jmxrmi
```

Note: SiteScope 8.x runs within Tomcat 5.x, and can be monitored as described above.

- ▶ Other vendors that have released versions of their software that are JSR 160 compliant, include JBoss, Oracle 10g, and IBM WebSphere.

You can find more information about JSR 160 on the Java Community Process Web site (<http://www.jcp.org/en/jsr/detail?id=160>).

Creating a JMX Monitor for a WebLogic 9.x or 10.x Server


WebLogic 9.x and 10.x servers cannot be monitored using a WebLogic monitor. To monitor a WebLogic 9.x or 10.x server, create a JMX monitor, and type the following in the **JMX URL** box:

```
service:jmx:rmi:///jndi/iiop://localhost:7001/weblogic.management.mbeanservers.runtime.
```

To help you to select the counters that you require, you can open a WebLogic monitor for versions prior to WebLogic 9.x (WebLogic 6.x, 7.x, and 8.x) and see the counters that were defined there. Search for these same counters in the counter tree. You can select additional counters that are available in the JMX monitor and were not available in the WebLogic monitors.

Troubleshooting the JMX Monitor

When using the JMX monitor to monitor performance statistics on a JBoss server, the **Good** status is displayed in the SiteScope Dashboard even when the JBoss server is unavailable. SiteScope handles the exceptions differently according to the platform.

- ▶ On Windows, each counter is set to **n/a**.
- ▶ On Linux and Solaris platforms, the counters are not reset, but the **no data** value is set (and **No Data Availability**  is displayed on the Dashboard).

A workaround when monitoring JBoss is to change the monitor's properties in Threshold Settings, by setting **If Unavailable** to **Set monitor status to error**.

For details on configuring this monitor, see “JMX Monitor Settings” on page 801.

Log File Monitor Overview

The Log File Monitor watches for specific entries added to a log file by looking for entries containing a text phrase or a regular expression. You can use it to automatically scan log files for error information. With SiteScope doing this for you at set intervals, you can eliminate the need to scan the logs manually. In addition, you can be notified of warning conditions that you may have otherwise been unaware of until something more serious happened.

By default, each time that SiteScope runs this monitor, it starts from the point in the file where it stopped reading last time it ran. This insures that you are notified only of new entries and speeds the rate at which the monitor runs. You change this default behavior using the **Check from Beginning** property. For details, see “Check from Beginning” on page 805.

Note: Monitoring log files using SSH on Windows platforms is supported from SiteScope version 8.5 and later.

Scheduling This Monitor

You can schedule your Log File Monitors to run as often as every 15 seconds. However, depending on the size of the log file, the total number of monitors you have running, and **Check from Beginning** option selected, the monitor may take 15 seconds or longer to check the file for the desired entries. The default update schedule of every 10 minutes is a reasonable frequency in most cases.

Customizing Log File Content Matches and Monitor Alerts

You can create a Log File monitor that triggers customized alerts for content matches according to the threshold status of the monitor.

To configure the Log File monitor with custom matches and alerts:

- 1** In the Main Settings, select the **for each log entry matched** option from the **Run Alerts** box.
- 2** In the Main Settings, type the text to look for in the log entries in **Content Match**. For example, to find text entries `redflag` and `disaster` in the log file, type `/(redflag|disaster)/`.
- 3** In the Advanced Settings, type a label name in the **Match Value Labels** box for the matched values found in the target log file. For example, type `matchedValue`.
- 4** In the Threshold Settings, set the error and warning threshold. For example, set `Error if matchedValue == disaster` and set `Warning if matchedValue == redflag`.
- 5** Configure error, warning, and good alerts for the Log File monitor. The alert that is sent depends on the threshold that is met for each entry matched. For example, if the error threshold is met, the error alert is triggered. For details on configuring alerts, see “Configure an Alert” on page 1409.

For details on configuring this monitor, see “Log File Monitor Settings” on page 802.

Script Monitor Overview

The Script Monitor can be used to run shell commands or other scripts on the machine where SiteScope is running or it can run a script that is stored on a remote machine.

One of the primary reasons for using the Script Monitor is to integrate into SiteScope an existing script that you use to do a particular system management function. For example, if you have a script that runs a diagnostic on an application and returns a 0 reading if everything is working, you could create a Script monitor that runs this script and recognizes any exit value other than 0 as an error. Then you could create an alert which would e-mail or page you in the event that this monitor was in error.

Script Options

The following is an overview of the possible script execution options and requirements for the SiteScope Script Monitor:

Script Option	Description
Local Script	A file stored and run on the SiteScope machine. The file should be stored in the <SiteScope root directory>\scripts directory.
Remote Script	<p>A remote script file (UNIX and Windows-SSH only) in a scripts subdirectory in the home directory of the account SiteScope uses to access the remote server. For example, <code>home/sitescope/scripts</code>.</p> <p>The remote scripts must include an echo construct to echo script results and exit codes back to SiteScope (see the Return Status Example section below).</p> <p>The monitor may fail if the required exit code is not echoed back to SiteScope.</p> <p>When running a script on a remote Windows server using SSH, you must include an "end script" string at the end of the script to avoid a timeout error. For example:</p> <pre>@echo off time echo end script</pre>
Remote Command	A script file containing a single command stored locally in the <SiteScope root directory>\scripts.remote directory. This script file is used to run a command on a remote server. The command may be used to run a remote script file that performs multiple functions.

Note: For SiteScope on Linux, the script itself must have a shell invocation line as the very first line of the script. This applies to scripts that you are trying to run locally on the SiteScope machine. For example, the first line of the script should include something like `#!/bin/sh` or `#!/usr/local/bin/perl`. If the shell invocation line is not found then the `exec()` call returns with a -1 exit status. This is a limitation of the Java Runtime in JRE prior to release 1.4. This has been fixed in the 1.4 JRE from Sun which is shipped with SiteScope version 7.8 and later.

Scheduling Script monitors is dependent on the script that you want SiteScope to run. You can use the scheduling option to have SiteScope run scripts at different intervals throughout the week.

Status

Each time the Script Monitor runs, it returns a status and writes it into the monitoring log file. It also reports a command result, a value, and the time it took to run the command.

The command result is the exit value returned by running the command. This works for local UNIX scripts, but does not work for remote UNIX scripts, or Win NT batch files. Win NT batch file (*.bat) exit codes are not passed out of the command interpreter, and remote UNIX script exit codes are not passed back through the remote connection. See the example below for a way to receive information from the script.

Caching Script Output

The Script Monitor includes an optional function that can be used to cache the output of a script execution. The cached output is useful in you want to:

- ▶ Have multiple script monitors check and alert on different parts of the output of a script
- ▶ Reduce network traffic and server load by minimizing the number of times a script is run

You can enable script output caching by entering a time value (in seconds) greater than zero in the **Cache Life** setting in the Advanced Settings section. To configure multiple Script monitors to use the data in the cache you must ensure that each monitor instance:

- ▶ Is configured to use the same remote Server profile.
- ▶ Is configured to use the same Script file.
- ▶ Has a **Cache Life** value greater than zero.

The **Cache Life** value entered for each monitor should approach, but not exceed, the equivalent of the value selected for the **Frequency** setting for that monitor. For example, if the **Frequency** setting is 10 minutes, the **Cache Life** value can be set to a value of 590 because 10 minutes is equivalent to 600 seconds and 590 is less than 600. Any monitor that detects the end of its Cache Life runs the script again and refreshes the cache.

Setting a Timeout Value for Script Execution

You can set a timeout value for the Script Monitor for SiteScope running on Windows. The timeout value is the total time, in seconds, that SiteScope should wait for a successful run of the script. You can use this option to have SiteScope run the monitor but kill the script execution if a script exit code is not detected within the timeout period.

The requirements and limitations of this option are:

- It is only available with SiteScope for Windows.
- It can only be used with scripts stored and run on the local SiteScope server (that is, where the **Server** setting for the Script Monitor is this server or localhost).
- The timeout setting value is expressed in seconds.
- It only applies to Script Monitors.

Two methods exist for applying a timeout setting to Script monitors. One applies the setting as a property to an individual monitor. The second method adds the setting to groups, subgroups, or the entire SiteScope installation. The procedures for both are described below.

To set a Timeout Value for individual script monitor instances:

- 1** Stop the SiteScope service.
- 2** Using a text editor, open the SiteScope group file containing the monitor frame for the Script Monitor to which you want to apply the timeout setting.
- 3** Inside the Script Monitor frame (delimited by the # sign), insert a line and add the timeout setting as `_timeout=time` where `time` is replaced with the time in seconds.
- 4** Save the group file.

Note: Do not add blank lines, leading or trailing spaces to any record in the group file.

- 5** Restart the SiteScope service.

To set a Timeout Value for multiple script monitor instances:

- 1** Stop the SiteScope service.
- 2** Using a text editor, open the SiteScope group file containing one or more Script monitors to which you want to apply the timeout setting. Alternately, you can add the setting to the `SiteScope/groups/master.config` file.
- 3** Inside the group file frame at the top of the file before the first # symbol, insert a line and add the timeout setting as `_scriptMonitorTimeout=time` where `time` is replaced with the time in seconds.
- 4** Save the group file.

Note: Do not add blank lines, leading or trailing spaces to any record in the group file or `master.config` file.

- 5** Restart the SiteScope service.

Running Different Types of Scripts

In previous versions of SiteScope, it was not possible to run non-batch scripts, for example VBScript or Perl scripts, without wrapping them into a batch file. In SiteScope 9.50, you can do the following:

- ▶ You can see scripts with any extensions that you specify in the `_scriptExtensions` property of the **master.config** file. For example, to see **.pl**, **.py**, or **.php** scripts, use the following format:
`_scriptMonitorExtensions=.pl;.py;.php`
- ▶ You can run script interpreters with script extensions by specifying the `_scriptInterpreters` property of the **master.config** file as follows:
`_scriptInterpreters=pl=c:/perl/perl.exe;py=c:/python/python.exe;php=c:/php/php.exe`

For details on configuring this monitor, see “Script Monitor Settings” on page 808.

Web Service Monitor Overview

Use the Web Service Monitor to check the availability of a Web service accepting Simple Object Access Protocol (SOAP) requests. The Web Service Monitor checks that the service can send a response to the client in certain amount of time and to verify that the SOAP response is correct based on your selected match specifications.

The Simple Object Access Protocol is a way for a program running under one operating system to communicate with another program running under the same or different operating system (such as a Windows 2000 program talking to a Linux based program) The Simple Object Access Protocol uses the Hypertext Transfer Protocol (HTTP) and Extensible Markup Language (XML) for information exchange with services in a distributed environment.

This monitor uses a Web Services Description Language (WSDL) file to extract technical interface details about a Web service and uses information returned to create an actual SOAP request to that Web service. That is this monitor emulates a real Web service client making a request. The SOAP request can be used to confirm that the Web service is serving the expected response data and in a timely manner. The status of the Web Service Monitor is set based on the results of the SOAP request.

For information about SOAP, refer to the W3C Web site (<http://www.w3.org/TR/SOAP/>).

For information about WSDL, refer to the Microsoft site (<http://msdn2.microsoft.com/en-us/library/ms996486.aspx>).

Supported Technologies

The following specification features are currently supported:

- WSDL 1.2
- SOAP 1.1
- Simple and Complex Types based on XML Schema 2001
- SOAP binding with the HTTP(S) protocol only
- SOAP with Attachments is not supported
- Nested WSDL
- WSDL with multi-ports and multi-services

Note: The monitor does not support SOAP 1.2.

Important: SOAP and WSDL technologies are evolving. As a result, some WSDL documents may not parse accurately and some SOAP requests may not interact with all Web service providers. When SiteScope is unable to generate the correct skeleton code, for example, if the WSDL file has errors or the complexType element uses schema syntax that is not supported, you can modify the XML argument as necessary. For example, if an argument is displayed like this:

```
parameters[COMPLEX] =<pPatientSSN xsi:type="xs:string">***</pPatientSSN>
```

you can modify it by deleting the **xs:** and **xsi:** as follows:

```
parameters[COMPLEX] =<pPatientSSN type="string">***</pPatientSSN>
```

Status

The status reading shows the most recent result for the monitor. It is also recorded in the SiteScope log files, e-mail alert messages, and can be transmitted as a pager alert. The possible status values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- document moved
- unauthorized
- forbidden
- not found
- proxy authentication required
- server error
- not implemented
- server busy

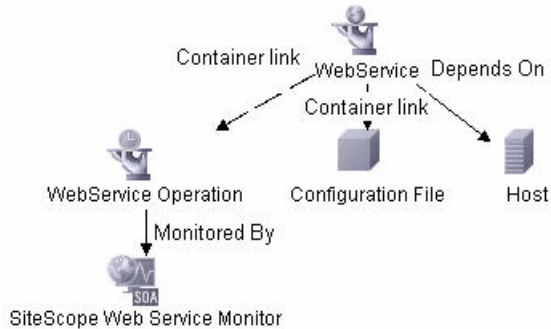
The final status result is either OK, error, or warning based on the threshold established for these conditions.

Integration with HP Business Availability Center for SOA

If SiteScope is reporting to HP Business Availability Center, the monitor sends SOA samples, in addition to the regular samples it sends, for use in HP Business Availability Center for SOA. If the **HP BAC Logging** setting is set to **Do not report to HP Business Availability Center**, the monitor does not send any samples to HP Business Availability Center.

Web Service Topology Settings

The Web Service monitor can identify the topology of the Web Service being monitored. If **Report SOA Topology to HP Business Availability Center** is selected in the Topology Settings (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



The CIs are created only for the monitored entities according to the counters that you select.

Note:

- ▶ This direct integration between SiteScope and Business Availability Center is available only when the Business Availability Center for SOA license is installed.
 - ▶ The SiteScope Web Service Monitor CI replaces the legacy SiteScope Monitor CI for the Web Service monitor instances when upgrading from previous versions of SiteScope to SiteScope 9.50. The SiteScope Monitor CI is removed from CMDB, which causes it to be removed from instance views that included it or from SLAs to which it was attached.
-

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 50.

For information about the SOA topology, see “SOA Views and Reports” in *Solutions and Integrations*.

For details on configuring this monitor, see “Web Service Monitor Settings” on page 814.

XML Metrics Monitor Overview

Use the XML Metrics Monitor to monitor metrics for systems that make performance data available in the form of an XML file or page. The XML Metrics Monitor gathers information from a source, organizes it into a browsable tree structure, and allows you to choose which items in the tree should be monitored. It works by requesting an XML file that is accessible by an URL. When the monitor runs, the XML metrics file is parsed to extract values for each of the counters selected during setup.

The XML metrics must be in a format where each metric is a separate, unique entity in the tree/leaf format. An optional XSL facility can help with formatting.

XML Requirements

A monitor instance must be defined and run against the same XML metrics file format. That is, when running this monitor, SiteScope expects the XML file it is monitoring to have the same format that was used when defining that monitor.

SiteScope parses the input XML content according to the following assumptions:

- ▶ The XML content has only one root node. This means that all of the XML content is encapsulated within a single parent element and not multiple instances of a repeating root element.
- ▶ A leaf node, an element containing only character data and no child elements, is considered a counter and must be of the form:

```
<node_tag>node_value</node_tag>
```

where `<node_tag>` becomes the counter name, and `<node_value>` is reported as the counter value.

- ▶ Each leaf node (and therefore each counter) must have a unique path within the hierarchy of the XML content.
- ▶ The XML metric file should contain at least one leaf node.

If your XML metric file does not conform to these rules, you can specify an XSLT (eXtensible Stylesheet Language: Transformations) file that transforms your XML file into a file that does conform. Such a file usually has a file extension of .xsl.

If you need to develop a XSLT file to transform the XML content for this monitor, SiteScope includes a Tools page you can use to verify the transformation output. For more information, see the section “XSL Transform Tool” on page 1634.

For details on configuring this monitor, see “XML Metrics Monitor Settings” on page 819.

Generic Monitors User Interface

This section describes:

- ▶ Composite Monitor Settings on page 793
- ▶ Directory Monitor Settings on page 795
- ▶ File Monitor Settings on page 797
- ▶ JMX Monitor Settings on page 801
- ▶ Log File Monitor Settings on page 802
- ▶ Script Monitor Settings on page 808
- ▶ Web Service Monitor Settings on page 814
- ▶ XML Metrics Monitor Settings on page 819

Composite Monitor Settings

Description	<p>Designed to simplify the monitoring of complex network environments by checking the status readings of a set of other SiteScope monitors and/or monitor groups.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Composite Monitor Overview" on page 774

The Add/Edit ColdFusion Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Items	Choose one or more monitors (using CONTROL-CLICK) and/or groups that you want in the Composite Monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Monitor Delay	<p>If Run Monitors is checked, this is the number of seconds to wait between running each monitor.</p> <p>This setting is useful if you need to wait for processing to occur on your systems before running the next monitor.</p>
Run Monitors	<p>Select if you want the Composite Monitor to control the scheduling of the selected monitors, as opposed to just checking their status readings.</p> <p>Monitors that are to be run this way should not also be run separately, so edit the individual monitors, set the Update Every box for that monitor to zero ("0"), and save the changes. Those monitors then run only when scheduled by the Composite Monitor. This is useful if you want the monitors to run one after another or run at approximately the same time.</p>
Check All Monitors in Groups	<p>When selected, all of the monitors in selected groups (and their subgroups) are checked and counted.</p> <p>Default value: A group is checked and counted as a single item when checking status readings.</p>

Directory Monitor Settings

Description	<p>The Directory Monitor watches an entire directory and reports on the total number of files in the directory, the total amount of disk space used, and the time (in minutes) since any file in the directory was modified. This information is useful if you have limited disk space, you want to monitor the number of files written to a specific directory, or you want to know the activity level in a certain directory.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Directory Monitor Overview" on page 774

The Add/Edit Directory Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	<p>Select the server name where the file is located. The list of servers includes the remote UNIX or NT servers that have been specified to SiteScope.</p> <p>Note: Monitoring log files using SSH on Windows platforms is supported for this monitor only if the remote SSH server supports SSH File Transfer Protocol.</p>

GUI Element	Description
Directory Path	<p>Type the directory that you want to monitor.</p> <ul style="list-style-type: none"> ▶ To monitor directories on a remote Windows NT/2000 server through NetBIOS, the path should contain the name of the shared folder for remote NetBIOS servers. You can also specify an absolute path of the directory on the remote machine without specifying the server name. For example, if you type <code>c:\test</code>, the remote directory is accessed as <code>\\Server\C\$\test</code>. ▶ To monitor a directory on a remote Windows SSH machine, the path must be relative to the home directory of the user account used to log in to the remote machine. ▶ To monitor a directory on remote UNIX machines, the path must be relative to the home directory of the UNIX user account used to log in to the remote machine. You must also select the corresponding remote UNIX server in the Servers box described above. For details on which UNIX user account to use for the applicable remote server, see “UNIX Remote Preferences” on page 220. <p>To monitor a directory that is created automatically by some application and the directory path includes date or time information, you can use SiteScope's special data and time substitution variables in the path of the directory. For details, see “SiteScope Date Variables” on page 1506.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
No Subdirectories	Select this box if you do not want SiteScope to count subdirectories.
File Name Match	Type text or an expression to match against (optional). Only file names which match are counted in the totals.

File Monitor Settings

Description	<ul style="list-style-type: none"> ➤ Reads a specified file. ➤ Checks the size and age of a file. ➤ Helps you verify the contents of files by: <ul style="list-style-type: none"> ➤ Matching the contents for a piece of text, or by, ➤ Checking to see if the contents of the file have changed. <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ➤ In the monitor tree, right-click a group and select Add Monitor. ➤ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"File Monitor Overview" on page 775

The Add/Edit File Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	<p>Select the server name where the file is located. This monitor supports UNIX remotes and the local SiteScope machine only. Windows machines (including SSH on Windows) are not supported for this monitors.</p>
File Name	<p>Type the path and name to the file you want to monitor. For reading files on remote UNIX machines, the path must be relative to the home directory of the UNIX user account being used to login to the remote machine.</p> <p>Example: It may be necessary to provide the full path to the target file, such as <code>/opt/application/logs/user.log</code>.</p> <p>You must also select the corresponding remote UNIX server in the Servers box described above. For details on which UNIX user account to use for the applicable remote server, see “UNIX Remote Preferences” on page 220.</p> <p>For reading files on remote Windows NT/2000 servers, you use NetBIOS to specify the server and UNC path to the remote log file.</p> <p>Example: <code>\\remoteserver\sharedfolder\filename.log</code>.</p> <p>You can also monitor files local to the server where SiteScope is running.</p> <p>Example: <code>C:\application\appLogs\access.log</code>.</p> <p>Optionally, you can use regular expressions for special date and time variables to match on log file names that include date and time information.</p> <p>Example: You can use a syntax of <code>s/ex\$shortYear\$\$0month\$\$0day\$.log/</code> to match a current date-coded file. For details on using regular expressions and dates, see “SiteScope Date Variables” on page 1506.</p>

GUI Element	Description
File Encoding	<p>If the file content to be monitored uses an encoding that is different than the encoding used on server where SiteScope is running, type the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the target file. This enables SiteScope to match and display the encoded file content correctly.</p> <p>Examples: Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Match Content	<p>Type a string of text to check for in the returned page. If the text is not contained in the page, the monitor displays no match on content. The search is case sensitive. HTML tags are part of a text document, so include them if they are part of the text you are searching for. This works for XML pages as well.</p> <p>Example: Hello World</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p>Example: /href=Doc\d+\.html/ or /href=doc\d+\.html/i</p> <p>To save and display a particular piece of text as part of the status, use parentheses in a Perl regular expression.</p> <p>Example: /Temperature: (d+). This returns the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</p> <p>For details, see “Using Regular Expressions” on page 1493. You can also use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 1618.</p>

GUI Element	Description
Check for Content Changes	<p>Unless this is set to "no content checking" (the default) SiteScope records a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs. If the checksum changes, the monitor has a status of "content changed error" and goes into error. If you want to check for content changes, you should use "compare to saved contents".</p> <p>The options for this setting are:</p> <ul style="list-style-type: none"> ➤ no content checking (default). SiteScope does not check for content changes. ➤ compare to last contents. The new checksum is recorded as the default after the initial content changed error occurs, so the monitor returns to OK until the checksum changes again. ➤ compare to saved contents. The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor gets a content changed error and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents. ➤ reset saved contents. Takes a new snapshot of the page and saves the resulting checksum on the first monitor run after this option is chosen. After taking the snapshot, the monitor reverts to compare to saved contents mode.
No Error if File Found	<p>Check this if you want this monitor to remain in GOOD status, if the file is not found. The monitor status is GOOD regardless of how the monitor's thresholds have been configured.</p>

JMX Monitor Settings

Description	<p>Allows you to monitor the performance statistics of those Java-based applications that provide access to their statistics by using the standard JMX remoting technology.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"JMX Monitor Overview" on page 776

The JMX Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
JMX URL	<p>The URL to gather JMX statistics. Typically the URL begins with <code>service:jmx:rmi:///jndi</code>, followed by information specific to the application.</p> <p>Note: When creating a JMX monitor for a WebLogic 9.x or 10.x server, type the following URL: <code>service:jmx:rmi:///jndi/iop://localhost:7001/weblogic.management.mbeanservers.runtime</code></p>
Domain Filter	Domain filter to show only those counters existing within a specific domain (optional).
User Name	User name for connection to the JMX application (optional).

GUI Element	Description
Password	Password for connection to the JMX application (optional).
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters. When the server being monitored is a WebLogic 9.x or 10.x server, see “Creating a JMX Monitor for a WebLogic 9.x or 10.x Server” on page 778 for further details.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Log File Monitor Settings

Description	<p>The Log File Monitor watches for specific entries added to a log file by looking for entries containing a text phrase or a regular expression.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“Log File Monitor Overview” on page 779

The Add/Edit Log File Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	<p>If the log file is on a UNIX or NT SSH server, select the server name where the file located. The list of servers includes the remote UNIX or NT SSH servers that have been specified to SiteScope.</p> <p>Note: From SiteScope version 8.6, Remote Windows computers that use the NetBIOS connection method do appear in the Servers list. Use the UNC format to specify the path to the remote log file.</p>

GUI Element	Description
Log File Pathname	<p>Type the path to the log file you want to monitor.</p> <ul style="list-style-type: none"> ▶ For reading log files on remote UNIX machines, the path must be relative to the home directory of the UNIX user account being used to log in to the remote machine. You must also select the corresponding remote UNIX server in the Servers box below. For information about which UNIX user account is being used for the applicable remote server, see “UNIX Remote Preferences” on page 220. ▶ For reading log files on remote Windows NT/2000 servers using the NetBIOS method, use UNC to specify the path to the remote log file. Example: \\remoteserver\sharedfolder\filename.log ▶ For reading log files on remote Windows NT/2000 servers using the SSH method, specify the local path of the remote log file on the remote machine. Example: C:\Windows\System32\filename.log <p>You must also select the corresponding remote Windows SSH server in the Servers box. For details on configuring a remote Windows server for SSH, see “Configuring Remote Windows Servers for SSH Monitoring” on page 1545.</p> <p>You can also monitor files local to the server where SiteScope is running. Example: C:\application\appLogs\access.log</p> <p>Optionally, you can use special date and time regular expression variables to match log file names that include date and time information. For example, you can use a syntax of <code>s/ex\$shortYear\$\$0month\$\$0day\$.log/</code> to match a current date-coded log file. For details on using regular expressions, refer to “SiteScope Date Variables” on page 1506.</p>

GUI Element	Description
Run Alerts	<p>Select the method for running alerts for this monitor.</p> <ul style="list-style-type: none"> ▶ If the for each log entry matched option is chosen, the monitor triggers alerts for every matching entry found according to the defined threshold status. The alert that is sent depends on the status specified by the thresholds. For example, if you have a good, warning, and error alert configured for the monitor and the warning threshold is met, the warning alert is triggered. After the monitor run, no additional alerts are triggered and monitor returns to good status. For details on how to perform this task, see “Customizing Log File Content Matches and Monitor Alerts” on page 780. ▶ If the once, after all log entries have been checked option is chosen, then the monitor counts up the number of matches and then triggers alerts. <p>Note: The status category is resolved according to the last content that matched the regular expression. If the last matched content does not meet the threshold measurement, an alert is not triggered.</p>
Check from Beginning	<p>Select the file checking option for this monitor instance. This setting controls what SiteScope looks for and how much of the target file is checked each time that the monitor is run.</p> <ul style="list-style-type: none"> ▶ Never. Checks newly added records only. ▶ First Time Only. Checks the whole file once, and then newly added records only. ▶ Always. Always checks the whole file. <p>Default value: Never</p>

GUI Element	Description
Content Match	<p>Type the text to look for in the log entries. You can also use a regular expression in this entry to match text patterns. Unlike the content match function of other SiteScope monitors, the Log File Monitor content match is run repeatedly against the most recent content of the target log file until all matches are found. This means the monitor not only reports if the match was found but also how many times the matched pattern was found. To match text that includes more than one line of text, add an <code>s</code> search modifier to the end of the regular expression. For details, see “Using Regular Expressions” on page 1493. You can also use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 1618.</p> <p>Note: If you type more than four values in this box, when you create a report by clicking the monitor title, the report includes only the first four values.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Rules File Pathname	<p>In rare cases, it may be necessary to create a custom rules file to specify the log entries to match and the alerts to send. An example rules file is located in <code><SiteScope root directory>\conf\examples\sample.rules</code>. Make a copy of this file and rename. There is no required naming convention. Open the file with the editor of your choice, and using the comments as a guideline, edit the file to meet your needs. When you are finished, type the full path to your rules file in this box.</p>
No Error if File Not Found	<p>Select if you want this monitor to remain in GOOD status if the file is not found. The monitor status remains GOOD regardless of the monitor threshold configuration.</p>

GUI Element	Description
Match Value Labels	<p>Use this option to type labels for the matched values found in the target log file. The match value labels are used as variables to access retained values from the Content Match expression for use with the monitor threshold settings. Separate multiple labels with a comma (,). The labels are used to represent any retained values from the Content Match regular expression in the parameters available for the status threshold settings (Error if, Warning if, and Good if). These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.</p> <p>Note: If you type more than four values in this box, when you create a report by clicking the monitor title, the report includes only the first four values.</p>
Log File Encoding	<p>If the log file content to be monitored uses an encoding that is different than the encoding used on server where SiteScope is running, type the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the target log file. This enables SiteScope to match and display the encoded log file content correctly.</p> <p>Examples: Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.</p>
Multi Line Match	<p>Enables you to run a regular expression match on multiple lines of text.</p>

Script Monitor Settings

Description	<p>The Script Monitor runs an external command and reports the result. It is one way to integrate existing system management scripts into the SiteScope environment. The Script Monitor can be tailored to run scripts at regular intervals. In addition to reporting the command result, the Script Monitor can also parse and report a specific value from the command output.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Script Monitor Overview" on page 781

The Add/Edit Script Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	<p>You can have SiteScope run a script that is stored on a remote machine by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. These are the remote servers that are available to SiteScope. <p>Note: Only UNIX servers and Windows remote servers that use an SSH connection are listed. The Script monitor cannot use Windows remotes that do not use an SSH connection.</p> ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in the Remote UNIX Preferences page, type the IP address or name of the server to monitor. <p>Default value: SiteScope runs script files that are stored locally on the SiteScope machine in the <code><SiteScope root_directory>\scripts</code> directory.</p>

GUI Element	Description
Script	<p>Type the name of the script to run. For security reasons, only scripts placed into the <SiteScope root directory>\scripts directory may be used. In that directory, there are several examples scripts with comments describing each one.</p> <p>If you choose USE COMMAND, you must also specify a USE COMMAND script file name in the Advanced Settings section below. SiteScope sends the command or commands found in the USE COMMAND script file to be run as a command line on the remote UNIX Machine. Script files for the USE COMMAND option must be created in the <SiteScope root directory>\scripts.remote directory.</p> <p>Example: Create a file named test.sh and save it in the <SiteScope root directory>\scripts.remote directory. Edit test.sh to include the command syntax <code>ps -ef;echo "all done"</code> as the content of the file. Then create a Script monitor with the USE COMMAND option selected, select a remote UNIX machine, and select test.sh as the USE COMMAND script to run.</p> <p>Note: The diskSpace.bat script only accepts two required parameters: host name and physical drive name. Because the connection to the remote host is made using the current SiteScope account, you can only use this script if SiteScope can access this account. If the specified account does not have the privileges to access the remote host, it is recommended that you use the Disk Space monitor instead.</p>

GUI Element	Description
Parameters	<p>Use this text box to specify any additional parameters to pass to the script.</p> <p>Optionally, you can use a regular expression or one of SiteScope's date variables to insert date and time into the parameters box.</p> <p>Example: s/\$month\$ \$day\$ \$year\$/ passes the current month, day and year to the script.</p> <p>Syntax exceptions:: For security reasons, the following characters are not allowed to be passed to scripts by SiteScope:</p> <p>` (apostrophe), ; (semicolon), & (ampersand), (vertical pipe), < (less than), > (greater than).</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Match Value Labels	Type labels for the matched values found in the script output. Separate multiple labels with a comma (,).
Remote Script Command File	<p>If you have selected the USE COMMAND as the Script option above and a remote machine as the Server, select the script file that contains the commands that SiteScope should send to the remote machine. You can save one or more commands in the text script file and save the file in the <SiteScope root directory>\ scripts.remote directory. SiteScope opens this file and runs the command at the command line of the remote server chosen in the Choose Server option above. You can then use the Match Expression option to parse the output of the command and display valuable information.</p> <p>The USE COMMAND script can make use of positional parameters such as \$1, \$2 (or alternatively %1, %2), and so on, inside the script. Type the parameters you want SiteScope to pass to the script in the Parameters box provided above.</p> <p>You can use one or more commands per USE COMMAND script file.</p> <p>Field Exception: Do not include any carriage returns or any command that would normally discontinue script processing (for example, do not use the <code>exit</code> command).</p>

GUI Element	Description
Cache Life	<p>You use this option only if you want to use multiple Script monitor instances to check or match on content returned by a single run of a script.</p> <ul style="list-style-type: none"> ▶ Type a time value (in seconds) greater than zero to have SiteScope cache the output of the script execution. <p>Each time the monitor is run, SiteScope checks if the cache life has expired. If it has not, then the monitor uses the cached script output data, otherwise the script is run again to update the cache and the monitor.</p> <ul style="list-style-type: none"> ▶ Type a value of 0 (zero) to disable the cache function. This causes the monitor to run the script each time that it runs.
Match Expression	<p>To retrieve a value from the script output, type a regular expression in this box.</p> <p>Example: The expression: <code>/(\d+)/</code> matches one or more digits returned by the script.</p> <p>The retrieved value can be used to set the error or warning status of the monitor and to trigger alerts. SiteScope checks up to four values returned.</p> <p>Note: If this item is left blank, no value is retrieved from the script.</p>
Maximum For Measurement	<p>(Optional) Type a maximum value, in milliseconds, for creating the gauge display.</p> <p>Example: If the runtime of the script is 4 seconds, and this value is set to 8 seconds (8000 milliseconds), the gauge shows at 50%.</p> <p>Default value: 0</p>

Web Service Monitor Settings

<p>Description</p>	<p>The Web Service Monitor is used to check Simple Object Access Protocol (SOAP) enabled Web services for availability and stability. The Web Service Monitor sends a SOAP based request to the server and checks the response to verify that the service is responding.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p>Useful Links</p>	<p>"Web Service Monitor Overview" on page 787</p>

The Add/Edit Web Service Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Web Service Descriptor Language URL or WSDL File	<p>Type the URL of the WSDL file to be used for this monitor, and click the Get Data button.</p> <p>All file paths entered must be relative to the location <SiteScope root directory>\templates.wsdl\</p> <p>Your WSDL files must have the extension .wsdl.</p> <p>(Optional) Select a WSDL file from this drop-down list. This list reflects the files found by searching on <SiteScope root directory>\templates.wsdl/*.wsdl.</p>
Get Data	<p>Clicking the Get Data button causes the specified WSDL file to be retrieved and analyzed for method arguments. The ensuing page displays the measurements available for monitoring.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Content Match	<p>Type a string of text to check for in the returned page or frameset. If the text is not contained in the page, the monitor displays the message <code>no match on content</code>.</p> <p>HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for. This works for XML pages as well. Example: "< B> Hello< /B> World"</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <code>i</code> after the trailing slash to indicate that the search is not case sensitive. Example: <code>/href=Doc\d+\.\html/</code> or <code>/href=doc\d+\.\html/i</code></p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression. Example: <code>/Temperature: (\d+)</code></p> <p>Note: The search is case sensitive.</p>
Use User-Defined SOAP XML	Select this check box to use the XML in the Use SOAP XML box. This enables you to use XML that has been manually defined.
Use SOAP XML	Displays the SOAP XML for the selected Web service extracted from the WSDL file. You can make changes to the default XML, and use the manually defined XML in this box by selecting the Use User-Defined SOAP XML check box.
Web Service Server URL	Shows the URL of the Web service server to be monitored.
HTTP Content Type	The content type of the HTTP request.
HTTP User Agent	The HTTP user agent for the SOAP request.

GUI Element	Description
Use .NET SOAP	Select this check box if the Web service is based on Microsoft .NET.
Request's Schema	The request schema. Currently SiteScope only supports SOAP.
Method Name Space	The XML name space for the method in the SOAP request. During initial setup, this value is extracted from the WSDL file.
Schema Name Space	The XML name space for the schema in the SOAP request. During initial setup, this value is extracted from the WSDL file.
SOAP ACTION	The SOAP ACTION URL in the header of the SOAP request to the Web Service. During initial setup, this is extracted from the WSDL file.
NTLM Domain	If the Web service requires NTLM / Challenge Response authentication, a domain name is required as part of your credentials (as well as a user name and password below).
Authorization User Name	<p>If the web service requires a user name and password for access (Basic, Digest, or NTLM authentication), type the user name in this box.</p> <p>Alternately, you can leave this entry blank and type the user name in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.</p>
Authorization Password	<p>If the web service requires a user name and password for access (Basic, Digest or NTLM authentication), type the password in this box.</p> <p>Alternately, you can leave this entry blank and type the password in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.</p>

GUI Element	Description
HTTP Proxy	(Optional) A proxy server can be used to access the URL. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the URL, type the name here. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the URL, type the password here. Note: Your proxy server must support Proxy-Authentication for these options to function.

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Report SOA Topology to HP Business Availability Center	This monitor can identify the topology of the server being monitored. If this option is selected, the monitor creates a SOA topology in Business Availability Center's CMDB. For information about the topology, see "Web Service Topology Settings" on page 790.

XML Metrics Monitor Settings

Description	<p>The XML Metrics Monitor allows you to monitor metrics for systems that make performance data available in the form of an XML file or page. The error and warning thresholds for the monitor can be set on one or more different objects.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"XML Metrics Monitor Overview" on page 791

The Add/Edit XML Metrics Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Authorization User Name	If the URL with the XML content you want to monitor requires a user name and password to access it, type the user name in this box.
Password	If the URL with the XML content you want to monitor requires a name and password for access, type the password in this box.
Proxy Server	(Optional) If you must use a proxy server to access the XML URL, type the host or domain name and port of the proxy server in this box.

GUI Element	Description
Proxy Server User Name	If you use a proxy server and the proxy requires a name and password to access the target URL, type the user name in this box. Note: The proxy server must support Proxy-Authenticate for these options to function.
XML URL	Type the URL of the XML page or file that contains the metrics that you want to monitor.
XSL File	(Optional) Convert the XML metrics file into a format that SiteScope can use.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	The number of seconds that the monitor should wait the XML page to complete downloading before timing-out. Once this time period passes, the monitor logs an error and reports an error status.
Authorization NTLM Domain	Type the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL.

GUI Element	Description
Preemptive Authorization	<p>Select when the Authorization User Name and Authorization Password should be sent if SiteScope requests the target URL.</p> <ul style="list-style-type: none"> ▶ Use Global Preference. Select to have SiteScope use the When to Authenticate setting as specified in the Preemptive Authorization section of the General Preferences page. ▶ Authenticate first request. Select to send the user name and password on the first request SiteScope makes for the target URL. Note: If the URL does not require a user name and password, this option may cause the URL to fail. ▶ Authenticate if requested. Select to send the user name and password on the second request if the server requests a user name and password. Note: If the URL does not require a user name and password, this option may be used. <p>All options use the Authorization User Name and Authorization Password entered for this monitor instance. If these are not specified for the individual monitor, the Default Authentication Username and Default Authentication Password specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p>Note: Preemptive Authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
Accept Untrusted Certs for HTTPS	<p>Check this option if you need to use certificates that are untrusted in the cert chain to access the target XML URL using Secure HTTP (HTTPS).</p>
Accept Invalid Certs for HTTPS	<p>Check this option if you need to accept an invalid certificate to access the target XML URL using Secure HTTP (HTTPS). This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.</p>

18

Network Monitors

This chapter includes the main concepts and reference information for monitoring network health and availability.

This chapter includes:

Concepts

- ▶ DHCP Monitor Overview on page 824
- ▶ DNS Monitor Overview on page 825
- ▶ FTP Monitor Overview on page 826
- ▶ Formula Composite Monitor Overview on page 828
- ▶ MAPI Monitor Overview on page 830
- ▶ Mail Monitor Overview on page 834
- ▶ Microsoft Windows Dial-up Monitor Overview on page 834
- ▶ Network Bandwidth Monitor Overview on page 837
- ▶ Ping Monitor Overview on page 838
- ▶ Port Monitor Overview on page 839
- ▶ RTSP Monitor Overview on page 840
- ▶ SNMP Monitor Overview on page 844
- ▶ SNMP Trap Monitor Overview on page 845
- ▶ SNMP by MIB Monitor Overview on page 846

Reference

- ▶ Network Monitors User Interface on page 849

DHCP Monitor Overview

Use the DHCP Monitor to monitor your DHCP servers to verify that they are working properly. If your DHCP server fails, machines relying on DHCP are unable to acquire a network configuration when rebooting. Additionally, as DHCP address leases expire on already-configured machines, those machines drop off the network when the DHCP server fails to renew their address lease.

Most networks have a DHCP server listening for DHCP requests. This monitor finds DHCP servers by broadcasting a request for an IP address and waiting for a DHCP server to respond.

Note: This monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running. The DHCP Monitor type does not appear in the interface until this library is installed. See the section on Installation of DHCP Software Library below for more information.

Installation of DHCP Software Library

The SiteScope DHCP Monitor uses the jDHCP library, available from <http://www.dhcp.org/javadhcp/>. After downloading the library (either in .zip or in .tar.gz format), extract the file named **JDHCP.jar** and place it in the **<SiteScope root directory>\java\lib\ext** directory, such that the file is located at **<SiteScope root directory>\java\lib\ext\JDHCP.jar**. After installing the **JDHCP.jar** file, stop and restart the SiteScope service.

Scheduling This Monitor

Each time the DHCP Monitor runs, it returns a status and writes it in the monitoring log file. It also writes the total time it takes to receive and release an IP address in the log file. Your DHCP server is a critical part of providing functionality to other hosts on your network, so it should be monitored frequently (every 2-5 minutes).

For details on configuring this monitor, see “DHCP Monitor Settings” on page 850.

DNS Monitor Overview

Use the DNS Monitor to monitor your DNS servers to verify that they are working properly. If your DNS server is not working properly, you cannot get out on the network and people trying to reach your server are not able to find it.

Most companies have both a primary and a secondary DNS server. If your company employs a firewall, these servers may sit outside the firewall with another DNS server located inside the firewall. This internal DNS server provides domain name service for internal machines. It is important to monitor all of these servers to check that each is functioning properly.

Scheduling This Monitor

If you have both a primary and secondary DNS server outside your firewall and an internal DNS server inside your firewall, you should monitor your internal server and your primary DNS server every 2-5 minutes. You can monitor the secondary DNS server less frequently (about every 10-15 minutes).

For details on configuring this monitor, see “DNS Monitor Settings” on page 851.

FTP Monitor Overview

If you provide FTP access to files, it is important to check that your FTP server is working properly. Use the FTP monitor to check FTP servers to insure the accessibility of FTP files.

Setup Requirements

To use this monitor, you must:

- ▶ have network access to an FTP server
- ▶ know the relative paths, if any, to the files on the FTP server
- ▶ know an applicable user name and password to access the files
- ▶ know the filenames of one or more files available for FTP transfer

In addition to retrieving specific files, the FTP Monitor can help you verify that the contents of files, either by matching the contents for a piece of text, or by checking to see if the contents of the file ever changes compared to a reserve copy of the file.

While you may have many files available for FTP from your site, it is not necessary to monitor every one. It is recommended that you check one small file and one large file.

A common strategy is to monitor a small file every 10 minutes or so just to verify that the server is functioning. Then schedule a separate monitor instance to FTP a large file once or twice a day. You can use this to test the ability to transfer a large file without negatively impacting your machine's performance. You can schedule additional monitors that watch files for content and size changes to run every 15 minutes to half hour. Choose an interval that makes you comfortable.

If you have very important files available, you may also want to monitor them occasionally to verify that their contents and size do not change. If the file does change, you can create a SiteScope alert that runs a script to automatically replace the changed file with a back-up file.

Status

The reading is the current value of the monitor. Possible values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- login failed
- file not found
- contents changed

The status is logged as either **good** or **error**. An error status is returned if the current value of the monitor is anything other than OK.

For details on configuring this monitor, see “FTP Monitor Settings” on page 853.

Formula Composite Monitor Overview

Use this monitor if you have devices or systems in your network that return values that you want to combine in some way to produce a composite value. The following monitor types can be used to build a Formula Composite Monitor:

- ▶ Database Query monitor. For more information see “Database Query Monitor Overview” on page 729.
- ▶ Microsoft Windows Performance Counter Monitor. For more information see “Microsoft Windows Performance Counter Monitor Overview” on page 898.
- ▶ Script Monitor. For more information see “Script Monitor Overview” on page 781.
- ▶ SNMP Monitor. For more information see “SNMP Monitor Overview” on page 844.

If you need alert logic that is more complex than SiteScope's standard alerts allow, you can use the Formula Composite Monitor to create custom alert behavior. For example, if you have two parallel network devices that record network traffic but the values need to be combined to produce an overall figure of network traffic. This monitor may also be used to combine the results returned by scripts run on two different machines.

Each time the Formula Composite Monitor runs, it returns a status based on the measurement results of the two subordinate monitors and the calculation specified for the composite monitor.

Notes and Limitations

- ▶ You must create at least two individual Script, SNMP, Database Query or Microsoft Windows Performance Counter monitor instances before you can set up a Formula Composite Monitor for those monitors.
- ▶ The monitors you create for use with a Formula Composite monitor should be configured to return a single value per monitor. This is generally simple with SNMP monitors. Database Query and Script monitors should use queries and scripts that return a single value. For Microsoft Windows Performance Counter monitors, you can use the (Custom Object) option for the **PerfMon Chart File** setting and then specify a single performance **Object**, **Counter**, and **Instance** (if applicable) in the Advanced Settings section of the monitor setup. If a subordinate monitor is configured to return more than one numeric measurement, only the first numeric measurement from that monitor instance is used by the Formula Composite Monitor.
- ▶ You should only use the Formula Composite monitor for calculations that you consider to be compatible data types. The monitor does not verify that the data returned by the subordinate monitors are compatible.
- ▶ You can select two different types of monitors as subordinate monitors of a Formula Composite monitor. For example, one monitor may be a Script monitor and the other may be a Database Query monitor.
- ▶ Moving any of the monitors being used by the Formula Composite Monitor causes the composite monitor to report an error. If it is necessary to move either of the underlying monitors, recreate or edit the Formula Composite Monitor to select the monitor from its new location.

For details on configuring this monitor, see “Formula Composite Monitor Settings” on page 856.

MAPI Monitor Overview

Use the MAPI Monitor to monitor the availability of Microsoft Exchange 5.5 and above. The monitor checks for e-mail delivery time. This allows you to verify availability of the MAPI server by sending and receiving a test message in a Microsoft Exchange e-mail account. Create a separate MAPI monitor instance for each Microsoft Exchange server in your environment.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

System Requirements

There are several important configuration requirements that must be performed or verified before the MAPI Monitor can be used. This section describes the steps you use to configure your environment for this monitor. The following are several definitions that are used in the steps listed below.

- ▶ **Local Administrator.** An account that has administrative privileges on the local machine. An account can have this privilege either implicitly by having Domain Admin privileges or explicitly by adding as a member of the Administrators group on the local machine. Consult your system administrator, if necessary, for help with creating accounts.
- ▶ **MailBox Owner.** This is an "owner" account for which an Exchange mailbox has been set up. To use the MAPI Monitor, this account must be a Local Administrator (see definition above) on the SiteScope server.
- ▶ **SiteScope User.** This is the account that is used to run the SiteScope service. This account must also be a Local Administrator (see definition above).

Before creating a MAPI Monitor, you must perform the setup steps as described in “Preparing the System for Using the MAPI Monitor” below.

Preparing the System for Using the MAPI Monitor

Before creating a MAPI Monitor, perform the following setup steps:

1 Create mailbox accounts on each Exchange Server to be monitored with the MAPI monitor.

Exchange mailbox accounts are used by SiteScope to measure the roundtrip time for a message to originate and arrive in a mailbox account. The MAPI Monitor setup page supports up to two mailboxes per Exchange Server. If only one mailbox is specified on the MAPI Monitor setup page the same mailbox can be used for the sender and receiver accounts. Consult your Exchange system administrator if you need help setting up mailbox accounts for use with the SiteScope MAPI monitor.

2 Add each Exchange Mailbox Owner to the Administrators users group on the SiteScope server.

The Mailbox Owner accounts setup in step 1, which are by definition domain logons, must be added as to the Administrators group on the SiteScope server.

- ▶ Click **Start > Settings > Control Panel > Users and Passwords > Advanced tab** or open the Computer Management utility and expand the **Local Users and Groups** folder in the left pane and click the **Groups** folder.
- ▶ Double-click the Administrators group icon to open the Administrators Properties window.
- ▶ Click the **Add** button to add each Mailbox Owner you expect to use with the MAPI Monitor.

Note: Make sure that the domain logon description is of the form domain\logon.

3 Install Microsoft Outlook or an equivalent MAPI 1.0 mail client on the SiteScope server.

The SiteScope server requires a MAPI 1.0 client such as Outlook XP or Outlook 2003 or later. Consult your system administrator, if necessary, for help installing a compliant MAPI client.

4 Configure Outlook for the MailBox User.

After logging in to the SiteScope server as the MailBox User created in step 1 the Outlook wizard may start for setting up an Outlook profile for the mail box. If an Outlook client is already installed, then you may run that Outlook client and click **Tools > e-mail Accounts** to create a profile for the mailbox/logon you intend to use with the MAPI Monitor. See your Exchange System administrator for help configuring an Outlook client on your SiteScope server if necessary.

Creating an Outlook profile is not necessary, although it may be helpful for the purpose of troubleshooting. Once the wizard prompts you to set up a profile you can cancel to exit the wizard.

5 Verify that the SiteScope user logon is a member of Administrators group or a domain administrator account.

Important: The SiteScope user account must be a Local Administrator or be a member of the domain admins group.

To change the logon account for the SiteScope user:

- ▶ Open the **Services** control utility on the SiteScope server.
- ▶ Right-click the **SiteScope** service entry and click **Properties**. The SiteScope Properties settings page opens.
- ▶ Click the **Log On** tab.
- ▶ Verify that the SiteScope user is run as a member of Administrators group or a domain logon account. To change the logon properties, click the **This account** radio button and type the SiteScope user logon.
- ▶ Restart the SiteScope server after making changes to the SiteScope service logon account.

6 Add the SiteScope user account to the "Act as part of the operating system" local security policy.

To add the SiteScope user account to the "Act as part of the operating system" local security policy.

- Click **Start > Programs > Administrative Tools > Local Security Policy**. The Local Security Policy panel opens.
- Click the **Local Policies** folder in the left pane and then click the **User Rights Assignments** folder to display the list of policies.
- Double-click the **Act as part of the operating system** policy item in the right pane. The Local Security Policy Setting list opens.
- If the SiteScope user is not in the list of logons for this security policy setting then it must be added now. Click the **Add** button to bring up the Select Users or Groups window.
- Type the SiteScope user logon using the **domain\logon** format if the SiteScope user is a domain account.
- After adding the SiteScope service logon, you must reload the security settings. To do this, right-click the **Security Settings** root folder in the left pane and click **Reload**.
- Restart the SiteScope service after making changes to security policy.

For details on configuring this monitor, see "MAPI Monitor Settings" on page 859.

Mail Monitor Overview

The Mail Monitor checks to see that the mail server is both accepting and delivering messages. This enables you to verify that all your mail servers, including internal servers where a firewall is used, are working properly. Each time the Mail Monitor runs, it returns a status and writes it in the log file. It also writes the total time it takes to send and receive the mail message in the log file.

It is recommended to monitor your primary mail server at least every five minutes. The other mail servers can be monitored less frequently. You may find it useful to set up a special mail account to receive the test e-mail messages send by SiteScope.

For details on configuring this monitor, see “Mail Monitor Settings” on page 862.

Microsoft Windows Dial-up Monitor Overview

Use the Microsoft Windows Dial-up Monitor to measure the availability and performance of your Internet applications from a dial-up user's perspective. The Microsoft Windows Dial-up Monitor can also be used to monitor the availability and performance of remote access servers.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

If you are primarily interested in dial-up availability, then you can just have the Microsoft Windows Dial-up Monitor try to connect, and if successful, run one or two low impact monitors to verify that the connection is operating properly. If you are more interested in the perspective of a dialup user, then running a suite of monitors that represent typical user tasks gives you more complete assessment.

To set up the Remote Access Service on a Windows NT machine, go to the Network Control Panel, and add the service. At that time you also have the option of adding one or more modems as Remote Access modems. At least one of the modems has to have dial out capability for this monitor to work.

Notes and Limitations

- ▶ The Microsoft Windows Dial-up Monitor should not be used on a machine that is used for accessing resources outside of the local network. This is because the monitor uses Remote Access, which affects the entire machine's network connectivity when it establishes a connection. For example, if you are using a Web browser on the machine where SiteScope is running a Microsoft Windows Dial-up Monitor, and the Microsoft Windows Dial-up Monitor is connected, all the requests by the browser out to the Internet also use the dial-up connection. This affects the speed of the browser and the reading from the Microsoft Windows Dial-up Monitor.
- ▶ The Microsoft Windows Dial-up Monitor prevents the other SiteScope monitors (those not being run by this Dial-up Monitor) from running while the dial-up connection is established (they are held up until the Microsoft Windows Dial-up Monitor is completed).
- ▶ No two Microsoft Windows Dial-up Monitors are run at the same time.
- ▶ The Microsoft Windows Dial-up Monitor uses the dial-up connection only for requests outside of the local network. If you have monitors that access network resources on the local network, their readings are the same as if the Microsoft Windows Dial-up Monitor was not used. However, monitors that access network resources outside the local network use the dial-up connection. For example, if you ran two Ping monitors in the Microsoft Windows Dial-up Monitor, one of which was `yourserver.com` (on the local network), and the other of which was `externalserver.com` (on an external network), the `yourserver.com` Ping would be very fast, because it would use the LAN, while the `externalserver.com` Ping would take longer, because it would go through the dial-up connection.

Scheduling This Monitor

The Microsoft Windows Dial-up Monitor stops other monitors from running while it is connected, so you should take into account the number and kinds of monitors that are running while the connection is established as well as the number of other monitors that are running. If SiteScope is running only Microsoft Windows Dial-up Monitors, then you can schedule them more frequently (every 5 or 10 minutes). However, if you are monitoring many other items, choose a large interval (hours), so that other monitoring is not disrupted.

Only one Microsoft Windows Dial-up Monitor can run at a time, so if you have more than one Microsoft Windows Dial-up Monitor, take that into account when scheduling the monitors.

Status

Each time the Microsoft Windows Dial-up Monitor runs, it returns a reading and status message and writes them in the monitoring log file. The reading is the current value returned by the monitor. For example, "5 of 5 monitors OK in 55 sec", or "The line was busy". The status is logged as either OK or warning.

For reports, the Microsoft Windows Dial-up Monitors saves the total time taken (to connect and run the monitors), the connect time (the time for the modem to establish a physical connection), the authorization time (the time after physical connection is established before the connection can actually be used), and the percentage of the monitors run that were OK.

For details on configuring this monitor, see "Microsoft Windows Dial-up Monitor Settings" on page 867.

Network Bandwidth Monitor Overview

Use the Network Bandwidth Monitor to monitor SNMP-enabled network appliances such as routers and switches. The Network Bandwidth Monitor operates like many other browsable monitors to gather information from a source and enable the user to choose which items in the tree it should monitor. It works by connecting to the specified network component and returning a list of interfaces.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

The MIB files in **SiteScope\templates.mib** are used to create a browsable tree that contains names and descriptions of the objects found during the traversal. Note that an object may or may not be displayed with a textual name and description, depending on the MIB's available in **SiteScope\templates.mib**. SiteScope does not display objects for user selection when it has no knowledge of how to display those objects. For example, a plain OctetString may contain binary or ascii data, but SiteScope has no way to decode and display this data correctly without more information.

Performing Sanity Checks

By default, SiteScope performs a sanity check for every run of the monitor. This checks that the values returned by the monitor are in the valid range. You can also choose to disable these sanity checks.

To disable the sanity checks, clear the **Network Bandwidth monitor sanity** check box in the Infrastructure Settings Preferences page. To access this setting, expand **Preferences** in the left menu tree, choose **Infrastructure Settings Preferences**, and select the **Monitor Settings** section.

For details on configuring this monitor, see “Network Bandwidth Monitor Settings” on page 869.

Ping Monitor Overview

The Ping Monitor obtains two of the most common measurements used to determine if your network connection is congested: Round Trip Time and Loss Percentage. An increase of either of these suggests that you are experiencing problems.

In the case of Loss Percentage, you want to see a 0% reading. A 100% reading indicates your link is completely down. Some loss may happen occasionally, but if it becomes common, either some packets are being lost or the router is exceptionally busy and dropping packets.

Each time the Ping Monitor runs, it returns a reading and a status message and writes them in the monitoring log file. It also writes the total time it takes to receive a response from the designated host in the log file.

What to Monitor

It is recommended that you set up monitors that test your connection to the Internet at several different points. For example, if you have a T1 connection to a network provider who in turn has a connection to the backbone, you would want to set up a Ping Monitor to test each of those connections. The first monitor would ping the router on your side of the T1. The second would ping the router on your provider's side of the T1. The third monitor would ping your provider's connection to the backbone.

In addition to these monitors, it is also a good idea to have a couple of other monitors ping other major network providers. These monitors do not really tell you whether the other provider is having a problem, but it does tell you if your network provider is having trouble reaching them.

Scheduling This Monitor

You can monitor your own router as often as every two minutes without compromising system performance. The monitors that watch your provider's connection to your line and to the backbone should only be run every ten minutes or so. This minimizes traffic while still providing you with sufficient coverage.

For details on configuring this monitor, see “Ping Monitor Settings” on page 874.

Port Monitor Overview

Use the Port Monitor for monitoring network applications that none of the other SiteScope monitors watch such as Gopher and IRC services, some media services, or other custom network applications. You are notified immediately if SiteScope is unable to connect to the monitored port.

Scheduling This Monitor

Scheduling Port monitors depends on the application or system you are monitoring. The Port Monitor does not use many resources, so you can schedule it to run as often as every 15 seconds if necessary. Monitoring most systems every 10 minutes is normally sufficient.

Status

Each time the Port Monitor runs, it returns a status message and writes them in the monitoring log file. It also writes the total time it takes to receive a response from the remote service.

The reading is the current value of the monitor. The possible values for the Port Monitor are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- match error

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

For details on configuring this monitor, see “Port Monitor Settings” on page 875.

RTSP Monitor Overview

Use the RTSP Monitor to check the availability of a media source or media file, check that it can be retrieved, that the file is complete, and that the download rate meets your requirements.

Note: The RTSP Monitor does not support Real Media file types (for example: *.ra, *.ram files) or Windows Media files (for example: *.asf files). Use the Real Media Server Monitor and Real Media Player Monitor or the Microsoft Windows Media Server Monitor and Microsoft Windows Media Player Monitor to monitor these types of services. For more information see “Stream Monitors” on page 941.

Solaris and Linux Requirements

For SiteScope on Solaris or Linux, the RTSP Monitor requires that an X11 server be available. If SiteScope is unable to contact the X11 server specified by the DISPLAY environment variable, it cannot load the JMF player used by this monitor and issues a "Player Create Error" error message.

The DISPLAY environment variable must be set prior to starting SiteScope. For convenience, this variable can be set in the SiteScope user's login environment scripts.

The following are three options for meeting the configuration requirement for the RTSP Monitor on Solaris and Linux:

- ▶ Log in to the graphical system console, run `xhost +localhost`, and set your DISPLAY variable to the required value before starting SiteScope.

You must remain logged into the graphical console to maintain the X11 server active. If you log out of the console session, the X11 server shuts down and the RTSP Monitor is not able to contact it.

- ▶ Run a PC X11 server, such as Exceed, and specify the required value for DISPLAY prior to starting SiteScope.

The X11 server process (such as Exceed), must be running as long as SiteScope is running. If the RTSP Monitor is unable to contact the X11 server it generates a Player Create Error message.

- ▶ Install and run Xvfb, the X Virtual Frame Buffer on your Solaris/Linux system. Xvfb is an X11 server emulator which can be run as a daemon and meets the X11 server requirements of the RTSP Monitor.

Most Linux distributions include Xvfb, and it is also available on Solaris 9. For earlier Solaris versions, you must download the X11R6 source code from ftp.x.org.

After installing Xvfb, a startup script can be configured to start Xvfb on system boot with a command similar to the following:

```
/path_to_xvfb/Xvfb:77 > /dev/null 2>&1 &
```

The **:77** parameter tells Xvfb to run on display number 77. In this example, you must set your display variable to `<hostname>:77`.

The advantage of Xvfb over the other two options is that it provides a working X11 server without requiring that a user be logged into a system console on either an NT or UNIX system.

The RTSP Monitor makes use of the Java Media Framework (JMF) which provides the capability of monitoring a variety of real time digital media types and protocols. This includes HTTP retrieval of media files and RTSP streaming of many types of files. The table below is an overview of the media formats that have some support in the RTSP Monitor.

Note: Due to the many variations of media recording options, not all files of the types listed below are supported by the Java Media Framework and RTSP Monitor. For example, some MP3 and MOV options are not supported. We recommend that you test a variety of files with the RTSP Monitor to determine if the file format you want to monitor can be decoded by the RTSP Monitor.

Media Type	File Format
Audio Interchange File Format (Apple)	*.aiff
Audio Video Interleave (Microsoft)	*.avi
Flash (Macromedia)	*.swf, *.spl
Global Standard for Mobile Communications GSM (wireless telephony standard)	*.gsm
HotMedia (IBM)	*.mvr
Musical Instrument Digital Interface (MIDI)	*.mid
Motion Picture Experts Group MPEG-1 Video	*.mpg
MPEG Layer II Audio	*.mp2
MPEG Layer III Audio	*.mp3
QuickTime Movie (Apple)	*.mov
Sun Audio (Sun Microsystems)	*.au
Wave audio file format (Microsoft)	*.wav

A more complete list of supported media types can be found at <http://java.sun.com/products/java-media/jmf/2.1/formats.html#RTPFormats>.

Note: The SiteScope RTSP Monitor does not support RealMedia formats from RealNetworks. To monitor RealMedia servers and media formats, see the Real Media Server Monitor or Real Media Player Monitor in “Stream Monitors” on page 941.

Scheduling This Monitor

This monitor should be set to run according to your reasonable acceptable error period. The utilization of monitoring bandwidth and overall monitoring system performance should be considered in setting the run interval for this type of monitor. The default run interval is set to 10 minutes.

Status

Each time a RTSP Monitor runs, it attempts to open and read a specified media stream or download and play a specified media file. The monitor records a status and stream or file statistics when the session is completed. If the file or stream is not supported or is unavailable, an error is reported.

Each time the monitor runs it returns a status which includes the current value of the monitor. The possible status values are:

- OK
- warning
- error

The final status result is either OK, error, or warning based on threshold established for these conditions.

For details on configuring this monitor, see “RTSP Monitor Settings” on page 877.

SNMP Monitor Overview

Use the SNMP Monitor to monitor devices that communicate with the SNMP protocol, such as firewalls, routers, and UPS's. Several operating systems suppliers also provide SNMP agents and Management Information Bases (MIB's) for accessing workstation or server performance metrics, interface statistics, and process tables by using SNMP.

You can use the SNMP Monitor to watch any values known by the SNMP agent running on a device, provided that you can supply an OID that maps to that value. If your router supports SNMP, for example, you could have SiteScope monitor for packet errors, bandwidth, or device status.

Note: To have SiteScope listen for SNMP traps from multiple devices, use the SNMP Trap Monitor.

Setup Requirements

Requirements for using the SNMP Monitor include:

- ▶ SNMP agents must be deployed and running on the servers and devices that you want to monitor.
- ▶ The SNMP agents must be supplied with the necessary Management Information Bases (MIB's) and configured to read those MIB's.
- ▶ You must know the Object ID's (OIDs) of the parameters you want to monitor. In some cases, an equipment manufacturer may supply a list of OIDs that are available. Otherwise, you may need to locate a MIB browser utility to parse a MIB and extract the values of interest to you. The monitor supports monitoring agents of SNMP versions 1, 2, and 3. If you want the monitor to get you the next OID of the OID you entered, you can type the OID with a plus sign (+) at the end of the OID (for example, 1.3.6.1.2.1.4.3+). For each monitor run, the monitor retrieves the next OID value and not the OID that you entered. This may be helpful if you want to reach one of the SNMP table columns.

For information about monitoring SNMP systems, refer to the HP Software Self-solve knowledge base (<http://h20230.www2.hp.com/selfsolve/documents>). To enter the knowledge base, you must log in with your HP Passport ID.

For details on configuring this monitor, see “SNMP Monitor Settings” on page 879.

SNMP Trap Monitor Overview

Note: To have SiteScope query a specific device for a specific value, use the SNMP Monitor.

Use the SNMP Trap Monitor for automatically collecting SNMP Traps from other devices. With SiteScope doing this for you at set intervals, you can eliminate the need to check for the SNMP Traps manually. In addition, you can be notified of warning conditions that you may have otherwise been unaware of until something more serious happened. Each time that it runs this monitor, SiteScope checks traps that have been received since the last time it ran.

You also must configure the network devices to send SNMP Traps to SiteScope. On Windows 2000 systems, this can be configured by using the **Administrative Tools > Services > SNMP Service > Properties > Traps** page. SNMP agents on UNIX platforms usually require that you edit the configuration files associated with the agent. For an example of working with other devices, see the instructions on the Cisco Web site for SNMP Traps and Cisco Devices.

Note: The SNMP Trap Monitor uses port 162 for receiving traps. If another application or process on the machine where SiteScope is running has bound this port, the monitor reports an **Address in use** error.

For details on configuring this monitor, see “SNMP Trap Monitor Settings” on page 884.

SNMP by MIB Monitor Overview

The SNMP by MIB Monitor gathers information from a source, organizes it into a browsable tree structure, and allows you to choose which items in the tree it should monitor. It works by connecting to the specified SNMP agent and performing a full traversal of the MIB's implemented by the agent. Thus, you do not need to know which objects are present on the agent in advance. The monitor supports agents of version 1, 2, and 3.

The MIB files in **SiteScope\templates.mib** are then used to create a browsable tree that contains names and descriptions of the objects found during the traversal. Note that an object may or may not be displayed with a textual name and description, depending on the MIB's available in **SiteScope\templates.mib**. SiteScope does not display objects for user selection when it has no knowledge of how to display those objects. For example, a plain OctetString may contain binary or ascii data, but SiteScope has no way to decode and display this data correctly without more information.

Troubleshooting MIB Compilation

As mentioned above, you can add to the MIBs of which SiteScope is aware by putting new MIB files in the `templates.mib` directory. To recompile any new MIBs, you must restart SiteScope. Unfortunately, because MIB files may depend on other MIB files, and because ASN.1 syntax is not always obeyed completely by vendors, you may encounter compilation errors with some MIBs. Below is a series of steps you can follow when compiling new MIBs and troubleshooting compilation failures:

- Add new MIB files to the **templates.mib** directory. SiteScope only compiles MIBs in ASN.1 format which abide by the SMIV1 or SMIV2 standards.
- Restart SiteScope.
- Proceed as if to add a new SNMP by MIB Monitor. Before adding the monitor, check to see that your new MIB files are listed in the MIB File drop-down box. If they are, then they were successfully compiled and you may now use the SNMP by MIB monitor and the SNMP by MIB tool to browse devices that implement these MIBs. If your newly added MIBs are not listed in the MIB File drop-down box, then proceed to the next step.
- Open the file **error.log** in the logs directory. Look for error messages about MIB compilation near the time of your most recent restart. The error messages in the file contain descriptions of compilation errors encountered in each file, together with the line number that helps you identify the source of the errors.
- Correct the errors found in **error.log**. Usually, these errors can be fixed by one of the following:
 - Adding a MIB to **templates.mib** on which some of the new MIBs depend.
 - Removing a MIB from **templates.mib** which is duplicated or upgraded in the new MIBs.

- ▶ Fixing broken comments in the new MIBs. Note that a comment is defined as follows: "ASN.1 comments commence with a pair of adjacent hyphens and end with the next pair of adjacent hyphens or at the end of the line, whichever occurs first." This means that a line containing only the string "-----" is a syntax error, whereas the a line containing only the string "----" is a valid comment. Beware of lines containing only hyphens, as adding or subtracting a single hyphen from such lines may break compilation for that MIB.
- ▶ Fixing missing IMPORT statements. Some MIBs may neglect to import objects that they reference which are defined in other MIBs. You can also search in Web sites for the error that you get in **error.log**. There is a lot of information about these errors on the Web.
- ▶ After correcting the errors described in **error.log**, restart SiteScope and follow the procedure above to verify that the new MIB files compiled correctly.

Note:

- ▶ To check compilation of the new MIB, you can also use the command line tool, which is located in <SiteScope root directory>\tools \SNMPMIBCompilation. This tool enables you to check the new MIB compilation, so that you do not need to restart SiteScope for every change you make in the MIB file. The directory also contains a **ReadMe** file which explains how to use the tool.
- ▶ If the MIB is compiled using another tool (for example, MG-SOFT or iReasoning), you are not notified that the MIB file is compiled in SiteScope. The different compilers have different behaviors. Some are more restrictive than others.

For details on configuring this monitor, see "SNMP by MIB Monitor Settings" on page 886.

Network Monitors User Interface

This section describes:

- DHCP Monitor Settings on page 850
- DNS Monitor Settings on page 851
- FTP Monitor Settings on page 853
- Formula Composite Monitor Settings on page 856
- MAPI Monitor Settings on page 859
- Mail Monitor Settings on page 862
- Microsoft Windows Dial-up Monitor Settings on page 867
- Network Bandwidth Monitor Settings on page 869
- Ping Monitor Settings on page 874
- Port Monitor Settings on page 875
- RTSP Monitor Settings on page 877
- SNMP Monitor Settings on page 879
- SNMP Trap Monitor Settings on page 884
- SNMP by MIB Monitor Settings on page 886

DHCP Monitor Settings

Description	<p>Checks a DHCP Server by using the network. It verifies that the DHCP server is listening for requests and that it can allocate an IP address in response to a request.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<ul style="list-style-type: none"> ▶ This monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running. The DHCP Monitor type does not appear in the interface until this library is installed. For more information, see "Installation of DHCP Software Library" on page 824. ▶ Monitors must be created in a group in the monitor tree.
Useful Links	"DHCP Monitor Overview" on page 824

The Add/Edit DHCP Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	Type the time, in seconds, to wait for an IP address.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Requested Client Address	Optionally, the IP address to request from the DHCP server.

DNS Monitor Settings

Description	<ul style="list-style-type: none"> ▶ Checks a Domain Name Server by using the network. ▶ Verifies that the DNS server is accepting requests. ▶ Verifies that the address for a specific domain name can be found. <p>Returns a status and writes it in the monitoring log file with each running.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"DNS Monitor Overview" on page 825

The Add/Edit DNS Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Host Name	Type the host name to lookup. If you only want to verify that your DNS server is operating, the host name you type here can be any valid host name or domain name. Example: demo.thiscompany.com To verify that a domain name resolves to a specific IP address, type the IP address that corresponds to the host name you type in the Host address box in the Advanced Settings section below.
DNS Server Address	Type the IP address of the DNS server that you want to monitor. Example: 206.168.191.1

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Host address	(Optional) You can use the DNS monitor to verify that a host name or domain name resolves to the correct IP address or addresses. Type the IP address or addresses that are mapped to the Host Name (domain name) entered above. Note: If you type more than one IP address, the monitor reports a status of good , even if only one of the IP addresses that you type is mapped correctly to the Host Name . When using this option, the monitor only reports an error if none of the IP addresses entered in this box are mapped to the given Host Name .

FTP Monitor Settings

Description	<p>Attempts to log into an FTP server and retrieve a specified file. A successful file retrieval indicates that your FTP server is functioning properly.</p> <p>Use this page to add a monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"FTP Monitor Overview" on page 826

The FTP Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
FTP Server	<p>Type the IP address or the name of the FTP server that you want to monitor.</p> <p>Example: 206.168.191.22 or ftp.thiscompany.com</p>
File	<p>Type the file name to retrieve in this box.</p> <p>Example: /pub/docs/mydoc.txt</p>
User Name	<p>Type the name used to log into the FTP server in this box. A common user name for general FTP access is user name anonymous.</p>
Password	<p>Type the password used to log into the FTP server in this box. If using the anonymous login, the password is also anonymous.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	The number of seconds that the FTP monitor should wait for a file to complete downloading before timing-out. Once this time period passes, the FTP monitor logs an error and reports an error status.
FTP Proxy	You may instruct SiteScope to run the FTP through an HTTP proxy. Generally, if you use an HTTP proxy you have it set up in your browser. Type that same information here. Remember to include the port. Example: proxy.thiscompany.com:8080 Note: The FTP Monitor does not support an FTP Proxy server.
Passive Mode	Select this box if you want SiteScope to use FTP passive mode. You use this mode to enable FTP to work through firewalls.
Proxy Server User Name	If the proxy server requires a name and password to access the file, type the name here. The proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the file, type the password here. The proxy server must support Proxy-Authenticate for these options to function.
Connection Timeout	The number of seconds that the FTP monitor should wait to connect to the FTP server before timing-out. Once this time period passes, the FTP monitor logs an error and reports an error status. Default value: 30

GUI Element	Description
Match Content	<p>Type a string of text to check for in the returned file. If the text is not contained in the file, the monitor displays no match on content. The search is case sensitive. You may also perform a regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching.</p> <p>Example: <code>"/Size \d\d/"</code> or <code>"/size \d\d/i"</code></p>
Check for Content Changes	<p>SiteScope records a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs. If the checksum changes, the monitor has a status of content changed error and go into error. If you want to check for content changes, you usually want to use compare to saved contents.</p> <p>The options for this setting are:</p> <ul style="list-style-type: none"> ➤ no content checking (default). SiteScope does not check for content changes. ➤ compare to last contents. Any changed checksum is recorded as the default after the change is detected initially. Thereafter, the monitor returns to a status of OK until the checksum changes again. ➤ compare to saved contents. The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor gets a content changed error and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents. ➤ reset saved contents. Takes a new checksum of the file and saves the resulting checksum on the first monitor run after this option is chosen. After taking the updated checksum, the monitor reverts to compare to saved contents mode.

 **Formula Composite Monitor Settings**

Description	<p>Simplifies the monitoring of complex network environments by checking the status readings of two SNMP, Script, Database Query, or Microsoft Windows Performance Counter monitors and performing an arithmetic calculation on their results.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Formula Composite Monitor Overview" on page 828

The Add/Edit Formula Composite Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Items	Choose two SNMP monitors, two Script monitors, two Database monitors, or two Microsoft Windows Performance Counter monitors from the selection menu that the Formula Composite Monitor should operate on. You can select individual monitors and then click the right arrow to the right of the selection menu to move the monitor to the selection list on the right. Select the second monitor from the list on the left and click the right arrow to move the selection to the list on the right. You may also control-click two monitors on a single operation and click the right arrow to move them to the list on the right.
Operation	Select the arithmetic operation to be performed on the results of the two monitors selected above. For example: Add the results, Multiply the results of the two monitors, Subtract the results of the first from the second, Divide the second by the first, and so on.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Run Monitors	<p>Select this box if you want the Formula Composite Monitor to control the scheduling of the selected monitors, as opposed to just checking their status readings. This is useful if you want the monitors to run one after another or run at approximately the same time.</p> <p>Note: Any monitors that are to be run this way should not also be run separately, so edit the individual monitors, blank out the Update Every box for that monitor, and save the changes. Those monitors then only run when scheduled by the Formula Composite Monitor.</p>
Monitor Delay	<p>If Run Monitors is checked, this is the number of seconds to wait between running each monitor.</p>
Constant	<p>Type an operator and a constant to operate on the result of the calculation specified in the Operation item above. For example, if an Operation of Add is selected above, entering the characters *8 in the Constant box multiplies the result of the Add operation by 8. The syntax for this box should be <operator> <number>. Valid operators are + (addition), - (subtraction), * (multiplication), and / (division). Numbers may be integers or decimals.</p>
Result Label	<p>Type a name for the result of the formula calculation.</p>



MAPI Monitor Settings

Description	<p>The MAPI Monitor checks a Messaging Application Program Interface (MAPI) server to confirm that e-mail operations can be run. The monitor is designed to test the operation of a Microsoft Exchange Server. It verifies that the server is accepting requests, and also verifies that a message can be sent and retrieved. It does this by sending a standard e-mail and deleting the mail if the message is successfully sent and received. If the received part of the monitoring fails (for example, because of a delay in sending the e-mail or due to a short timeout for receiving the mail) the test mail remains in the mailbox. The error and warning thresholds for the monitor are set based on the e-mail delivery time.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<p>Monitors must be created in a group in the monitor tree.</p>
Useful Links	<p>"MAPI Monitor Overview" on page 830</p>

The MAPI Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Receiver Server	Type the hostname or address of a Microsoft Exchange Server. The name can be an IP address or other name that can be resolved by the DNS server. It is recommended that you copy the server name as it appears in the Properties of the e-mail account you are using with this monitor.
Receiver Mailbox	Type the name (alias) of the mailbox to be used for this monitor. This is often the e-mail account name but it may be a different name. It is recommended that you copy the mailbox name as it appears in the E-Mail Account properties for the e-mail account you are using with this monitor.
Receiver Domain	Type the domain to which both the owner of the mailbox being used and the Microsoft Exchange server belong. Note: The owner of the mailbox to be used by this monitor must also have administrative account privileges on the machine where SiteScope is running. SiteScope also needs user account access to the domain where the Microsoft Exchange server is running.
Receiver User Name	Type the NT account login name for the user associated with the above e-mail account.
Receiver User Password	Type the NT account login password for the user name above.

GUI Element	Description
Sender Server	Type the sender's Microsoft Exchange server name. Notes: <ul style="list-style-type: none"> ▶ The MAPI sender is ignored if an SMTP sender is specified in the Advanced Settings. ▶ If no SMTP sender values are specified in the Advanced Settings, the receiver values are used if any of the sender values are not specified.
Sender Mailbox	Type the alias of the sending mailbox.
Sender Domain	Type the domain to which both the sending mailbox owner and the sending Microsoft Exchange server belong.
Sender User Name	Type the login name for the NT account of the sending mailbox owner.
Sender Password	Type the NT account login password for the sender account above.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Transaction Timeout	Type the number of seconds for the monitor to wait for the message to arrive before the monitor should timeout. The monitor reports an error if timeout value is met before the e-mail message is delivered.
SMTP Server	Type the SMTP server through which an outgoing message is sent. Note: If you set any of the SMTP values (Server , Sender or Receiver) they override the MAPI sender options specified in the Main Settings.
Sender	Type the e-mail address of the SMTP sender.

GUI Element	Description
Receiver	Type the e-mail address of the receiver. This must match the receiver mailbox alias specified in the Main Settings
Attachment	Type the full path of a file to attach to the outgoing SMTP message.

Mail Monitor Settings

Description	<p>The Mail Monitor checks a Mail Server by using the network. It verifies that the mail server is accepting requests, and also verifies that a message can be sent and retrieved. It does this by sending a standard mail message using SMTP and then retrieving that same message by using a POP user account. Each message that SiteScope sends includes a unique key that it checks to insure that it does not retrieve the wrong message and return a false OK reading. If SiteScope is unable to complete the entire loop, it generates an error message.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Mail Monitor Overview" on page 834

The Add/Edit Mail Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Action	<p>Select the action the Mail Monitor should take with respect to the mail server:</p> <ul style="list-style-type: none"> ▶ Send and Receive. This option allows you to send a test message to an SMTP server and then to receive it back from the POP3 or IMAP4 server. This checks that the mail server is up and running. ▶ Receive Only. This option allows you to check the incoming POP3 or IMAP4 mail servers for a message that was sent previously. This check is done by matching the content of the previously sent message. Note: If the Receive Only option is selected, the Match Content text box must have a value to match against. Also note that if the Receive Only option is selected, you should use this monitor for a dedicated mail account that is NOT being accessed by any other mail client. If another mail client attempts to retrieve mail messages from the account that the Mail Monitor is monitoring in Receive Only mode, the monitor and the other mail client may lock each other out of the account such that neither is able to retrieve the messages. ▶ Send Only. This option checks that the receiving mail server has accepted the message.
Sending E-Mail Server (SMTP)	<p>Type the hostname of the SMTP mail server to which the test mail message should be sent.</p> <p>Example: mail.thiscompany.com</p>

GUI Element	Description
Send to Address	<p>Type the mail address to which the test message should be sent. This should be the address for the POP account that you specified in the Mail Server User Name box.</p> <p>Example: If you specified support as the Mail Server User Name, the To Address may be support@mycompany.com.</p>
Receiving Protocol	<p>Select the protocol used by the receiving mail server. You use the POP3 option to check the POP3 mail server for a sent message. You use the IMAP4 option to check the IMAP mail server for a sent message.</p>
Receiving E-Mail Server	<p>Type the hostname of the POP3/IMAP4 mail server that should receive the test message. This can be the same mail server to which the test message was sent.</p> <p>Example: mail.thiscompany.com</p>
Receiving E-Mail Server User Name	<p>Type a POP user account name on the receiving mail server. A test e-mail message is sent to this account and the Mail monitor logs in to the account and verifies that the message was received. No other mail in the account is touched; therefore you can use your own personal mail account or another existing account for this purpose.</p> <p>Example: support</p> <p>Note: If you use a mail reader that automatically retrieves and deletes messages from the server, there is a chance that the Mail Monitor won't see the mail message and therefore reports an error.</p>
Receiving E-Mail Server Password	<p>Type a password, if necessary, for the receiving mail account.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
RECEIVE ONLY Content Match	<p>Type a string of text to match against the contents of the incoming message. If the text is not contained in the incoming message, the monitor is in error. This is for the receiving only option. The search is case sensitive.</p> <p>Example: Subject:MySubject</p> <p>HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, < B> Hello< /B> World). This works for XML pages as well.</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an i after the trailing slash indicating case-insensitive matching.</p> <p>Example: /href=Doc\d+\.html/ or /href=doc\d+\.html/i</p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a regular expression.</p> <p>Example: /Temperature: (\d+)/</p> <p>This would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</p>
Timeout	<p>The number of seconds that the Mail monitor should wait for a mail message to be received before timing-out. Once this time period passes, the Mail monitor logs an error and reports an error status.</p>
POP Check Delay	<p>After SiteScope sends the test message, it immediately logs into the mail account to verify that the message has been received. If the message has not been received, SiteScope automatically waits 10 seconds before it checks again. You can adjust this wait time by indicating an alternate number of seconds to wait in this box.</p>

GUI Element	Description
Attachment	<p>Type the full path of a file to add as an attachment to the e-mail message. Use this option to check that your e-mail server can accept and forward messages with attached files. Optionally, you can use a regular expression to insert date and time variables to create a filename or file path.</p> <p>Example: s/C:\firstdir\\${shortYear}\${0month}\${0day\$}/</p>
Attachment Encoding	<p>If the attachment file content uses an encoding that is different than the encoding used on server where SiteScope is running, type the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the attachment file.</p> <p>Examples: Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.</p>
SMTP User	<p>Type the user name required for SMTP authentication if the SMTP server requires authentication before sending messages.</p>
SMTP Password	<p>Type the password for the SMTP authentication (if required).</p>
NTLM Authentication	<p>If NTLM authentication is used by the e-mail server, choose if you need version 1 or version 2.</p>

Microsoft Windows Dial-up Monitor Settings

Description	<p>The Windows Dial-up Monitor (available only on the Windows NT version of SiteScope) uses the Windows NT Remote Access Service to connect to an Internet Service Provider or Remote Access server and optionally runs a user-defined set of monitors. The monitor confirms that the dial-up connection can be established, and measures the performance of the connection and of the network services using the dial-up connection.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Microsoft Windows Dial-up Monitor Overview" on page 834

The Add/Edit Microsoft Windows Dial-up Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Phone Number	<p>Type the phone number for the dial-up account, adding any extra modem digits or pauses that are required.</p> <p>Example: 9,4432266 includes a "9," for getting an outside line. Insert a comma wherever you need a short pause.</p>
Account Login	The login name for the dial-up account.

GUI Element	Description
Account Password	The password for the dial-up account.
Monitor(s) to Run	<p>Select the groups and/or monitors that you want to run while the dial-up connection is established.</p> <p>Monitors that are used by Microsoft Windows Dial-up Monitors should not be scheduled to run by themselves because some of their data would be through the dial-up connection, and some of their data would be through the local connection.</p> <p>Make sure that the Update Every box for these monitors is blank.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	The timeout limits the total time that the Microsoft Windows Dial-up Monitor takes to connect, authenticate, and run each of its monitors. If the time ever exceeds this time, then the connection is hung up, and the monitor completes with a timeout error.

Network Bandwidth Monitor Settings

Description	<p>You use the Network Bandwidth Monitor to monitor SNMP-enabled network appliances such as routers and switches. The error and warning thresholds for the monitor can be set on one or more different objects. This monitor type also provides a Real-time metrics report, available as a link in the More column on the Group Detail Page.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Network Bandwidth Monitor Overview" on page 837

The Network Bandwidth Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Type the name of the server you want to monitor.
SNMP Version	Select the version of SNMP to use when connecting.
Community	Type the community string (valid only for version 1 or 2 connections).
SNMP V3 Authentication Type	Select the type of authentication to use for version 3 connections.
SNMP V3 Username	Type the user name for version 3 connections.
SNMP V3 Authentication Password	Type the authentication password to use for version 3 connections.
SNMP V3 Privacy Password	Type the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.
SNMP V3 Context Engine ID	Type a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.

GUI Element	Description
SNMP V3 Context Name	Type the Context Name to use for this connection. This is applicable for SNMP V3 only.
Timeout	Type the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. Default value: 5 seconds
Retries	Type the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. Default value: 1
Port	Type the port to use when requesting data from the SNMP agent. Default value: 161
Starting OID	Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered in this box. You should edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value did not enable retrieving any counters, then you may have to type a different value in this box. Default value: 1
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box. Select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Device Type	Select an optional device type for device specific monitoring. The default is Do not monitor device-specific metrics . By specifying a device type, you enable the Network Bandwidth monitor to watch certain device-specific metrics. For information about controlling the metrics associated with these device types and on adding new device types, see the section entitled Device Specific Metrics Config File.
Duplex or Half-Duplex	Select the duplex state to use when calculating percent bandwidth utilized for all selected interfaces on this device.

GUI Element	Description
Interface index	<p>Metrics for network interfaces on an SNMP-enabled device are presented as a table of management information (the ifTable), where each row corresponds to a different interface. Unfortunately, there is no requirement that the mapping from interface-to-row in this table remain constant across device reboots. The Interface Index parameter may help prevent the interfaces SiteScope is monitoring from becoming confused after a device restarts.</p> <p>The three possible options are:</p> <ul style="list-style-type: none"> ▶ Indexed by Interface Name. The ifDescr field of the ifTable is used to maintain monitoring consistency across device reboots. ▶ Indexed by Physical Address. The ifPhysAddr field of the ifTable is used to maintain monitoring consistency across device reboots. ▶ Indexed by ifTable Row Number. SiteScope assumes that the interfaces remain in the same row in the ifTable across device reboots. <p>Note: Some devices (Cisco, for instance) may have a configuration option to not jumble the position of interfaces in the ifTable during reboot. This may be the safest option, as not all interfaces may always have a unique ifDescr, and not all interfaces may have an ifPhysAddr (loopback interfaces do not typically have a physical address).</p>
Show Bytes In/Out	Select this option to display a graph for bytes in/out along with the percent bandwidth utilized on the Real-Time Metrics page.
Real-Time Data Vertical Axis	Type the maximum value on the vertical axis for real-time graphs (leave blank to have this automatically calculated by SiteScope).
Real-Time Data Time Window	Type the number of hours for which real-time graph data should be stored.

Ping Monitor Settings

Description	<p>The Ping Monitor checks the availability of a host by using the network. Use this monitor to check that your connection to the Internet is available.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Ping Monitor Overview" on page 838

The Add/Edit Ping Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Host Name	<p>Type the IP address or the name of the host that you want to monitor.</p> <p>Example: 206.168.191.21 or demo.thiscompany.com</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Time Out	The time, in milliseconds, that should pass before the ping times out. To change the threshold, type the new value in the text box. Default value: 5000 milliseconds
Packet Size	The size, in bytes, of the ping packets sent. To change the threshold, type the new value in the text box. Default value: 32 bytes

Port Monitor Settings

Description	<p>The Port Monitor verifies that a connection can be made to a network port and measures the length of time it takes to make the connection. Optionally, it can look for a string of text to be returned or send a string of text once the connection is made.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Port Monitor Overview" on page 839

The Add/Edit Port Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Host Name	Type the IP address or the name of the host that you want to monitor. Example: 206.168.191.21 or demo.thiscompany.com
Port Number	Choose the port number to connect to from the list of Commonly Used Ports , or type a port number in the Other Ports text box. Additional entries can be added to the list by editing the <code><SiteScope root directory>\groups\master.config</code> file.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Send String	Customize the string sent to the host after a connection is made.
Match String	Check for a string of text after a connection is made. If the text is not received, the monitor displays the message no match on content. Note: The search is case sensitive.
Timeout	The number of seconds that the Port monitor should wait for the connection to the port, and for any sending and receiving to complete. Once this time period passes, the Port monitor logs an error and reports an error status.

RTSP Monitor Settings

Description	<p>Real Time Streaming Protocol (RTSP) Monitor can be used to check the availability of certain kinds of time-based media files and real-time media streams.</p> <p>The RTSP Monitor does not support Real Media file types (for example, *.ra, *.ram files) or Windows Media files (for example, *.asf files). Use the Real Media Server Monitor and Real Media Player Monitor or the Microsoft Windows Media Server Monitor and Microsoft Windows Media Player Monitor (“Stream Monitors” on page 941) to monitor these types of services.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“RTSP Monitor Overview” on page 840

The Add/Edit RTSP Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Media URL	<p>Type the URL of the media file (for HTTP download and playback) or the URL of the media stream (for RTSP streaming) to be tested.</p> <p>Note: The RTSP Monitor may not process media reference files or media metadata files that are commonly used with RealNetworks RealPlayer reference files and with some QuickTime movies.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	<p>The time, in milliseconds, that should pass before the RTSP Monitor process is timed out. To change the threshold, type the new value in the text box.</p> <p>To test media files to completion, the Timeout value should be set to a value greater than the time that it should take to playback the subject media download.</p> <p>Example: If the media file should normally playback in 90 seconds, the Timeout value should be set for greater than 90 seconds.</p> <p>Default value: 60000 milliseconds</p>
Stop Time	<p>You can stop the media download after some specified amount of time has elapsed:</p> <ul style="list-style-type: none"> ▶ A value of 0 causes the media stream to download until end of media is detected. ▶ A value greater than 0 stops the download of continuous broadcast streams (such as radio station multicasts) or very large media streams.
Maximum for Gauge Measurement	<p>(Optional) Type a maximum value for the Object ID. The maximum is calculated to create the gauge display.</p>

SNMP Monitor Settings

Description	<p>The SNMP Monitor reads a value from an SNMP device. Many network devices support the SNMP protocol as a way of monitoring them. You must know the OIDs (Object ID's) for the device you want to monitor. These may be available in the product documentation or in the form of a MIB file.</p> <p>Note: To have SiteScope listen for SNMP traps from multiple devices, use the SNMP Monitor (see “SNMP Monitor Overview” on page 844).</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“SNMP Monitor Overview” on page 844

The Add/Edit SNMP Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Host Name	<p>Type the host name or IP address of the SNMP device that you want to monitor (for example, demo.thiscompany.com).</p> <p>Default value: 161</p> <p>If your SNMP device is using a different port, add it to the hostname using :port.</p> <p>Example: demo.SiteScope.com:170 (to use port 170)</p>

GUI Element	Description
Object ID	<p>Select the Object ID mnemonic from the drop-down list or type the Object Identifier (OID) for the SNMP value you want to retrieve. The OID specifies which value should be retrieved from the device.</p> <p>Example: 1.3.6.1.2.1.4.3</p> <p>To troubleshooting basic connectivity to the device and to confirm that the SNMP agent is active, select the system.sysDescr object from the drop-down list if other objects can not be found.</p> <p>Note: SiteScope version 7.1 and later supports SNMP version 1 and version 2. To send a trap using snmpv2, you must select the version number in the Advanced Settings section.</p> <p>If you receive the error message error - noSuchName, it means SiteScope was able to contact the device but the OID given is not know by the device. You must provide an OID that is valid to the device to obtain a value.</p> <p>If you have a MIB file for the device you want to monitor, you can copy the *.mib (or *.my) file into the <SiteScope root directory>\templates.mib subdirectory and use the MIB Help utility to compile the MIB and browse the OIDs for the device. To use the MIB Helper tool, select Tools > MIB Browser and type the connection details. After copying a new MIB file to SiteScope, SiteScope must be restarted. Select the MIB file to browse using the drop-down list. Click the browse button to show the OIDs from the selected MIB file. A tree is displayed that represents the chosen MIB on the specified server. You can browse that tree to find the OID that you want to monitor.</p> <p>Note: It is not necessary to browse a MIB file with the SiteScope Mib Helper to monitor a device. The MIB Helper is provided simply as a tool to help you discover OIDs available on a device, but it is not the only tool available. You can find other alternative tools on the Web (for example, MG-SOFT or iReasoning).</p>

GUI Element	Description
Index	<p>The index of the SNMP object. Values for an OID come as either scalar or indexed (array or table) values.</p> <ul style="list-style-type: none"> ➤ For a scalar OID, the index value must be set to 0. ➤ For an indexed or table value, you must provide the index (a positive integer) to the element that contains the value you want. For example, OID 1.3.6.1.2.1.2.2.1.17 is an indexed value that contains four elements. To access this second element of this OID you type an index of 2 in the Index text box. To access the fourth element, type an Index value of 4. <p>In some vendor specific MIB's, the indexed entries (often referred to in tables) can have compound index values. For example, the OID for the process entry table in a Sun Microsystems server MIB may be: .1.3.6.1.4.1.42.3.12.1.1. This indexed or table object may have up to eleven nodes with OIDs ranging from .1.3.6.1.4.1.42.3.12.1.1.1 to .1.3.6.1.4.1.42.3.12.1.1.11. Each of these nodes contains an indexed list of entries with index values that range from 0 to over 27300 where the Index value represents the process ID number used by the operating system (view examples using the ps -ef command in UNIX). In this example, the index values may not be consecutive from 0 to 27300.</p>
Community	<p>Type the Community string for the SNMP device.</p> <p>The Community string provides a level of security for a SNMP device. Most devices use public as a community string. However, the device you are going to monitor may require a different Community string to access it.</p> <p>If you try to monitor an SNMP agent through specific community, you must make sure that the SNMP agent is familiar with that community. For example, if you try to monitor a Windows 2003 server through public community, you must make sure that the SNMP agent has this community configured. Otherwise, the monitor cannot connect to the agent.</p> <p>Note: The field is valid only for version 1 or 2 connections.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	Type the total number of seconds SiteScope should wait for a successful reply.
SNMP Version (V1, V2, or V3)	Select the SNMP version used by the SNMP host you want to monitor. SiteScope supports SNMP version 1, version 2, and version 3.
Retry Delay	Type the number of seconds SiteScope should wait before retrying the request. It continues to retry at the interval specified here until the Timeout threshold is met. Default value: 1
Scaling	If you choose a scaling option from the Commonly Used Values list, SiteScope divides the returned value by this factor before displaying it. Alternatively, you can specify a factor by which the value should be divided in the Other Values text box.
Match Content	Use this item to match against an SNMP value, using a string or a regular expression or XML names.
Units	Type an optional units string to append when displaying the value of this counter.
Measurement Label	Type an optional text string to describe the measurement being made by the monitor.
Measure as Delta	Click this box to have SiteScope report the measurement as the difference between the current value and the previous value.
Measure as Rate per Second	Click this box to have SiteScope divide the measurement by the number of seconds since the last measurement.

GUI Element	Description
Percentage Base	Type a number or SNMP object ID in this box. If entered, the measurement is divided by this value to calculate a percentage. If an object ID is entered, the Index value from the Main Settings pane is used.
Measure Base As Delta	Select this option to have SiteScope calculate the Percentage Base as the difference between the current base and the previous base. Use this option when an SNMP object ID is used for Percentage Base and the object is not a fixed value.
Gauge Maximum	Type a maximum value for the Object ID. The maximum is calculated to create the gauge display (Optional).
SNMP V3 Username	If you are using SNMP version 3, type the user name to be used for authentication. Note: SiteScope only supports MD5 authentication for SNMP V3.
SNMP V3 Password	If you are using SNMP version 3, type the password to be used for authentication for SNMP V3.

SNMP Trap Monitor Settings

Description	<p>The SNMP Trap Monitor watches for SNMP Traps received by SiteScope from other devices. The agents for the SNMP enabled devices must be configured to send traps to the SiteScope server.</p> <p>Note: To have SiteScope query a specific device for a specific value, use the SNMP Monitor, “SNMP Monitor Overview” on page 844.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“SNMP Trap Monitor Overview” on page 845

The Add/Edit SNMP Trap Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Run Alerts	<p>Select the method for running alerts:</p> <ul style="list-style-type: none"> ▶ If For each SNMP Trap matched is chosen, then the monitor triggers alerts for every matching entry found. ▶ If Once, after all SNMP Traps have been checked is chosen, then the monitor counts up the number of matches and triggers alerts based on the Error if and Warning if thresholds defined for the monitor in the Advanced Settings section.

GUI Element	Description
Content Match	<p>Type the text to look for in SNMP Traps. Regular expressions may also be used in this box for pattern matching.</p> <p>All SNMP Traps received by SiteScope are logged to <SiteScope root directory>\logs\SNMPTrap.log file.</p> <p>Example: The following shows two traps received from one router and another trap received from a second router:</p> <pre>09:08:35 09/10/2001 from=router1/10.0.0.133 oid=.1.3.6.1.4.1.11.2.17.1 trap=link down specific=0 traptime=1000134506 community=public agent=router1/10.0.0.133 var1=The interface Serial1 is down</pre> <pre>09:08:45 09/10/2001 from=router1/10.0.0.133 oid=.1.3.6.1.4.1.11.2.17.1 trap=link up specific=0 traptime=1000134520 community=public agent=router1/10.0.0.133 var1=The interface Serial1 is up</pre> <pre>09:10:55 09/10/2001 from=router2/10.0.0.134 oid=.1.3.6.1.4.1.11.2.17.1 trap=enterprise specific specific=1000 traptime=1000134652 community=public agent=router2/10.0.0.134 var1=CPU usage is above 90%</pre> <p>The examples shown here may wrap across multiple lines to fit on this page. The actual traps are in a single extended line for each trap.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Match Value Labels	<p>Use this option to type labels for the matched values found in the trap. The match value labels are used as variables to access retained values from the Content Match expression for use with the monitor threshold settings.</p> <p>You can set up to four labels. The labels are used to represent any retained values from the Content Match regular expression in the parameters available for the status threshold settings (Error if, Warning if, and Good if). These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.</p> <p>Note: Separate multiple labels with a comma (,).</p>

SNMP by MIB Monitor Settings

Description	<p>The SNMP by MIB Monitor allows you to monitor objects on any SNMP agent. The error and warning thresholds for the monitor can be set on one or more different objects.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"SNMP by MIB Monitor Overview" on page 846

The Add/Edit SNMP by MIB Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Type the name of the server you want to monitor.
SNMP Version	Select the version of SNMP to use when connecting.
Community	Type the community string. If you try to monitor SNMP agent through a specific community, you must make sure that the SNMP agent is familiar with that community. If you try to monitor Windows 2003 server through public community, you must make sure that the SNMP agent has this community configured. Otherwise, the monitor cannot connect to the agent. Note: This is valid only for version 1 or 2 connections.
SNMP V3 Authentication Type	Select the type of authentication to use for version 3 connections.
SNMP V3 Username	Type the user name for version 3 connections.
SNMP V3 Authentication Password	Type the authentication password to use for version 3 connections.
SNMP V3 Privacy Password	Type the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.
SNMP V3 Context Engine ID	Type a hexadecimal string representing the Context Engine ID to use for this connection. Note: This is applicable for SNMP V3 only.
SNMP V3 Context Name	Type the Context Name to use for this connection. Note: This is applicable for SNMP V3 only.

GUI Element	Description
Timeout	Type the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.
Retries	Type the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.
Port	Type the port to use when requesting data from the SNMP agent. Default value: 161
Starting OID	Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered in this box. Default value: 1 Note: You should edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value of 1 did not enable retrieving any counters, then you may have to type a different value in this box.
MIB File	Select the MIB file which contains the objects you are interested in monitoring. If you select a specific MIB file, then only the objects described in that MIB file are displayed. If you select All MIBs , then all objects retrieved from the agent during the MIB traversal are displayed. If no MIB information is available for an object, it is still displayed but with no textual name or description. To make this monitor aware of new or additional MIBs, place new MIB files in the <SiteScope root directory>\templates.mib directory and restart SiteScope.

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box. Select the counters you want to monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Counter Calculation Mode	<p>Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. Calculations are either of the following:</p> <ul style="list-style-type: none"> ▶ a simple delta of the current value from the previous value ▶ a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements <p>Note: This option only applies to the aforementioned object types. An SNMP by MIB Monitor that monitors Counter objects as well as DisplayString objects only performs this calculation on the Counter objects.</p>

19

Server Monitors

This chapter includes the main concepts and reference information for monitoring server health and availability.

This chapter includes:

Concepts

- ▶ Browsable Windows Performance Counter Monitor Overview on page 892
- ▶ CPU Utilization Monitor Overview on page 893
- ▶ Disk Space Monitor Overview on page 894
- ▶ IPMI Monitor Overview on page 894
- ▶ Memory Monitor Overview on page 895
- ▶ Microsoft Windows Event Log Monitor Overview on page 897
- ▶ Microsoft Windows Performance Counter Monitor Overview on page 898
- ▶ Microsoft Windows Resources Monitor Overview on page 899
- ▶ Microsoft Windows Services State Monitor Overview on page 903
- ▶ Service Monitor Overview on page 904
- ▶ UNIX Resources Monitor Overview on page 906
- ▶ Web Server Monitor Overview on page 906

Reference

- ▶ Server Monitors User Interface on page 907

Browsable Windows Performance Counter Monitor Overview

Use the Browsable Windows Performance Counter Monitor to monitor the values of Windows performance statistics. Each time the Browsable Windows Performance Counter Monitor runs, it returns readings and a status message and writes them in the monitoring log file. The status is displayed in the group detail table for the monitor which represents the current value returned by this monitor. The status is logged as either OK or warning. A count of the number of counters that could not be read is also kept, and error conditions can be created depending on this count.

Note:

- ▶ The Browsable Windows Performance Counter Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ This monitor can only be added by deploying a Solution template or SiteScope Health. For information about using templates to deploy monitors, see “SiteScope Templates” on page 1189.
- ▶ This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

For details on configuring this monitor, see “Browsable Windows Performance Counter Monitor Settings” on page 908.

CPU Utilization Monitor Overview

Use the CPU Monitor to monitor the percentage of CPU time that is currently being used on the server. By monitoring CPU usage, you can prevent poor system response times and outages before they occur.

Whether the servers in your infrastructure are running with a single CPU or with multiple CPUs, you only need to create one CPU monitor per remote server. If you have multiple CPUs, SiteScope reports on the average usage for all of them, as well as each individual CPU usage.

Scheduling This Monitor

In general, the CPU Monitor does not need to be run as often as some of the other monitors. If you do not usually suffer from CPU problems, you can run it less frequently, perhaps every half hour or so. If you are prone to CPU usage problems, you should run it more frequently. All machines have short spikes of CPU usage, but the primary thing that you are looking for is high usage on a regular basis. This indicates that your system is overloaded and that you need to look for a cause.

Status

The Status reading is the current value returned by this monitor; for example, 68% used. SiteScope displays an average for multiple CPU systems. On NT, this is the average CPU usage between runs of the monitor. On UNIX, this is the instantaneous CPU when the monitor runs.

The status is logged as either OK or warning. A warning status is returned if the CPU is in use more than 90% of the time.

For details on configuring this monitor, see “CPU Utilization Monitor Settings” on page 910.

Disk Space Monitor Overview

Use the Disk Space Monitor to monitor the amount of disk space that is currently in use on your server. Having SiteScope verify that your disk space is within acceptable limits can save you from a crashed system and corrupted files.

The disk space monitor does not require many resources, so you can check it as often as every 15 seconds, but every 10 minutes should be sufficient. You may want to have SiteScope run a script (using a Script Alert) that deletes all files in certain directories, such as /tmp, when disk space becomes constrained. For details on using a Script Alert, see “Working with Script Alerts” on page 1402.

For details on configuring this monitor, see “Disk Space Monitor Settings” on page 912.

IPMI Monitor Overview

The Intelligent Platform Management Interface (IPMI) provides an interface for reporting on device operations, such as whether fans are turning and voltage flowing within server hardware. You use the IPMI Monitor to monitor server and network element platforms to get a more complete view of component health and operation statistics for IPMI enabled devices running version 1.5.

You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch key operational factors that can seriously effect availability and degrade performance. Create a separate monitor instance for each server you are running.

System Requirements

The following are requirements for using the IPMI Monitor:

- ▶ The device you want to monitor has to be IPMI-enabled. In most cases, this means that the device must be designed for IPMI sensing and include a separate, dedicated IPMI network adapter. The monitor supports IPMI version 1.5 only.
- ▶ You must know the IP address of the IPMI network adapter for the device you want to monitor. In many cases, this IP address is different than the IP address used for other network communication to and from the device. Use an applicable IPMI utility to query for the IP address or contact the applicable system administrator.

For details on configuring this monitor, see “IPMI Monitor Settings” on page 914.

Memory Monitor Overview

Memory is one of the primary factors that can affect your Web server's performance. Use the Memory Monitor to monitor how much virtual memory is currently in use on a server. The two most important measurements to detect problems in this area are Pages per Second and Percentage of Virtual Memory Used. Each time the Memory Monitor runs, it returns a status message and writes it in the monitoring log file.

Scheduling This Monitor

In most environments, the Memory Monitor does not put a heavy load on your server. For monitoring remote UNIX servers, SiteScope usually needs to open a telnet or SSH connection to the remote server. While the monitor actions generally do not load the either server, managing a large number of remote connections can results in some performance problems. You use the error and warning thresholds to have SiteScope notify you if memory on a remote server starts to get low.

Common Problems and Solutions

Pages per second measures the number of virtual memory pages that are moved between main memory and disk storage. If this number is consistently high (>10 pages/sec), system performance is being affected. One solution is to add more memory. Another solution is to turn off non-critical services that are using memory, or move these services to a different machine. The SiteScope Service Monitor measures the memory usage for each service.

Percentage of Virtual Memory Used measures the percentage of memory and paging file space used. If this number reaches 100%, services that are running may fail and new ones are unable to start. Increasing the size of the paging file may solve the immediate problem but may decrease performance by increasing paging. A slow increase in Virtual Memory Used is often caused by a memory leak in a service.

Use the **Processes** tool, available from the **Tools** container in the monitor tree, to view the memory used by each service. The ideal solution is to install an upgraded version of the service without the leak. An interim solution is to use the Service Monitor to measure the service size and run a SiteScope Script Alert to restart the service when it becomes too large. If restarting the service does not fix the leak, it may be necessary to add a Script Alert to restart the server when memory usage is too high. For details on using a Script Alert, see “Working with Script Alerts” on page 1402. For details on using the Service Monitor, see “Service Monitor Overview” on page 904.

When deploying the Memory monitor on a remote UNIX machine, the monitor displays swap memory usage and not virtual memory usage. To monitor virtual memory usage, deploy the UNIX Resources monitor. For details, see “UNIX Resources Monitor Overview” on page 906.

For details on configuring this monitor, see “Memory Monitor Settings” on page 915.

Microsoft Windows Event Log Monitor Overview

Use the Microsoft Windows Event Log Monitor to monitor added entries in one of the Microsoft Windows Event Logs (System, Application, or Security). The Microsoft Windows Event Log Monitor examines only log entries made after the time that the monitor is created. Each time the monitor runs thereafter, it examines only those entries added since the last time it ran. You can choose to filter out messages that are not important by using the boxes listed under Advanced Settings to specify values that must appear in the event entry for the entry to match.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

When setting up SiteScope alerts for Microsoft Windows Event Log Monitors that are set to alert **for each event matched**, it is most useful to select the NTEventLog template for the e-mail, pager, SNMP, or script alert. This alert template sends the alert with the event entry fields broken out. The type of SiteScope alert triggered depends on the type of the log event entry:

Event Log Entry Type	SiteScope Alert Type
Error	Error
Warning	Warning
Information	OK

Each time the Microsoft Windows Event Log Monitor runs, it returns a reading and status message and writes them in the `<SiteScope install path>\SiteScope\logs\SiteScopeyyyy_mm_dd.log` file.

Status

The status for the Microsoft Windows Event Log Monitor includes the number of entries examined, and the number of entries matched. If an interval is specified, the number of events in that interval is also displayed. Matched entries and interval entries can trigger alerts.

For details on configuring this monitor, see “Microsoft Windows Event Log Monitor Settings” on page 917.

Microsoft Windows Performance Counter Monitor Overview

Use the Microsoft Windows Performance Counter Monitor to monitor the values of any Windows performance statistic. Each time the Microsoft Windows Performance Counter Monitor runs, it returns a reading and a status message and writes them in the monitoring log file. The status is displayed in the group detail table for the monitor which represents the current value returned by this monitor. The status is logged as either OK or warning. An error occurs if the counter could not be read.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

For details on configuring this monitor, see “Microsoft Windows Performance Counter Monitor Settings” on page 923.

Microsoft Windows Resources Monitor Overview

Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. This allows you to watch server loading for performance, availability, and capacity planning. You can monitor multiple parameters or counters on a single, remote server with each monitor instance. Create one or more Microsoft Windows Resources Monitor instances for each remote server in your environment.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

The Microsoft Windows Resources Monitor uses performance counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you must define the connection to these servers under the Microsoft Windows Remote Preferences option in the SiteScope Preferences container. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.

You can create a Server-Centric Report for the Windows server by clicking the server name in the Target column of the row corresponding to the Microsoft Windows Resources Monitor in Dashboard. For details, see “Server-Centric Report” on page 440.

If you need to develop a XSLT file to transform the XML content for this monitor, SiteScope includes a Tools page you can use to verify the transformation output. For more information, see the section “XSL Transform Tool” on page 1634.

Note: When monitoring Windows servers configured using SSH, you must use the **Direct Registry Queries** option for the **Collection Method** in the Advanced Settings area when you configure the monitor.

Configuring the Microsoft Windows Resources Monitor to Run on Windows 2003 as a Non-Administrator User

For the Microsoft Windows Resources Monitor to monitor a Windows 2003 machine if the SiteScope user account is not in the Administrators group, you must either:

- ▶ Use the same domain account on both the SiteScope and the remote monitored system, or
- ▶ Use local accounts on both systems, provided that the user accounts have the same name and password and are always synchronized on both systems. You cannot use **Local System** or other similar system predefined accounts that do not enable you to specify a password for them.

In addition, you must configure the user account settings on SiteScope and the remote monitored machine to log on using the selected non-administrator user account (domain or local account). You can then use a standard Windows perfmon utility to verify that it works.

To configure user account settings on SiteScope:

- 1** In the **Services** control panel, right-click the **SiteScope** service, and then click **Properties**. The SiteScope Properties dialog box opens.
- 2** Click the **Log On** tab, and configure the user account to log on using the selected non-administrator user account (domain or local account).

To configure user account settings on the remote monitored machine:

- 1** Check that you can access the remote machine. Perform a ping test and check DNS resolves the server name with its IP address.

It is also recommended that you check there are no other network-related problems by using the selected user account to map a network drive of the monitored machine to the drive used on the SiteScope machine.

- 2** In the **Services** control panel, check that the **RemoteRegistry** service is running and that the selected user account has access to it. You can use the following command from the Windows 2003 Resource Kit (run it under an administrator account):

```
subinacl /service RemoteRegistry /grant=tester=f
```

This command grants **Full Access** to the RemoteRegistry service for the local user **tester**.

- 3** Add the domain or local user account to be used into the **Performance Monitor Users** and **Performance Log Users** local user groups. Make sure that these groups have at least read permissions for the following registry key (and all its subkeys):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib]
```

Tip: To check read permissions, select **Start > Run**, and type **Regedt32.exe**. In the Registry Editor, select the registry key, click **Security**, and select **Permissions**. In the Name pane, highlight the user SiteScope uses to access the remote machine, and make sure that the **Allow** check box for **Read** is selected in the **Permissions** pane.

- 4 Make sure that the domain or local user account to be used has at least read permissions on the following objects:
 - Registry key:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg]
 - Files in %WINDIR%\System32\perf?XXX.dat, where XXX is the basic language ID for the system. For example, 009 is the ID for the English version.

Note: If the required Performance Counter Library Values are missing or are corrupted, follow the instructions in Microsoft knowledge base article KB300956 (<http://support.microsoft.com/kb/300956/en-us>) to manually rebuild them.

To verify that the non-administrator user account works:

- 1 Launch a standard Windows perfmon utility. You can either:
 - Launch it interactively when logged on to the SiteScope machine with the selected user account by typing perfmon.
 - Launch it when logged on to the SiteScope machine with some other account through the RunAs command, which allows you to launch commands under different user account. Type the following command:

```
runas /env /netonly /user:tester "mmc.exe perfmon.msc"
```

Then type the password (in this example, for the tester account), and the command is run under the tester user account.
- 2 After the Performance window opens, right-click in the right graph area and select **Add Counters**. The Add Counters dialog box opens.

- 3 Select **Choose counters from computer** and type the remote monitored machine name or its IP address in the box.
- 4 Press the TAB key. If the perfmon utility is able to connect to the remote machine, the Performance object box is filled in with the performance objects that can be monitored from the remote machine.

For details on configuring this monitor, see “Microsoft Windows Resources Monitor Settings” on page 927.

Microsoft Windows Services State Monitor Overview

Use the Microsoft Windows Services State Monitor to monitor the services installed and running on remote Windows servers. By default, the monitor returns a list of all of the services that are set to be run automatically on the remote server. You can filter the list of services returned by the monitor using regular expressions. The monitor displays the number of services running and related statistics along with a summary listing of the services installed on the remote server.

Note:

- This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).
 - The Microsoft Windows Services State Monitor only retrieves a list of installed services. It does not query the list of processes that may be running on the remote machine (use the Service Monitor for this).
-

To use this monitor to create event alerts, configure alert definitions associated with this monitor to alert **Once, after the condition has occurred exactly 1 times**. This is because the Microsoft Windows Services State Monitor only signals a change in state for services relative to the previous run of the monitor. For example, if the monitor is set to signal an error if a service has changed from running to not running, the monitor only signals an error status for one monitor run cycle. The number of services running and not running is reset for each monitor run and this number is used for comparison with the next monitor run.

For details on configuring this monitor, see “Microsoft Windows Services State Monitor Settings” on page 931.

Service Monitor Overview

The Service Monitor verifies that specific processes are listed as running, and optionally, it can also check to see how much CPU a process is using. If a process that should be running does not show up or if it is using too much memory, SiteScope can either alert you to the problem so that you can address it yourself, or it can run a script to automatically restart the process to help minimize the effect on other operations and downtime.

You should create a Service Monitor for any service or process that should be running on a consistent basis. You can also create a Script Alert that restarts the service automatically if the service monitor in SiteScope cannot find it. The **restartService.bat** script, located in the **<SiteScope root directory>\scripts** directory, is a template that you can customize to create a script for SiteScope to run in the event your monitor fails. For details on using a Script Alert, see “Working with Script Alerts” on page 1402.

Scheduling This Monitor

The Service Monitor does not put a heavy load on your server. For monitoring remote UNIX servers, SiteScope usually needs to open a telnet or SSH connection to the remote server. While the monitor actions generally do not load the either server, managing a large number of remote connections can results in some performance problems. You probably want to monitor critical services and services that have a history of problems every five minutes or so. Less critical services and processes should be monitored less frequently.

Status

Each time the Service Monitor runs, it returns a reading and a status message and writes them in the monitoring log file.

The reading is the current value of the monitor. For this monitor, the possible readings are:

- ▶ Running
- ▶ Not found

The status is logged as either OK or error. An error status is returned if the service is not found.

For details on configuring this monitor, see “Service Monitor Settings” on page 934.

UNIX Resources Monitor Overview

Use the UNIX Resources Monitor to monitor the server system statistics on UNIX servers. You can monitor multiple parameters or measurements with a single monitor instance. This allows you to monitor the remote server for loading, performance, and availability at a basic system level. See the list of example system measurements that can be monitored. Create a separate UNIX Resources monitor instance for each UNIX server in your environment.

The UNIX Resources Monitor queries the list of UNIX servers currently configured in the UNIX Remote Preferences container. To monitor a remote UNIX server, you must define a UNIX Remote connection profile for the server before you can add a UNIX Resources Monitor for that server. For details, see “UNIX Remote Preferences” on page 220.

You can create a Server-Centric Report for the UNIX Server by clicking the server name in the Target column of the row corresponding to the UNIX Resources Monitor in Dashboard. For details, see “Server-Centric Report” on page 440.

For details on configuring this monitor, see “UNIX Resources Monitor Settings” on page 937.

Web Server Monitor Overview

The Web Server Monitor gathers information about a Web Server by reading the server log files. Using this information, you can see how busy your Web site is, and plan hardware upgrades and configuration changes to improve performance.

It is most effective if you create a separate Web Server Monitor for each Web server you are running. If you are running multiple Web servers, each one should have its own log file so that SiteScope can report on them separately. For information about what data is recorded, see “SiteScope Log File Columns” on page 383.

For details on configuring this monitor, see “Web Server Monitor Settings” on page 939.

Server Monitors User Interface

This section describes:

- [Browsable Windows Performance Counter Monitor Settings on page 908](#)
- [CPU Utilization Monitor Settings on page 910](#)
- [Disk Space Monitor Settings on page 912](#)
- [IPMI Monitor Settings on page 914](#)
- [Memory Monitor Settings on page 915](#)
- [Microsoft Windows Event Log Monitor Settings on page 917](#)
- [Microsoft Windows Performance Counter Monitor Settings on page 923](#)
- [Microsoft Windows Resources Monitor Settings on page 927](#)
- [Microsoft Windows Services State Monitor Settings on page 931](#)
- [Service Monitor Settings on page 934](#)
- [UNIX Resources Monitor Settings on page 937](#)
- [Web Server Monitor Settings on page 939](#)

Browsable Windows Performance Counter Monitor Settings

Description	<p>The Browsable Windows Performance Counter Monitor tracks the values of Windows performance statistics. These are the same statistics that can be viewed using the Performance Monitor application under Windows.</p> <p>This monitor is only available on the Windows version of SiteScope.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<ul style="list-style-type: none"> ▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ▶ This monitor can only be added by deploying a Solution template or SiteScope Health. For more information, see “SiteScope Templates” on page 1189 and “SiteScope Server Health” on page 365. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. ▶ Monitors must be created in a group in the monitor tree.
Useful Links	<p>“Browsable Windows Performance Counter Monitor Overview” on page 892</p>

The Add/Edit Browsable Windows Performance Counter Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Choose the server where the performance counters you want to monitor are found. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.
Counter File	Choose the file that contains a list of counters from which to choose to monitor. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope. The files in this list all reside in the <code><SiteScope root directory>\templates.perfmon\browsable</code> directory under SiteScope. There are a number of default files in the standard SiteScope distribution.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

CPU Utilization Monitor Settings

Description	<p>Reports the percentage of CPU time that is currently being used on the server.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none">▶ In the monitor tree, right-click a group and select Add Monitor.▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"CPU Utilization Monitor Overview" on page 893

The Add/Edit CPU Utilization Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the CPU utilization you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to type or select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.

Disk Space Monitor Settings

Description	<p>Track how much disk space is currently in use on your server.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Disk Space Monitor Overview" on page 894

The Add/Edit Disk Space Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the disk space you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to select a server name.

GUI Element	Description
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	<p>Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.</p>
Disk	<p>Select the disk drive that you want to monitor from the list.</p> <p>Note: Disk performance counters are unavailable by default in standard Windows 2000 installations. In order for you to monitor disk drives using the SiteScope Disk Monitor on servers running Windows 2000, you must enable these disk counters. Use the <code>diskperf -y</code> command line on each Win2000 machine you want to monitor disk space and then reboot each server. You should then be able to select the disk drives for those servers in the SiteScope Disk Monitor form.</p>

IPMI Monitor Settings

Description	<p>Monitors component health and operation statistics for Intelligent Platform Management Interface (IPMI) enabled devices running version 1.5.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"IPMI Monitor Overview" on page 894

The IPMI Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server Name	<p>Type the IPMI server name or IP address of the IPMI network adapter.</p> <p>Note: The IP address is normally not the same as the ordinary ethernet NIC adapter address.</p>
Port Number	<p>Type the port number of the IPMI device.</p> <p>Default value: 623</p>
User Name	Type the user name to access the IPMI server.
Password	Type the password to access the IPMI server.

GUI Element	Description
Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.</p>
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Memory Monitor Settings

Description	<p>The Memory Monitor provides a tool for you to track how much virtual memory is currently in use on a server. Running out of memory can cause server applications to fail and excessive paging can have a drastic effect on performance.</p> <p>Use this page to add a monitor or edit the monitor’s properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“Memory Monitor Overview” on page 895

The Memory Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the memory you want to monitor is running. You cannot directly edit this box. The default is to monitor memory on the server on which SiteScope is installed. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.

Microsoft Windows Event Log Monitor Settings

Description	<p>The Microsoft Windows Event Log Monitor watches one of the Microsoft Windows Event Logs (System, Application, or Security) for added entries.</p> <p>This monitor is only available on the Windows version of SiteScope.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Microsoft Windows Event Log Monitor Overview" on page 897

The Add/Edit Microsoft Windows Event Log Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the event log you want to monitor is running. You cannot directly edit this box. The default is to monitor the server on which SiteScope is installed. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.

GUI Element	Description
Log Name	Choose from the following logs: <ul style="list-style-type: none"> ▶ System ▶ Application ▶ Security ▶ Directory Service ▶ DNS ▶ File Replication Service <p>Note: This is a static list of those logs available when deploying this monitor. These log files do not necessarily exist on the server you are monitoring.</p>
Event Type	Select the event type: <ul style="list-style-type: none"> ▶ Any ▶ Error ▶ Warning ▶ Error or Warning ▶ Information
Run Alert	Select the method for running alerts. <ul style="list-style-type: none"> ▶ If for each event matched is chosen, then the monitor triggers alerts for every matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error). ▶ If once, after all events have been checked is chosen, then the monitor counts up the number of matches and triggers alerts.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Source and ID Match	<p>Type the match string identifying the source of the event and the event ID in the form: <Event Source>:<Event ID>.</p> <p>Example: Type Print:20 to match event source named Print and event ID of 20.</p> <p>To match against all events from a specific source, type just the event source name.</p> <p>Example: W3SVC</p> <p>To match an exact event ID from an event source, specify both.</p> <p>Example: Service Control Mar:7000</p> <p>You can also use a regular expression for more complex matches. You can also use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 1618.</p>

GUI Element	Description
<p>Source and ID NOT Match</p>	<p>Type the match string identifying the source of the event to NOT MATCH in the form: <Event Source>:<Event ID>.</p> <p>Example: Print:20 ignores all events of Print source and event ID 20.</p> <p>To ignore all events from a particular source, specify just the source name. Example: W3SVC</p> <p>To ignore an exact event ID from an event source, specify both. Example: Service Control Mar:7000</p> <p>You can also use a regular expression for a more complex NOT MATCH. Example:</p> <ul style="list-style-type: none"> ▶ to ignore all Perflib sources from 200 to 299 use: /Perflib:2\d\d/ ▶ to ignore all events from the Perflib source, use: Perflib:* <p>You can also use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 1618.</p>
<p>Description Match</p>	<p>Type the text string to match against the description text for the event entry. The description text is the same as the description that is displayed when viewing the detail of an event log entry in the Windows Event Viewer. You can also type a regular expression in this box to match on patterns. You can also use the Regular Expression Test tool to check your regular expressions.</p>

GUI Element	Description
Description Not Match	<p>Microsoft Windows Event Log Monitor triggers an alert only if the text entered in this box does not appear in the event entry's description text.</p> <p>The description text can be viewed in the detail view of the event log entry by using the Windows Event Viewer.</p> <p>You can also type a regular expression in this box to match on patterns. You can also use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 1618.</p>
Event Category	Match the category number of the event entry.
Event Machine	Match against the machine that added the entry to the log file.
Interval	<p>Type an time period, in minutes, for which matching event log entries are totaled. This is useful when the case you are interested in is a quantity of events happening in a given time period.</p> <p>Example: If you wanted to detect a succession of service failures, 3 in the last 5 minutes, you would specify 5 minutes for the interval, and then change the Error If threshold to matches in interval >= 3.</p>

Microsoft Windows Performance Counter Monitor Settings

Description	<p>The Microsoft Windows Performance Counter Monitor tracks the values of any Windows performance statistic. These are the same statistics that can be viewed using the Performance Monitor application under Windows.</p> <p>This monitor is only available on the Windows version of SiteScope.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Microsoft Windows Performance Counter Monitor Overview" on page 898

The Add/Edit Microsoft Windows Performance Counter Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	<p>The server on which you want to monitor Windows performance statistics. You cannot directly edit this box. The default is to monitor the server on which SiteScope is installed. Use the Get Servers button to select a server name.</p> <p>When using a settings file from the Microsoft Windows Performance Counter Monitor, all counters are measured on the server specified by this entry.</p>
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>

GUI Element	Description
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.
Perfmon Chart File	<p>Select the Microsoft Windows Performance Counter Monitor setting file you want to use for your settings. These files can be saved in the Microsoft Windows Performance Counter Monitor (perfmon) and have either a .pmc or .pmw extension. On Windows 2000 Platform these can be saved using the .htm format. The files in this list all reside in the <SiteScope root directory>\templates.perfmon directory under SiteScope. There are a number of default files in the standard SiteScope distribution.</p> <p>Note: If you make your own settings file, it must be placed in the <SiteScope root directory>\templates.perfmon directory. You can optionally specify the settings directly for a single counter below under the Advanced Settings section.</p> <p>If you create your own .pmc file, any server specified in the .pmc file is ignored by SiteScope. The server to be queried is the one selected by using the Server selection box on monitor setup page (see above). Therefore, do not include identical counters directed at different servers in a single .pmc file. One .pmc file can be used by more than one Microsoft Windows Performance Counter Monitor instance, but any single instance of the Microsoft Windows Performance Counter Monitor only queries one server regardless of the servers assigned in the .pmc.</p> <p>If you have specified the settings directly in the Advanced Settings section, this list displays (Custom Object).</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Object	The Object is the same as the "Object" in the Performance Monitor application - just type it in this box. The Object is the high level item that is measured, such as Processor or Server. The object name is case sensitive. If you are using a Performance Monitor file for counter settings, leave this item blank.
Counter	The counter is the same as the "Counter" in the Performance Monitor application - just type it in this box. The Counter is the specific aspect of the Object that is measured, such as Interrupts/sec. The counter name is case sensitive. If you are using a Performance Monitor file for counter settings, leave this item blank.
Instance	Some counters can have multiple instances - for example, on machines with two CPUs, there are two instances of the Processor object. The instance is the same as the "Instance" in the Performance Monitor application - just type it in this box. Note that the instance name is case sensitive. If you are using a Performance Monitor file for counter settings, leave this item blank.
Units	If you want units to be displayed with the counter's values to make them more readable, type the units here.
Scale	If you want the raw performance counter value scaled to make it more readable, select the scale here. The raw value of the counter is multiplied by the scale to determine the value of the monitor. The kilobytes option divides the raw value by 1,024 (the number of bytes in 1 K), and the megabytes option divides the raw value by 1,048,576 (the number of bytes in 1 MB). If there are multiple counters specified by using a Performance Monitor file, this scaling applies to all counters.

Microsoft Windows Resources Monitor Settings

<p>Description</p>	<p>The Microsoft Windows Resources Monitor allows you to monitor system performance data using the Performance Data Helper (PDH) interface on Windows systems. The error and warning thresholds for the monitor can be set on one or more performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p>Useful Links</p>	<p>"Microsoft Windows Resources Monitor Overview" on page 899</p>

The Add/Edit Microsoft Windows Resources Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the Microsoft Windows Resources Monitor you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>

GUI Element	Description
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.
Get Measurements	<p>Click to open the list of available measurements, and select the objects, instances, and counters you want to check with the Microsoft Windows Resources Monitor.</p> <p>The performance parameters or counters available for the Microsoft Windows Resources Monitor vary depending on what operating system options and applications are running on the remote server.</p> <p>The Selected Measurements list displays the measurements currently selected for this monitor.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Collection Method	<p>Select the collection method from the following options:</p> <ul style="list-style-type: none"> ▶ Windows PDH Library. This is the default and most common option. ▶ Use Global Setting. Instructs the monitor to use the value configured in the master.config file for the _wrmCollectionMethod property. If this property has not been added to the master.config file, the default option is used. ▶ Direct Registry Queries. Use this option if Windows PDH library is not accessible or if the monitor is having trouble using the Windows PDH library. You must use this option when monitoring Windows servers configured using SSH.
Enable Server Centric Report	<p>Select to enable collecting data specifically for generating the Server-Centric Report. The report displays various measurements for the server being monitored. For details, see “Generating a Server-Centric Report” on page 416.</p>

 **Microsoft Windows Services State Monitor Settings**

Description	<p>The Microsoft Windows Services State Monitor is used to monitor a list of services running on Windows systems and report changes in the number of services that are running and list the services that changed state.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none">▶ In the monitor tree, right-click a group and select Add Monitor.▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Microsoft Windows Services State Monitor Overview" on page 903

The Add/Edit Microsoft Windows Services State Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server you want to monitor. You cannot directly edit this box. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Services to Include	<p>Type an optional regular expression to filter the list of services returned by the monitor.</p> <p>Default value: All of the services detected on the remote machine.</p> <p>When you use a regular expression to filter the list of services, the monitor calculates changes in state (that is, running or not running) based only on the services matched by the regular expression.</p> <p>Examples of services which can be monitored are:</p> <ul style="list-style-type: none"> ➤ Services added ➤ Services changed to not running ➤ Services changed to running ➤ Services currently not running ➤ Services currently running ➤ Services deleted ➤ Services last running ➤ Number of services added ➤ Number changed to not running ➤ Number of services currently not running ➤ Number of services currently running ➤ Number of services deleted

GUI Element	Description
Services to Ignore	Type an optional regular expression to filter the list of services matched by the expression used in the Services to Include setting. When you use a Services to Ignore regular expression to filter the list of Services to Include , the monitor calculates changes in state (that is, running or not running) based only on the services matched by the Services to Ignore regular expression.
Include Driver Services	Select this box to have the monitor include all low-level driver services. This generally increases the size of the list. You use the Services to Include and Service to Ignore options to filter the list of services returned using this option.

Service Monitor Settings

Description	<p>The Service Monitor checks to see if a service (Windows environment) or a specific process (UNIX and Windows) is running. There are many services or processes that play an important role in the proper functioning of your server, including Web server, Mail, FTP, News, Gopher, and Telnet. Web environments which support e-commerce transactions may have other important processes that support data exchange.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Service Monitor Overview" on page 904

The Add/Edit Service Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the service you want to monitor is running. You cannot directly edit this box. The default is to monitor services on the server on which SiteScope is installed. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>

GUI Element	Description
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.
Service	<p>Select the service (or process in UNIX) that you want to monitor from the System Services list.</p> <p>To monitor a service other than those listed, type the name of the service in the Other Service box.</p> <p>To monitor an NT process, select (Using Process Name) in the drop-down list and type the name in the Process Name text box (Advanced Settings pane).</p> <p>Note: The CPU % counter is relevant for processes and not for services, and it is displayed only if the selected service is by process name.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Process Name (NT Only)	<p>If you want to get information about the percentage of CPU being used by a specific process and/or the number of a specific type of process running, type the name of the process here.</p> <p>Note: The name of the process must be as it appears in NT Task Manager.</p> <p>Example: explorer.exe</p>
Measure Process Memory Use (UNIX Only)	Select this box if you want SiteScope to report the amount of virtual memory being used by a specific process.

Threshold Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Error if/ Warning if/ Good if	The CPU % measurement is relevant only for processes and not for system services. If the selected service is a process name, CPU % measurement is in the drop-down list. If the selected service is a system service, such as Event Log, CPU % measurement is not listed.

UNIX Resources Monitor Settings

Description	<p>The UNIX Resources Monitor enables you to monitor multiple system statistics on a single UNIX system. The error and warning thresholds for the monitor can be set on one or more server system statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"UNIX Resources Monitor Overview" on page 906

The Add/Edit UNIX Resources Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	Choose the server you want to monitor. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.
Get Measurements	Click to open the list of available measurements, and choose the server system measurements you want to check with the UNIX Resources Monitor. The Selected Measurements list displays the measurements currently selected for this monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Enable Server Centric Report	Select to enable collecting data specifically for generating the Server-Centric Report. The report displays various measurements for the server being monitored. For details, see “Generating a Server-Centric Report” on page 416.

Web Server Monitor Settings

Description	<p>The Web Server Monitor reports information about a Web server by reading the server log files. Each time the Web Server Monitor runs, it writes the current hits per minute and bytes per minute in the monitor status string and in the SiteScope logs.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Web Server Monitor Overview" on page 906

The Add/Edit Web Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server (for SiteScope running on Windows)	<p>The server where the Web Script instance you want to monitor is running. Type the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. These are the remote servers that are available to SiteScope. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor.

GUI Element	Description
Web Server	Select a Web server type for the selected Web server from the list of accessible server types.
Log File Pathname (for SiteScope running on UNIX/Linux)	To monitor Web server statistics on UNIX servers, type the full path of the Web server log file. Optionally, you can use a regular expression to insert date and time variables using SiteScope date variables. Example: s /firstdir/\$shortYear\$\$0month\$\$0day\$ inserts SiteScope's date and time variables.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Log File Pathname	If your Web server does not appear in the Web Server list, you may still monitor it by entering the full path to the Web server log file. Example: c:/ns-home/httpd-test/logs/access For servers that dynamically create the filename for log files, you can include regular expression as part of the log file path definition. The SiteScope can then retrieve data from a range of filenames based on evaluation of the regular expressions.
Request Size Column	If your Web server saves information in a custom format. Type the column number which contains the Request Size. If this item is blank, the common log file format is assumed.

20

Stream Monitors

This chapter includes the main concepts and reference information for monitoring applications that play media files and stream data.

This chapter includes:

Concepts

- ▶ Microsoft Windows Media Player Monitor Overview on page 942
- ▶ Microsoft Windows Media Server Monitor Overview on page 943
- ▶ Real Media Player Monitor Overview on page 944
- ▶ Real Media Server Monitor Overview on page 944

Reference

- ▶ Stream Monitors User Interface on page 945

Microsoft Windows Media Player Monitor Overview

Use the Microsoft Windows Media Player Monitor to monitor availability and delivery quality parameters for media files and streaming data compatible with Windows Media Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to report on delivery performance. Create a separate monitor instance for files or data streams that are representative of the content available from the site you want to monitor.

Note:

- ▶ This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).
- ▶ You should only monitor video, not audio, streams with this monitor.

You must have an instance of Windows Media Player installed on the machine where SiteScope is running to use this monitor.

For a list of the Media Player performance parameters or counters you can check with the Microsoft Windows Media Player Monitor, see “Performance Counters” on page 947.

For details on configuring this monitor, see “Microsoft Windows Media Player Monitor Settings” on page 946.

Microsoft Windows Media Server Monitor Overview

Use the Microsoft Windows Media Server Monitor to monitor the server performance parameters for Microsoft Windows Media Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Windows Media Server you are running.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

The Microsoft Windows Media Server Monitor uses performance counters to measure application server performance. SiteScope must be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you must define the connection to these servers under the Microsoft Windows Servers container in the SiteScope Preferences. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.

For details on configuring this monitor, see “Microsoft Windows Media Server Monitor Settings” on page 949.

Real Media Player Monitor Overview

Use the Real Media Player Monitor to monitor availability and delivery quality parameters for media files and streaming data compatible with RealNetworks Real Media Players. You can monitor multiple parameters or counters with a single monitor instance. This allows you to report on delivery performance. Create a separate monitor instance for files or data streams that are representative of the content available from the site you want to monitor.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

Before you can use the Real Media Player Monitor, Real Media Player client libraries must be installed on the server where SiteScope is running. Normally, it is sufficient to download and install a Real Media Player client on the server.

For details on configuring this monitor, see “Real Media Player Monitor Settings” on page 951.

Real Media Server Monitor Overview

Use the Real Media Server Monitor to monitor the server performance parameters for RealNetworks Real Media Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each RealSystem Server you are running.

Note: This monitor is supported on Windows versions of SiteScope only (the platform of the servers being monitored is irrelevant).

The Real Media Server Monitor makes use of Performance Counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you must define the connection to these servers under the Microsoft Windows Remote Preferences option in the SiteScope Preferences container.

The Remote Registry service must be running on the machine where the Real Media server is running if the Real Media Server is running on Windows 2000.

For details on configuring this monitor, see “Real Media Server Monitor Settings” on page 954.

Stream Monitors User Interface

This section describes:

- ▶ Microsoft Windows Media Player Monitor Settings on page 946
- ▶ Microsoft Windows Media Server Monitor Settings on page 949
- ▶ Real Media Player Monitor Settings on page 951
- ▶ Real Media Server Monitor Settings on page 954

Microsoft Windows Media Player Monitor Settings

Description	<p>The Microsoft Windows Media Player Monitor allows you to emulate a user playing media or streaming data from a Windows Media Server. The error and warning thresholds for the monitor can be set on one or more Windows Media Player performance statistics.</p> <p>This monitor does not support the .asx or .mov formats. Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Microsoft Windows Media Player Monitor Overview" on page 942

The Add/Edit Microsoft Windows Media Player Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
URL	<p>Type the URL of the media file or streaming source you want to monitor. This should be the URL of the media file.</p> <p>Example: mms://<servername>/sample.asf for a unicast stream or http://<servername>/stationid.nsc for a multicast stream using a Windows Media Server multicast station program.</p> <p>Note: This monitor does not support the .asx or .mov formats.</p>

GUI Element	Description
Counters	Select the media player performance parameters or counters you want to check with the Microsoft Windows Media Player Monitor. For details on the available parameters or counters, see “Performance Counters” on page 947.

Performance Counters

The media player performance parameters or counters you can check with the Microsoft Windows Media Player Monitor include:

GUI Element	Description
Buffering count	The number of times the Player had to buffer incoming media data due to insufficient media content.
Buffering time	The time spent waiting for sufficient media data to continue playing the media clip.
Interrupts	The number of interruptions encountered while playing a media clip. This includes buffering and playback errors.
Packets lost	The number of lost packets not recovered (applicable to network playback).
Packets recovered	The number of lost packets successfully recovered (applicable to network playback).
Packet quality	The percentage ratio of packets received to total packets.
Ratio bandwidth	The ratio (as a percentage) of the actual bandwidth used to the recommended bandwidth. Example: If the recommended bandwidth is 100 bps and the actual bandwidth is 50 bps, the ratio bandwidth is 50%. If the recommended bandwidth is 50 bps and the actual bandwidth is 100 bps, the ratio bandwidth is 200%.

GUI Element	Description
Recommended bandwidth	The recommended bandwidth in bits per second. When a .wmv file is opened in Media Player, the property bitrate is the recommended bandwidth. This bandwidth is embedded in the stream itself.
Recommended duration	The total duration of the media clip in seconds. This value is not effected by what was already played.
Sampling rate	The sampling rate in milliseconds, for collecting statistics.
Stream count	The packet count.
Stream max	The maximum number of packets.
Stream min	The minimum number of packets.
Stream rate	The packet rate indicating the speed at which the clip is played: 1 is the actual speed, 2 is twice the original speed, and so on.
Time quality	The percentage of stream samples received on time (no delays in reception).

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Duration	<p>Type the playback duration, in milliseconds, that the monitor should use for the media file or source indicated by the URL above. The duration value does not need to match the duration of the media contained in the file.</p> <p>Default value: 15000 milliseconds (15 seconds)</p> <p>Example: If a media file contains 45 seconds of media content, and you use the default setting of 15 seconds, the monitor instance connects to the media source and plays the media content for 15 seconds and reports the status for those 15 seconds. If the media content of the file or source you are monitoring is less than the Duration value selected for the monitor, the monitor plays the entire media content and reports the results, including the time required to play the media content.</p>

Microsoft Windows Media Server Monitor Settings

Description	<p>The Microsoft Windows Media Server Monitor allows you to monitor the availability of a Microsoft Windows Media server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more Windows Media server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
-------------	--

Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“Microsoft Windows Media Server Monitor Overview” on page 943

The Add/Edit Microsoft Windows Media Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the Windows Media Server you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ➤ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Real Media Player Monitor Settings

Description	<p>The Real Media Player Monitor allows you to emulate a user playing media or streaming data from a Real Media Server.</p> <p>The error and warning thresholds for the monitor can be set on one or more Real Media Player performance statistics.</p> <p>This monitor does not support metadata files such as the .smi format.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Real Media Player Monitor Overview" on page 944

The Add/Edit Real Media Player Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.
URL	Type the URL of the media file or streaming source you want to monitor. This should be the URL of the media file. Note: <ul style="list-style-type: none"> ➤ Only monitor video, not audio, streams with this monitor. ➤ This monitor does not support metadata files such as the .smi format.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Duration	<p>Type the playback duration (in milliseconds) that the monitor should use for the media file or source indicated by the URL above. The duration value does not need to match the duration of the media contained in the file.</p> <p>Example: You can direct SiteScope to monitor a media file that contains 45 seconds of media content. The default Duration for the Real Media Player Monitor is 15000 milliseconds which equals 15 seconds. In this configuration, the monitor instance would connect to the media source and play the media content for 15 seconds and report the status for those 15 seconds.</p> <p>If the media content of the file or source you are monitoring is less than the Duration value selected for the monitor, the monitor plays the entire media content and reports the results, including the time required to play the media content.</p>

Real Media Server Monitor Settings

<p>Description</p>	<p>The Real Media Server Monitor allows you to monitor the availability of an Real Media Server on Windows NT systems.</p> <p>The error and warning thresholds for the monitor can be set on one or more Real Media Server performance statistics.</p> <p>Use this page to add a monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p>Useful Links</p>	<p>"Real Media Server Monitor Overview" on page 944</p>

The Add/Edit Real Media Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Servers	The server where the Real Media Server you want to monitor is running. You cannot directly edit this box. Use the Get Servers button to select a server name.
Get Servers	<p>Click to open the Server List dialog box. Select the server you want to monitor by:</p> <ul style="list-style-type: none"> ▶ Servers. Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ▶ Other Server. If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Preferences, type the IP address or name of the server to monitor. <p>Note: To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.</p>
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Microsoft Windows/UNIX Remote Preferences. For details, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

21

Web Transaction Monitors

This chapter includes the main concepts, tasks, and reference information for monitoring Web-based applications.

This chapter includes:

Concepts

- ▶ eBusiness Transaction Monitor Overview on page 958
- ▶ Link Check Monitor Overview on page 960
- ▶ URL Monitor Overview on page 961
- ▶ URL Content Monitor Overview on page 965
- ▶ URL List Monitor Overview on page 968
- ▶ URL Sequence Monitor Overview on page 971
- ▶ Web Script Monitor Overview on page 984

Tasks

- ▶ Create a URL Sequence on page 994

Reference

- ▶ Web Transaction Monitors User Interface on page 996

eBusiness Transaction Monitor Overview

Use this monitor to verify that an end-to-end transaction and associated processes complete properly. For example, you could use this monitor to verify that the following steps, each of which is a step in a single transaction, run properly:

- ▶ Place an order on a Web site (Working with the URL Sequence Monitor)
- ▶ Check that the order status was updated (Working with the URL Sequence Monitor)
- ▶ Check that a confirmation e-mail was received (Mail Monitor Overview)
- ▶ Check that the order was added to the order database (Database Query Monitor Overview)
- ▶ Check that the order was transferred to a legacy system (Script Monitor Overview)

You should monitor any multi-step transaction process that causes other updates or actions in your systems. Monitor each of the actions taken to check that updates were performed properly and that actions were carried out successfully.

Using this example, you would first create the URL Sequence monitor, Mail monitor, Database monitor, and applicable Script monitor needed to verify each step of the chain. Then you would create an eBusiness Transaction Monitor and select each of these SiteScope monitors as a group in the order they should be run. If any one monitor indicates a failure, the eBusiness Transaction Monitor reports an error.

Each time the eBusiness Transaction Monitor runs, it returns a status based on the number and percentage of items in the specified monitors and/or groups currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

Editing the Order of the Monitors in the Chain

By default, the Add eBusiness Transaction Monitor page lists monitor groups and individual monitors in the order they are created. To have the eBusiness Transaction Monitor run the chain of monitors in the proper order, they must appear in the proper order in the selection menu on the Add eBusiness Transaction Monitor page. You can do this by creating the individual monitors in the order which they should be run.

Setting up Monitors for the eBusiness Chain

Before you can add an eBusiness Transaction Monitor, you must define other SiteScope monitors that report on the actions and results of the steps in the sequence chain. Using the example from the usage guidelines above, you may create one or more URL Sequence Monitor for verifying the sequence of online actions, a Mail Monitor to confirm that an e-mail acknowledgement is sent, and a Database Query monitor to see that information entered online is logged into a database. To facilitate administration, use the following steps.

To set up a URL sequence chain monitor:

- 1** Create a new group that contains all the individual monitors to be included in the sequence chain.
- 2** Open the new monitor group, and add the first individual monitor type needed to for the sequence (for example, URL Sequence Monitor).

Note: Monitors should be added in the order that they are run in the chain. For example, create a URL Sequence Monitor which triggers an e-mail event **before** you create the Mail Monitor to check for the e-mail. See the note on reordering monitors above.

- 3** If necessary, set up the values to be passed from one monitor to another in the chain. For information about how this works see the section on passing variables between monitors below.
- 4** Add the other monitors for this transaction chain in the required order of execution into the group.

Note: The individual monitors run by the eBusiness Transaction Monitor should generally not be run separately by SiteScope. You should make sure that the **Update Every** setting for each of these monitors is set to zero ("0").

- 5 Create a new group or open an existing group that contains the e-business transaction chain monitor you are creating.
- 6 Click **New Monitor** and select the eBusiness Transaction Monitor.
- 7 Complete the eBusiness Transaction Monitor configuration.

For details on configuring this monitor, see “eBusiness Transaction Monitor Settings” on page 997.

Link Check Monitor Overview

Use the Link Check Monitor to check the internal and external links on a Web page to insure that they can be reached. Each time the Link Check Monitor runs, it returns a status and writes it in the monitoring log file. It also writes the total number of broken links, the total number of links, the total number of graphics, and the average time for retrieving a page.

You should monitor the Web site for the availability of key content. This includes checking that image files and linked HTML files are accessible as referenced within the Web pages. Starting with your home page, the Link Check Monitor branches out and checks every link available on your entire site by default. If you only want it to check a portion of your site, specify the URL that links into the targeted area. You can limit the number of linked hops the monitor follows in the Advanced Settings section.

You probably only need to run the link monitor once a day to check for external links that have been moved or no longer work and internal links that have been changed. You can also run it on demand any time you do a major update of your Web site.

For details on configuring this monitor, see “Link Check Monitor Settings” on page 999.

URL Monitor Overview

The URL Monitor is used to monitor a specified Web page to verify that it can be retrieved. You can also use the URL Monitor to do the following:

- Check secure pages using SSL, 128 bit SSL, and client certificates
- Check for specific content on the retrieved Web page
- Check the Web page for change
- Check for specific error messages
- Check the Web page for a value
- Retrieve detailed download information
- Check XML

When the URL Monitor retrieves a Web page, it retrieves the page's contents. A successful page retrieval is an indication that your Web server is functioning properly. The URL Monitor does not automatically retrieve any objects linked from the page, such as images or frames. You can, however, instruct SiteScope to retrieve the images on the page by selecting **Retrieve Images** or **Retrieve Frames** in the Advanced Settings.

In addition to retrieving specific Web pages, the URL Monitor can verify that CGI scripts and back-end databases are functioning properly. You must input the complete URL used to retrieve data from your database or trigger one of your CGI scripts. The URL monitor verifies that the script generates a page and returns it to the user. For example, you can verify that your visitors are receiving a thank you page when they purchase something from your site. The URL monitor's string matching capability allows you to verify that the contents of the page are correct.

What to Monitor

You can create URL monitors to watch pages that are critical to your Web site (such as your home page), pages that are generated dynamically, and pages that depend on other applications to work correctly (such as pages that utilize a back-end database). The goal is to monitor a sampling of every type of page you serve to check that things are working. There is no need to verify that every page of a particular type is working correctly.

When you choose which pages to monitor, select pages with the lowest overhead. For example, if you have several pages that are generated by another application, monitor the shortest one with the fewest graphics. This puts less load on your server while still providing you with the information you need about system availability.

Scheduling This Monitor

Each URL Monitor puts no more load on your server than someone accessing your site and retrieving a page, so in most cases you can schedule them as closely together as you want. Keep in mind that the length of time between each run of a monitor is equal to the amount of time that can elapse before you are notified of a possible problem.

A common strategy is to schedule monitors for very critical pages to run every 1 to 2 minutes, and then schedule monitors for less critical pages to run only every 10 minutes or so. Using this strategy, you are notified immediately if a critical page goes down or if the entire Web site goes down, but you do not have an excessive number of monitors running simultaneously.

Status

Each time the URL Monitor runs, it returns a reading or status and writes it in the monitoring log file. It also writes in the log file the total time it takes to receive the designated document. This status value is also displayed in the SiteScope Monitor tables and is included as part of alert messages sent by using e-mail.

The status reading shows the most recent result for the monitor. This status value is displayed in the URL Group table within SiteScope. It is also recorded in the SiteScope log files, e-mail alert messages, and can be transmitted as a pager alert. The possible status values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- document moved
- unauthorized
- forbidden
- not found
- proxy authentication required
- server error
- not implemented
- server busy

The status is logged as either good, warning, or error. A warning status or error status is returned if the current value of the monitor is a condition that you have defined as other than OK.

SSL Connectivity

Web servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The `http://` prefix means that the server uses a non-encrypted connection. The `https://` prefix means that it is a secure, encrypted connection.

Monitoring a Web server which uses an encrypted connection, requires that you either:

- ▶ Select the **Accept Untrusted Certs for HTTPS** option in the Advanced Settings. For details, see “URL Monitor Settings” on page 1003.
- ▶ Import the server certificate. See below for details.

To import a server certificate:

- 1 Check the certificates already in the keyStore, from the `<SiteScope root directory>\java\lib\security` directory, by entering:

```
../../bin/keytool -list -keystore cacerts
```

- 2 Import the certificate, from the `<SiteScope root directory>\java\lib\security`, by entering:

```
../../bin/keytool -import -file myCert.cer -alias myalias -keystore cacerts
```

where `myCert.cer` is the certificate file name and `myalias` is the certificate alias.

Make sure that you specify a unique alias for every certificate you add. If you do not, the keytool uses an automatic alias and once you attempt to add more than one custom certificate, the new certificate overwrites the old and keeps the default alias.

The word `changeit` is the default password for the `jssecacerts` file.

- 3 Make a copy of `<SiteScope root directory>\java\lib\security\cacerts` and rename it `<SiteScope root directory>\java\lib\security\jssecacerts`. After doing this, manually check to make sure the file `jssecacerts` is located in the `<SiteScope root directory>\java\lib\security` directory. The reason for creating the `jssecacerts` file is that the default `cacerts` file is overwritten every time SiteScope is upgraded or re-installed. Creating a copy with a different name allows new certificates to be imported and not be overwritten with future installations or upgrades.

For details on configuring this monitor, see “URL Monitor Settings” on page 1003.

URL Content Monitor Overview

The URL Content Monitor is primarily used to monitor Web pages that are generated dynamically and display statistics about custom applications. By monitoring these pages, these statistics can be retrieved and integrated into the rest of your SiteScope system.

You should use the URL Content Monitor if you need to verify multiple values (up to 10 variables) from the content of a single URL. Otherwise, the standard URL Monitor is normally used. One use for this monitor is to integrate SiteScope with other applications that export numeric data through a Web page. The content values are matched using regular expressions. The monitor includes the matched values as part of the monitor status which are written to the log. If the matched values are numeric data, the results can be plotted in a report.

Scheduling This Monitor

The frequency depends on the statistics being monitored. For most statistics, every several minutes is often sufficient.

Status

Each time the URL Content Monitor runs, it returns a status and several match values and writes them in the monitoring log file. It also writes the total time it takes to receive the designated document in the log file.

The reading is the current value of the monitor. Possible values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- document moved
- unauthorized
- forbidden
- not found
- proxy authentication required
- server error
- not implemented
- server busy

The status is returned as **good**, **warning**, or **error** dependent on the results of the retrieval, content match, and the error or warning status criteria that you select.

SSL Connectivity

Web servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The `http://` prefix means that the server uses a non-encrypted connection. The `https://` prefix means that it is a secure, encrypted connection.

Monitoring a Web server which uses an encrypted connection, requires that you either:

- Import the server certificate as described below.
- Select the **Accept Untrusted Certs for HTTPS** option in the Advanced Settings as described in “URL Content Monitor Settings” on page 1014.

To import a server certificate:

- 1 Check the certificates already in the keyStore, from the `<SiteScope root directory>\java\lib\security` directory, by entering:

```
../../../../bin/keytool -list -keystore cacerts
```

- 2 Import the certificate, from the `<SiteScope root directory>\java\lib\security`, by entering:

```
../../../../bin/keytool -import -file myCert.cer -alias myalias -keystore cacerts
```

where `myCert.cer` is the certificate file name and `myalias` is the certificate alias.

Make sure that you specify a unique alias for every certificate you add. If you do not, the keytool uses an automatic alias and once you attempt to add more than one custom certificate, the new certificate overwrites the old and keeps the default alias.

The word `changeit` is the default password for the `jssecacerts` file.

- 3 Make a copy of `<SiteScope root directory>\java\lib\security\cacerts` and rename it `<SiteScope root directory>\java\lib\security\jssecacerts`. After doing this, manually check to make sure the file `jssecacerts` is located in the `<SiteScope root directory>\java\lib\security` directory. The reason for creating the `jssecacerts` file is that the default `cacerts` file is overwritten every time SiteScope is upgraded or re-installed. Creating a copy with a different name allows new certificates to be imported and not be overwritten with future installations or upgrades.

For details on configuring this monitor, see “URL Content Monitor Settings” on page 1014.

URL List Monitor Overview

You can use the URL List Monitor to check the availability of a list of URLs without having to create a separate URL monitor for each one. For example, this is useful if you host several Web sites and simply want to see that they are each serving pages as expected. The URL List Monitor is not used to confirm links between pages (see the “Link Check Monitor Overview” on page 960) or other Web transaction processes (see “URL Sequence Monitor Overview” on page 971).

A URL List is specified by giving a filename containing the list of URLs to check. The URLs that you want to monitor are saved in a plain text file. There is virtually no limit to the number that you can list though the run interval selected for the monitor may require that the number of URLs be limited. For each URL included in the URL list file, the monitor retrieves the contents of the URL or the server response to the request.

Scheduling This Monitor

This is strictly dependent on how often you want to check to see if the URLs are working. Once an hour is common, but you can schedule it to run more often.

There are a few factors that affect how long it takes the URL List Monitor to complete a run:

- ▶ number of URLs in the list
- ▶ URL retrieval time
- ▶ the number of threads used

In some cases this may lead to the monitor not running as expected. As an example, assume you have a list of 200 URLs that you want to monitor every 10 minutes, but, due to Internet traffic, SiteScope is not able to complete checking all of the 200 URLs in that amount of time. The next time the monitor was scheduled to run, SiteScope would see that it did not complete the previous run and would wait for another 10 minutes before trying again.

If this happens once in awhile, it is probably not a problem. If it happens more often, there are several things you can do to resolve the issue:

- ▶ Schedule the monitor to run less frequently. If this conflicts with some other objective, use the other options.
- ▶ Reduce the **pause interval** set under the Advanced Settings. This minimizes the time it takes for the monitor to retrieve all of the URLs.
- ▶ Increase the number of threads that SiteScope can use when checking the URLs. The more threads, the quicker SiteScope can check them. Increasing the number of threads can adversely affect SiteScope's performance.

Ideally, you want SiteScope to have just completed checking the URLs in the list when it is time to start checking again. This would indicate that the load was evenly balanced.

Each time the URL List Monitor runs, it returns the number of errors, if any, and writes it into the monitoring log file. It also writes the total number of URLs checked and the average time, in milliseconds, to retrieve each URL.

SSL Connectivity

Web servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The `http://` prefix means that the server uses a non-encrypted connection. The `https://` prefix means that it is a secure, encrypted connection.

Monitoring a Web server which uses an encrypted connection, requires that you either:

- ▶ Import the server certificate as described below.
- ▶ Select the **Accept Untrusted Certs for HTTPS** option in the Advanced Settings as described in “URL List Monitor Settings” on page 1023.

To import a server certificate:

- 1 Check the certificates already in the keyStore, from the `<SiteScope root directory>\java\lib\security` directory, by entering:

```
../../bin/keytool -list -keystore cacerts
```

- 2 Import the certificate, from the `<SiteScope root directory>\java\lib\security`, by entering:

```
../../bin/keytool -import -file myCert.cer -alias myalias -keystore cacerts
```

where `myCert.cer` is the certificate file name and `myalias` is the certificate alias.

Make sure that you specify a unique alias for every certificate you add. If you do not, the keytool uses an automatic alias and once you attempt to add more than one custom certificate, the new certificate overwrites the old and keeps the default alias.

The word `changeit` is the default password for the `jssecacerts` file.

- 3 Make a copy of `<SiteScope root directory>\java\lib\security\cacerts` and rename it `<SiteScope root directory>\java\lib\security\jssecacerts`. After doing this, manually check to make sure the file `jssecacerts` is located in the `<SiteScope root directory>\java\lib\security` directory. The reason for creating the `jssecacerts` file is that the default `cacerts` file is overwritten every time SiteScope is upgraded or re-installed. Creating a copy with a different name allows new certificates to be imported and not be overwritten with future installations or upgrades.

For details on configuring this monitor, see “URL List Monitor Settings” on page 1023.

URL Sequence Monitor Overview

You use URL Sequence Monitors to verify that multiple-page Web transactions are working properly. This is an important part of monitoring key business processes and services. For example, you can have SiteScope retrieve a login page, type an account name by using a secure Web form, check an account status for the page that is returned, and then follow a sequence of links through several more pages. URL Sequence Monitors are also useful for checking pages that include dynamically generated information, such as session IDs, that are embedded in the Web pages by using dynamic links or hidden input items.

The core of the URL Sequence Monitor is the sequence of URL and associated action requests that are performed by the monitor. A URL Sequence begins with a URL acting as the starting point or Step 1 for the sequence. This can then be followed by additional URLs that are accessed manually, or more commonly, by links or form buttons that a user would select to navigate or complete a specific transaction.

By default, SiteScope allows you to define up to twenty sequence steps. For each step you may specify a content match to search for, type a user name and password if required, define custom POST data, as well as other optional criteria for that step.

You can edit the steps in a URL sequence after they have been added. Making changes to a sequence step requires that you update both the individual step and update the monitor as a whole. Editing any step of a URL sequence may affect subsequent steps in the sequence and cause the sequence to fail. It may be necessary to change all of the steps that occur after the step that is changed.

You can delete steps from a URL sequence but they can only be deleted starting from the last step in the sequence. This is to prevent inadvertently breaking a sequence because, in most cases, one step is dependent on data returned by the previous step. When you update or delete steps, SiteScope attempts to run the changes to the step. The results of the monitor run are displayed in SiteScope Dashboard.

What to Monitor

You should monitor any multi-step Web page sequence that you have made available to general users to verify that they are available and function correctly. Web site visitors often assume that any problems they encounter are due to user error rather than system error, especially if they're not familiar with your application. By using this monitor to perform sequence testing, you can verify that users are able to successfully complete transactions.

Working with the URL Sequence Monitor

The URL Sequence Monitor is more complex than most other SiteScope monitor types and the steps for working with the monitor are different than for other monitors. The following is an overview of key concepts and actions you use when working with the URL Sequence Monitor:

- ▶ The URL Sequence Monitor can be configured with between one to twenty steps. Each step is defined individually in a sequence of numbered entries in the interface. The steps must be initially configured in the intended sequence as the request for one step provides the content used in the following step.
- ▶ When you first configure a URL Sequence Monitor, be sure to configure the steps you want to include in the sequence before you click the **OK** button to create the monitor.

- ▶ You configure the URL Sequence Monitor in text mode. The navigation links and form actions are displayed as text parsed from the HTML that is used to construct a page in Web browsers. In some cases, portions of HTML code may also be included. You must be familiar with HTML when working with this monitor.
- ▶ Many Web-based systems use session data to identify clients and track the state of a user's interaction with the server application. This session data is often sent back and forth to the client in the HTTP header or Post Data. You should be familiar with the session tracking methods used by the systems you want to monitor to effectively configure this monitor.
- ▶ Web-based sequences or transactions can be difficult to navigate when dealing with many Web pages. For example, Web pages that use many graphic images for navigation hyperlinks can present special challenges when configuring URL Sequence monitors. You must be familiar with HTML hyperlink syntax when working with this monitor.
- ▶ When you first configure the URL Sequence Monitor, the HTML text content returned from the request made in one step is displayed in a folding panel at the bottom of the following Step panel. This can be very useful for finding content on which you want to perform a match. You may also use this to correlate links and forms in the respective selection menus with their relative location on the page. For example, if there is a search entry form near the top of a Web page and another, different search form further down in the page, you can view the raw HTML to help determine the syntax associated with the form that you want to test.
- ▶ SiteScope does not parse or interpret embedded scripts or other client-side program code such as Javascript (ECMAScript). Web page content that is generated or controlled by client-side code does not usually appear in the URL Sequence Monitor. For information about dealing with Web page scripts, see "URL Sequence Monitor Settings" on page 1027 and Client-side Programs help page.

Defining Sequence Steps

The URL sequence must begin with an initial URL. SiteScope makes a request for the URL, and the data returned by this initial request is used for subsequent steps. The HTTP response header and the content of the URL are available in the HTML Source section at the bottom of the subsequent step dialog box.

When you have entered the first step, you can add more steps. You repeat this process depending on the number of Web pages and actions that need to be taken to complete the sequence. The step screens provide access to the available elements on the Web page requested by the previous step. This includes form buttons, hyperlinks, form input elements, and other data. You use these elements to create each subsequent sequence step separately. Most sequence steps involve one of the following elements:

Reference Type	Description
Go to URL Manually	Where the sequence uses the Common Gateway Interface (CGI) for data transmission between the client and the server, it may be useful to specify a particular URL and name-value pairs. You can type the URL you want to request along with any name-value pairs needed to get to the next sequence step even if those values are available through some other page element (such as a form). This option also allows you to copy URL and CGI strings directly from the location or address bar of another browser client that you may be using to step through the sequence you are building.
Following a Hyperlink	SiteScope parses the content of the URL returned by the previous step and creates a list of hyperlinks that are found on the page. This includes links that are part of an image map that may be virtual "buttons" on a navigation menu. Any links found on this page of the sequence can be viewed and selected using the drop-down list box to the right of the Link radio button. Use the following steps to add a link step to the sequence.

Reference Type	Description
Selecting a Form button	<p>SiteScope parses the content of the URL in the current step and creates a list of form elements of the type "Submit". If SiteScope finds any HTML forms on the current page of the sequence, they are displayed in a drop-down list.</p> <p>The listings are in the following format: {[formNumber]FormName}ButtonName</p> <p>Example: The Search button on a company's search page might be listed as: {[1]http://www.CompanyName.com/bin/search}search</p>
Selecting a Frame within a frameset	<p>If the URL for a step in the sequence contains an HTML FRAMESET and you need to access a hyperlink, form, or form button that is a page displayed in a frame, you must drill down into the Frameset to the actual page that contains the links or forms that you want before you can proceed with other steps in the sequence.</p>
Following a META REFRESH redirection	<p>If the page for this step of the sequence is controlled by a <META HTTP-EQUIV="Refresh" CONTENT="timedelay; URL=filename.htm"> tag, you can instruct SiteScope to retrieve the specified file as the next step. This sort of construct is sometimes used for intro pages, splash screens, or pages redirecting visitors from an obsolete URL to the active URL.</p>

Note: SiteScope does not parse or interpret embedded scripts or other client-side program code such as Javascript (ECMAScript). Web page content that is generated or controlled by client-side code usually does not appear in the URL Sequence Monitor.

SSL Connectivity

Web servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The `http://` prefix means that the server uses a non-encrypted connection. The `https://` prefix means that it is a secure, encrypted connection.

Monitoring a Web server which uses an encrypted connection, requires that you either:

- ▶ Import the server certificate as described below.
- ▶ Select the **Accept Untrusted Certs for HTTPS** option in the Advanced Settings as described in “URL Sequence Monitor Settings” on page 1027.

To import a server certificate:

- 1 Check the certificates already in the keyStore, from the `<SiteScope root directory>\java\lib\security` directory, by entering:

```
../../../../bin/keytool -list -keystore cacerts
```

- 2 Import the certificate, from the `<SiteScope root directory>\java\lib\security`, by entering:

```
../../../../bin/keytool -import -file myCert.cer -alias myalias -keystore cacerts
```

where `myCert.cer` is the certificate file name and `myalias` is the certificate alias.

Make sure that you specify a unique alias for every certificate you add. If you do not, the keytool uses an automatic alias and once you attempt to add more than one custom certificate, the new certificate overwrites the old and keeps the default alias.

The word `changeit` is the default password for the `jssecacerts` file.

- 3 Make a copy of `<SiteScope root directory>\java\lib\security\cacerts` and rename it `<SiteScope root directory>\java\lib\security\jssecacerts`. After doing this, manually check to make sure the file `jssecacerts` is located in the `<SiteScope root directory>\java\lib\security` directory. The reason for creating the `jssecacerts` file is that the default `cacerts` file is overwritten every time SiteScope is upgraded or re-installed. Creating a copy with a different name allows new certificates to be imported and not be overwritten with future installations or upgrades.

URL Sequences and Dynamic Content

Web pages which include client-side programming or dynamically generated content can present problems in constructing SiteScope URL Sequence monitors. Client-side programs might include Java applets, ActiveX controls, Javascript, or VBScript. Web pages which are generated by server-side programming (Perl/CGI, ASP, CFM, SSI, and so forth) can also present a problem if link references or form attributes are changed frequently.

SiteScope does not interpret Javascript, VBScript, Java applets, or Active X Controls embedded in HTML files. This may not be a problem when the functionality of the client-side program is isolated to visual effects on the page where it is embedded. Problems can arise when the client-side program code controls links to other URL's or modifies data submitted to a server-side program. Because SiteScope does not interpret client-side programs, actions or event handlers made available by scripts or applets are not displayed in the URL Sequence step dialog.

Some Web sites use dynamically generated link references on pages generated by server-side programming. While these Web pages do not contain client-side programs, frequently changing link references or cookie data can make it difficult to set up and maintain a URL Sequence Monitor.

Dynamic Content Workarounds

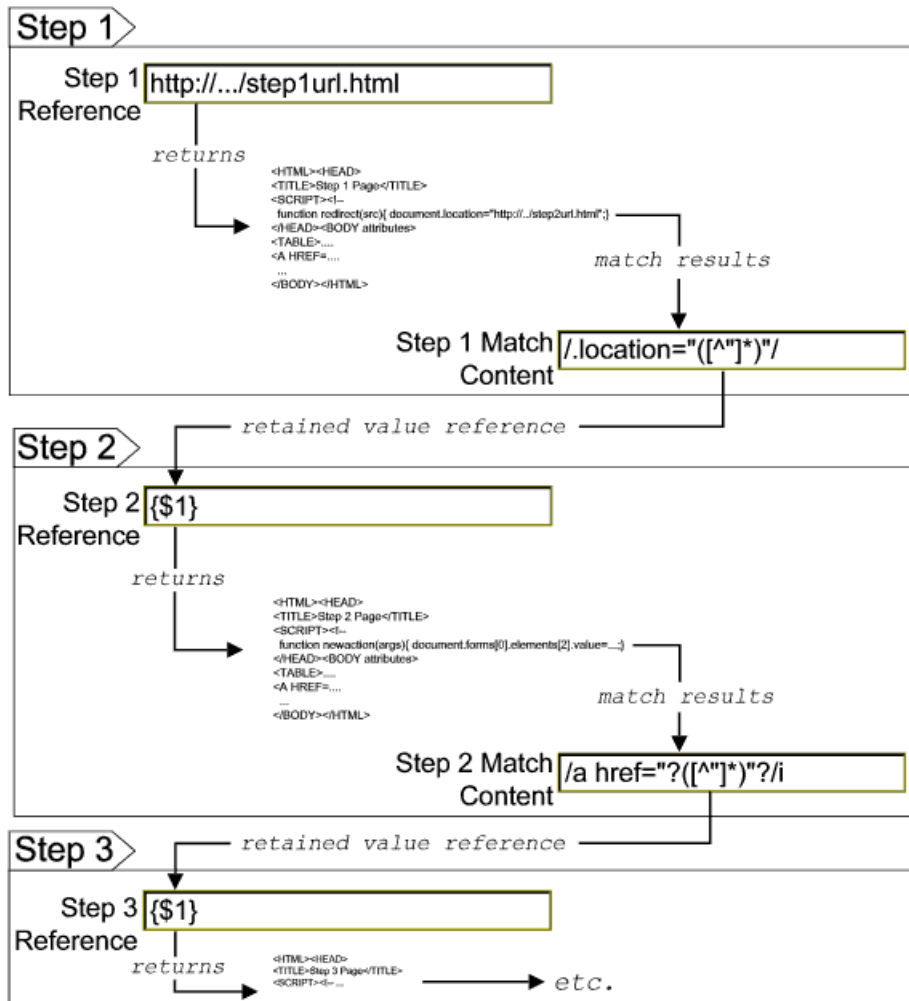
There are several ways to make a SiteScope URL Sequence monitor perform actions controlled by client-side programs and other dynamic content. Several of these workarounds are presented below. The workarounds generally require knowledge of the principles of Web page construction, CGI programming, Perl-style regular expressions, and the programming used to support the Web site being monitored.

Dynamic Content	SiteScope Workaround
<p>A Web page contains a script which controls a link to another URL.</p> <p>Example: <code>onClick = "document.location='http://..."</code></p>	<p>Use a Match Content regular expression in the sequence step for the subject page to retain the filename.ext value from the <code>.location="filename.ext"</code> match pattern. The retained value can then be passed as a URL in the URL box of the next step of the sequence.</p>
<p>A client-side program reformats, edits, or adds data to a POST or GET data set collected by HTML form inputs.</p>	<p>Manually edit the script changes into the NAME=VALUE pairs displayed for the subject sequence step. This is done in the POST Data box in the URL Sequence step dialog page. This requires familiarity with the script function and CGI request headers.</p>
<p>A client-side program generates HTML content which, after interpretation by a Web browser, includes HTML <code></code> links.</p>	<p>Use a Match Content regular expression to return the filename.ext value from the <code>HREF="filename.ext"</code> pattern and pass it to the URL box of the next sequence step.</p>
<p>A client-side program generates HTML content which, after interpretation by a Web browser, includes forms submitted to a CGI program.</p>	<p>Manually enter the NAME=VALUE pairs for the subject sequence step. This is done in the POST Data box in the URL Sequence step dialog page. This requires familiarity with the script, the form structure, and CGI request headers.</p>

Dynamic Content	SiteScope Workaround
A script dynamically sets the ACTION attribute of an HTML <FORM> tag.	Manually enter the ACTION URL for the next sequence step. This is done in the URL box under Reference Type in the URL Sequence step dialog page. This requires familiarity with the script.
A script dynamically sets the METHOD attribute of an HTML <FORM> tag.	Manually enter the POST or GET data for the next sequence step. For POST methods, type the data in the POST Data box in the URL Sequence step dialog page. For GET methods, type the ACTION URL plus the &NAME=VALUE pairs in the URL box under Reference Type in the URL Sequence step dialog page. This requires familiarity with the script, the form structure, and CGI request headers.

The figure below illustrates several of the principles of constructing a URL Sequence Monitor using regular expressions. The regular expressions shown in the figure can be used to extract URLs from Javascript or other Web page content. As indicated, content matches for a given step are performed on the content returned for that step. The parentheses used in the regular expressions cause the value matched by the expression inside the parentheses to be remembered or retained. This retained value can be passed on to the next step of the sequence by using the `{$n}` variable. Because the regular expression can contain more than one set of parentheses, the `$n` represents the match value from the `$nth` set of parentheses.

The example in the figure only uses one set of parentheses and thus references the retained value as `{$1}`.



Web pages containing code that perform the following present additional challenges:

- ▶ A script parses a cookie or other dynamic content to be added to a CGI GET request.
- ▶ Link information is contained in an external script file accessed by using a HTML `<SCRIPT HREF="http://... >` tag.

Web pages with dynamically generated link and form content may not be parsed correctly by the SiteScope URL Sequence Monitor.

Retaining and Passing Values Between Sequence Steps

One important function of the Match Content capability in URL Sequence Monitor is the ability to match, retain, and then reference values from one URL sequence step for use as input in a subsequent step. Using one or more sets of parentheses as part of a Match Content regular expression instructs SiteScope to remember the values matched by the pattern inside the parentheses. These values can then be referenced using the syntax described in the following example.

Example

Suppose you create a URL Sequence Monitor and include a Match Content expression for the first step to capture some session information. The Step 1 Match Content expression could be in the form of

```
/[\w\s]*?(pattern1)[\/\-\=]*?(pattern2)/
```

The two sets of parentheses in this expression instruct SiteScope to retain the two values matched by `pattern1` and `pattern2`. To use these values as input to the **next** step in the URL sequence, use the syntax `{$valuenum}`. In this example, the string `{$1}` references the value matched by `pattern1` and `{$2}` references the value matched by `pattern2`. Use the above syntax for passing the referenced values to the URL sequence step immediately following the step in which the content match was made (step 1 to step 2 in our example).

You can retain and pass matched values from one step to any other subsequent step by using a compound syntax of `$$$stepnum.valuenum`. If, in our example, you want to use the value matched by `pattern1` in step 1 as input in a FORM or URL request in step 4 of the URL sequence, you would include the syntax `$$$1.1` in Step 4. To reference the value matched by `pattern2`, use the `$$$1.2` syntax.

Sharing Cookies Between Monitor Runs and Configured Monitors

The URL Sequence Monitor also supports sharing cookies between monitor runs and between configured monitors. This is done by maintaining a persistency of both session cookies and permanent cookies that can be queried, updated and shared among other URL Sequence monitors.

Suppose you have a number of different URL Sequence Monitors that are currently configured on a SiteScope server. Assume that all the monitors simulate a URL transaction in which at least one of the steps uses a session cookie to send to the server instead of logging in each time. Using Cookie Persistency, you can configure one monitor to save the cookies it receives and configure all the other monitors to load the cookies. This can save system costs if there is a charge for each request to the login server from the monitoring tool. The monitor can 'log in' once and reuse the credentials from the login by other monitor runs and monitor instances. Thus, only one monitor needs to contain a login step. All the others can skip this step and send the login credentials in a cookie instead.

Notes:

- Configure the monitor designated to save cookies to run at a frequency that is not less than the time frame of the session to ensure that cookies remain valid throughout the time frame of a session. A monitor that loads cookies from the persistency file does not check to see whether the cookie it is loading and sending is still valid.
 - Configure the monitor designated to save cookies before you configure the loading monitors. This is to ensure that the persistency file exists when you configure monitors to load from the file. Configuring the saving monitor to run at a higher frequency than loading monitors does not ensure that the monitor saving cookies runs first.
-

For details on the steps and settings you use to create a URL sequence, see “Create a URL Sequence” on page 994.

For details on the URL Sequence Monitor user interface, see “URL Sequence Monitor Settings” on page 1027.

Web Script Monitor Overview

The Web Script Monitor proactively monitors Web sites in real time, identifying performance problems before users experience them. It enables you to monitor sites from various location where SiteScope is installed, emulating the end-user experience. You can assess site performance from different client perspectives.

Note: The Web Script Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

The Web Script Monitor runs the scripts created in the HP Virtual User Generator (VuGen). You use VuGen to create a script that emulates end-user actions. You can create the script with the steps that you want monitored on target Web sites.

Note to HP Business Availability Center users: The Web Script Monitor is not available when working in HP Business Availability Center. The monitor's data cannot be reported to HP Business Availability Center.

What to Monitor

You can create transactions to monitor pages that are critical to your Web applications, pages that are generated dynamically, and pages that depend on other applications to work correctly (such as pages that utilize a back-end database).

Counter Measurements and Transaction Breakdown Data

Each time the Web Script Monitor runs the VuGen script, it returns the transaction breakdown and performance data. The VuGen script also includes content match functionality, enabling you to check images, texts, links, and other areas of the Web site.

In addition, the monitor's reported data can include the following measurements:

- ▶ The amount of time needed to establish an initial connection with the Web server performing the transaction.
- ▶ The amount of time taken to establish an SSL connection for HTTPS connections.
- ▶ The time in milliseconds for the transaction to be run.
- ▶ Whether the transaction passed or failed to connect and perform its required steps.
- ▶ Number of pages accessed when running the transaction.
- ▶ Number of errors that occurred during the transaction run.

The monitor can provide early indicators of the following performance issues:

- ▶ Excessive connection or retry times.
- ▶ Slow DNS resolution or other problems with the DNS server.
- ▶ Problems along the network or whether the server is responsive to requests.
- ▶ Delays or failures in secured or authorized connections.
- ▶ Overall network quality.
- ▶ Web server delays.

Each of the measurements is available as a parameter for assigning thresholds. This means that thresholds can be set for specific transactions and measurements, providing status indicators per transaction.

For details on selecting measurement counters, see “Selecting Counters” on page 991.

Setting up the Web Script Monitor

Prior to configuring the Web Script Monitor in SiteScope, you must create the script in VuGen. The monitor runs only those scripts created in VuGen. Here is an overview of the steps necessary to set up the Web Script Monitor.

1 Download HP Virtual User Generator (VuGen).

Go to the HP Software Support site (<http://www.hp.com/go/hpsoftwaresupport>) and in the **Where do I find** section, click **Software patches**. In the **Product** section, select **SiteScope** and type **VuGen** in the optional search box. Download the required version of VuGen from the results. You must log in with your HP user name and password to access the Software Patches page.

To enable monitoring, you must also download the latest HP Virtual User Generator Feature Pack.

2 Familiarize yourself with how to create scripts.

The script you create in VuGen is run by the Web Script Monitor and must contain transactions.

The VuGen interface is easy-to-use and contains different access points for getting help. For details, see “Getting Started” on page 987.

3 Use the supported protocols in Virtual User Generator to create your script.

It is recommended to use the Web (Click and Script) protocol to create your script for use in SiteScope. For a list of all the supported protocols and for details on the Web (Click and Script) protocol, see “Supported VuGen Protocols” on page 988.

4 Include transactions and content match checkpoints in your script.

The VuGen script must contain transactions to be run by the Web Script Monitor in SiteScope.

Checkpoints are recommended for checking content while running the VuGen script.

For details, see “Inserting Transactions and Creating Checkpoints” on page 990.

5 Save the script's runtime files into a zip file and save the zip file into the required directory.

For details, see "Saving and Storing the Script" on page 990.

6 Ensure that the script runs properly in VuGen before continuing.

For details, refer to "Working with VuGen" > "Running Vuser Scripts in Standalone Mode" in the VuGen guide.

7 Create the Web Script Monitor in SiteScope.

For details, see "Web Transaction Monitors User Interface" on page 996.

Working with VuGen

VuGen can be used to automatically create a transaction script by recording the actual business processes and actions performed by users interacting with a Web application. VuGen captures all end-user activity between the client and the server, thereby capturing the exact tasks and functions users perform.

Note: The Web Script Monitor supports scripts created in HP Virtual User Generator version 9.1 and earlier.

Getting Started

The VuGen help is accessible from the VuGen product once it is downloaded. It can be accessed in the following ways:

- Press F1 for context-sensitive help when working with a specific function.
- Select **Help > Contents and Index > Contents** tab > **Books Online > VuGen** to view the entire online guide. Use this option when searching for a specific topic referred to in the description of this monitor.

- Select **Help > Books Online > HP Virtual User Generator User's Guide** to access the guide in pdf format.

The VuGen interface includes a detailed workflow that takes the user through the step-by-step process of creating a script. For information about the workflow, refer to "Working with VuGen" > "Viewing the VuGen Workflow" in the VuGen guide.

For more detailed information on creating scripts, refer to "Working with VuGen" > "Recording with VuGen" > "Creating New Virtual User Scripts" in the VuGen guide.

Supported VuGen Protocols

The following are the protocols supported for the Web Script Monitor.

Web (Click and Script) Protocol

This is the recommended protocol to use to record scripts to be run by the Web Script Monitor.

Web (Click and Script) is a new approach to Web scripting. It introduces a GUI-level scripting API, and a quicker way to create scripts.

- Easy-to-use scripting.
- Intuitive API functions describe user actions on Web objects (button, text link etc.).
- In tree view, the steps are grouped according to their pages.
- In snapshot viewer, the object corresponding to the active step is highlighted.

For details on using this protocol, refer to the "Creating Web Vuser Scripts" and "Working with Web (Click and Script) Vuser Scripts" sections under "E-Business Protocols" in the VuGen guide.

Web (Click and Script) Limitations

- ▶ Records and emulates on Internet Explorer version 6 only.
- ▶ Does not support recording on Microsoft Windows 2003.
- ▶ Does not support VBScript and applets.
- ▶ Does not support user actions on ActiveX objects and Macromedia Flash.
- ▶ Supports only English language applications.

Note: If any of these limitations affect your ability to record a script, use VuGen's Web (HTTP/HTML) Protocol instead. For details, see below. For information about choosing a protocol, refer to "E-Business Protocols" > "Choosing a Web Vuser Type" in the VuGen guide.

Web (HTTP/HTML) Protocol

This is the standard VuGen protocol for recording Web applications.

When recording a Web (HTTP/HTML) script, VuGen records the HTTP traffic and server response over the Internet. The scripts contain detailed information about your actions in the browser.

The Web (HTTP/HTML) Vuser provides two recording levels: HTML-based script and URL-based script. These levels let you specify what information to record and which functions to use when generating a Vuser script.

For details on using this protocol, refer to the "E-Business Protocols" > "Creating Web Vuser Scripts" in the VuGen guide.

Inserting Transactions and Creating Checkpoints

- ▶ While creating your VuGen script, you must insert transactions into the script. These transactions provide the breakdown performance data reported by the monitor.

For details on transactions, refer to "Working with VuGen" > "Enhancing Vuser Scripts" > "Inserting Transactions into a Vuser Script" in the VuGen guide.

- ▶ VuGen's Content Check mechanism allows you to check the contents of a page for a specific string. This is useful for detecting non-standard errors. It is recommended that you include content check checkpoints in your script.

For details on checkpoints, refer to the "Checking Web Page Content" and "Verifying Web Pages under Load" sections under "E-Business Protocols" in the VuGen guide.

Saving and Storing the Script

The script you create in VuGen must be saved as a zip file. It is recommended to save only the runtime files. For details, refer to the "Recording with VuGen" and "Using Zip Files" sections of the VuGen guide.

When saving the zip file:

- ▶ ensure that the zip file has the same name as the script
- ▶ ensure that each script used for a Web Script Monitor has a unique name

You can save the script into:

- ▶ The configured default location for VuGen scripts within the SiteScope root directory is **<SiteScope root directory>\templates.webscripts**. This directory is automatically created.

By default, all the scripts in this directory appear in the dropdown list of available scripts under Main Settings when configuring the monitor.

- ▶ A different location for VuGen scripts that you configure in SiteScope's General Preferences.

You can change the default location of VuGen scripts by entering a value in the **VuGen Scripts Path Route** box in General Preferences. The scripts stored in the location you type appear in the dropdown list of available scripts under Main Settings when configuring the monitor.

- ▶ Any other location accessible to the SiteScope machine.

When configuring the monitor, you can also type the full directory path and name of the script. The Web Script Monitor can access the script if the machine on which SiteScope is running has file system access to the path location.

Selecting Counters

The Web Script Monitor makes use of performance counters to measure Web sites performance. Select the counter metrics you want to monitor with the Web Script Monitor. For details on adding performance counter metrics, see “Web Script Monitor Settings” on page 1038. For details on the counter metrics available for the monitor, see “Web Script Performance Counters” on page 1041.

Advanced Information and Troubleshooting

The Web Script Monitor uses an internal engine to run the VuGen scripts you create. This section includes some advanced issues and troubleshooting.

SiteScope makes a copy of the script created in VuGen and stores it in a location within the SiteScope directory. SiteScope makes the necessary modifications for the script to be run properly by the Web Script Monitor. These modifications are automatic and cannot be manually duplicated. They include:

- ▶ Disabling the **Download Snapshots** operation.
- ▶ Disabling the **Think Time** operation.
- ▶ Disabling the **Iterations** operation.

Therefore:

- ▶ If there is any change made to the script in VuGen, including the name of the script, and you want the Web Script Monitor to run the revised version of the script, you must edit the monitor in SiteScope and select the edited script in its saved location.
- ▶ Each script must have a unique name even if the different zip files for the scripts reside in different directories.
- ▶ The name of the zip file selected for the monitor must be the same as the name of the script created in VuGen.

Troubleshooting

- ▶ Each time the monitor is run, a log is created. You can view the log to troubleshoot the monitor if you see there is a problem running the scripts. The logs are stored in `<SiteScope root directory>\cache\temp\WebScript\<name of script>\log`. You can search for the required log based on the name of the script run by the monitor and the time the log was created.

This directory is cleaned out every time SiteScope is restarted, which is every 24 hours by default.

- If the log files do not give you the necessary information to determine why the script is not running properly, run the script in VuGen. For details, refer to "Running Vuser Scripts in Standalone Mode" in the VuGen guide.
- If all the transaction breakdown counters for the monitor are reporting a status of -1 and there is a reported time for the Duration counter (the total running time of the transaction), it could be because the transaction breakdown times exceed the total running time. This can occur in rare cases because of the way the transaction breakdown times are calculated and because the Duration is an actual measurement of the total transaction time from start to finish, with no additional calculations. If the problem persists for a specific transaction, it is recommended that you adjust the counters selected for the transaction.
- If you get the message "Error: Fail to get performance data timeout (error)" during the monitor run, add `LogFileWrite=1` to the **default.cfg** file of the specific script file to get more details about the error. If the script log shows that some of the resources are taking more time than the monitor timeout, increase the **Web Script Timeout** value in General Preferences.
- The Web Script Monitor supports script names with English characters only.

For details on configuring this monitor, see "Web Script Monitor Settings" on page 1038.

Create a URL Sequence

This task describes the steps and settings you use to create a URL sequence.

This task includes the following steps:

- “Add a URL Sequence Monitor” on page 994
- “Start a New URL Sequence” on page 994
- “Define Additional Sequence Steps” on page 995
- “Enter an Encrypted or Unencrypted Password (if required)” on page 995
- “Configure Other Settings for the Monitor” on page 996

1 Add a URL Sequence Monitor

Add the URL Sequence Monitor to a monitor group container and type a **Name** and **Frequency** in the Main Settings section. For details on the user interface, see “URL Sequence Monitor Settings” on page 1027.

2 Start a New URL Sequence

You configure the first URL in the sequence in the URL Sequence dialog box. The URL sequence must begin with an initial URL.

- a** In the Main Settings panel of the New URL Sequence Monitor properties tab, click the **Add Step** button.
- b** Type the initial URL address in **Reference Type** box. This URL should be the initial Web page that the user is expected to see or the access point for the web-based system you are going to monitor.
- c** Complete the other settings as necessary and click **OK**. Generally, the URL is sufficient for the first step of most URL sequences. For details on the user interface, see “URL Sequence Steps Settings” on page 1033.

Note: When you first configure the URL Sequence Monitor, the HTML text content returned from the request made in the previous step is displayed in the **Steps** panel.

3 Define Additional Sequence Steps

Click the **Add Step** button again to configure the individual steps for the URL sequence. Use the **Reference Type** options to select how SiteScope progresses from one step of a URL sequence to the next. The options are:

- Go to a URL manually
- Following a hyperlink
- Selecting a form button
- Selecting frame within a frameset
- Following a METAFRESH redirection.

For details on the reference types, see “Defining Sequence Steps” on page 974.

For details on the URL Sequence Monitor user interface, see “URL Sequence Monitor Settings” on page 1027.

4 Enter an Encrypted or Unencrypted Password (if required)

You can give an encrypted or unencrypted password to the URL monitor in the URL Sequence dialog box.

- To give an unencrypted password, type the password in the **password=** box in the **POST Data** text box. The password you type is displayed in the text box.
- To give an encrypted password to the URL monitor form, type the string **password** in the **Post Data Password Key** text box. Type the password itself in the **Post Data Password Value** text box. The password is encrypted.

Example - Unencrypted Password

POST Data	<pre> [[2]signInForm}.email= [[2]signInForm}.newCustomer=registeredCustomer [[2]signInForm}.password=mypassword </pre>
Post Data Password Key	<input type="text"/>
Post Data Password Value	<input type="text"/>

Example - Encrypted Password

POST Data	<pre>{{[2]signInForm}email= {{[2]signInForm}newCustomer=registeredCustomer {{[2]signInForm}password= [2]signInForm}password=</pre>
Post Data Password Key	<input type="text" value="password"/>
Post Data Password	<input type="text" value="*****"/>

5 Configure Other Settings for the Monitor

After you have added a URL Sequence Monitor, you can edit the monitor configuration settings using the same steps as with other monitors. For details, see “URL Sequence Monitor Settings” on page 1027.

Note: You can set thresholds for individual steps or for the whole monitor.

Web Transaction Monitors User Interface

This section describes:

- eBusiness Transaction Monitor Settings on page 997
- Link Check Monitor Settings on page 999
- URL Monitor Settings on page 1003
- URL Content Monitor Settings on page 1014
- URL List Monitor Settings on page 1023
- URL Sequence Monitor Settings on page 1027
- Web Script Monitor Settings on page 1038

eBusiness Transaction Monitor Settings

Description	<p>Verifies that the multiple tasks that make up an online transaction are completed properly. This includes:</p> <ul style="list-style-type: none"> ▶ Successful navigation through a series of URLs ▶ Transmission of an e-mail confirming the sequence. ▶ Logging the information into a database file. <p>Runs a sequence of other SiteScope monitors, checking that each monitor returns a status of OK. Reports an Error status if any monitor in the sequence fails.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"eBusiness Transaction Monitor Overview" on page 958

The Add/Edit eBusiness Transaction Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Items	Using the control key or equivalent, click the group or set of monitors that make up the eBusiness Transaction Monitor. As noted in the set up section above, the monitors are run in the order that they are listed in their group.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Monitor Delay	<p>Type a number of seconds to wait between running each monitor.</p> <p>This setting is useful if you need to wait for processing to occur on your systems before running the next monitor.</p>
When Error	<p>Choose how you want errors during the sequence to be handled:</p> <ul style="list-style-type: none"> ▶ Continue, run the remainder of the monitors. This runs every monitor no matter what the status of a given monitor is. ▶ Stop, do not run any of the remaining monitors. This stops running the list of monitors immediately, if a monitor returns an error. ▶ Run the last monitor. This runs the last monitor in the list. It is useful if a monitor is used for closing or logging off a session opened in a previous monitor.
Single Session	<p>Select this box if you want any URL monitors to use the same network connection and the same set of cookies.</p> <p>This is useful if you are using the eBusiness Transaction Monitor to group several URL Sequence monitors and do not want to include the login steps as part of each transaction.</p>

Link Check Monitor Settings

Description	<p>Checks the internal and external links on a Web page to insure that they can be reached. SiteScope begins checking links from a URL that you specify, verifies that linked graphics can be found, and follows HREF links to the referenced URLs. The monitor can be configured to check all of the links on your site or to check a limited number of hops from the initial URL.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Link Check Monitor Overview" on page 960

The Link Check Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
URL	<p>Type the URL that is the starting point for checking links. The link monitor retrieves the page for this URL. Next, it reads the URLs for any links on the page. It continues until it has checked all of the links on the site. Links to other servers are checked but it does not continue and check all the links of those other servers.</p> <p>Example: http://demo.thiscompany.com</p>
Search External Links	<p>Select this option to have the Link Check Monitor follow all links on each page and not just links that contain the original base URL.</p> <p>Warning: Using this option may greatly increase the number of links that are tested and the amount of time required for the monitor to run. In some cases this may cause the monitor to run for more than 24 hours without being able to complete all of the link checks. If you select this option, be sure to limit the total number of links to test using the Maximum Links setting and limit the depth of the search using the Maximum Hops setting in the Advanced Settings.</p>

GUI Element	Description
Maximum Links	The maximum number of links this monitors checks. When the maximum number of links is reached the monitor stops and reports the results of those links that were checked. Increase this number if you have a large site and want to check every link on the site.
Maximum Hops	The maximum number of internal links that SiteScope should follow from the starting URL. Limiting the number of links reduces the number of URLs that SiteScope follows and shortens the time to complete the report. SiteScope does not follow any links on external pages. Select one of the predefined choices using the Commonly Used Values list. To type your own limit, type a numeric value in the Other Values box. Example: If you set the number of hops to 3, SiteScope checks all internal pages that can be reached within 3 links from the starting URL.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Pause	The delay, in milliseconds, between each link check. Larger numbers lengthen the total time to check links but decrease the load on the server.
Timeout	The number of seconds that the URL monitor should wait for a page to begin downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status.
Authorization User Name	If the URL specified requires a user name for access, type the name in this box.
Authorization Password	If the URL specified requires a password for access, type the password in this box.

GUI Element	Description
HTTP Proxy	Optionally, a proxy server can be used to access the URL. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name to access the URL, type the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a password to access the URL, type the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Post Data	Type any form values required for the first page being checked. This is useful if you need to log in by using an HTML form to reach the rest of the site that you are checking.



URL Monitor Settings

Description	<p>Provides you with end-to-end verification that your Web server is running, serving pages correctly, and doing so in a timely manner. It tests end-to-end, so it is also able to determine whether back-end databases are available, verify the content of dynamically generated pages, check for changed content, and look for specific values from a page.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<p>Monitors must be created in a group in the monitor tree.</p>
Useful Links	<p>"URL Monitor Overview" on page 961</p>

The Add/Edit URL Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
URL	<p>Type the URL that you want to monitor.</p> <p>Example: <code>http://demo.thiscompany.com</code></p> <p>For HTTPS monitoring (secure HTTP), if the URL starts with HTTPS, then a secure connection is made using SSL. SiteScope uses Java SSL libraries for HTTPS monitoring.</p> <p>Example: <code>https://www.thiscompany.com</code></p>
Match Content	<p>Type a string of text to check for in the returned page or frameset.</p> <p>If the text is not contained in the page, the monitor displays the message content match error.</p> <p>HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for. This works for XML pages as well.</p> <p>Example: <code>< B> Hello< /B> World</code></p> <p>You can also perform a regular expression match by enclosing the string in forward slashes, with a letter <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p>Example: <code>/href=Doc\d+\.html/</code> or <code>/href=doc\d+\.html/i</code></p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression.</p> <p>Example: <code>/Temperature: (\d+)</code>. This returns the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</p> <p>Note: The search is case sensitive.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	<p>The number of seconds that the URL monitor should wait for a page to complete downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status.</p> <p>If you have checked the Retrieve Frames or Retrieve Images option, SiteScope waits for these items to be retrieved before considering the page to be fully downloaded.</p>
Retrieve Images	<p>Select this box if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by IMG, BODY (from the background property), and INPUT TYPE=IMAGE HTML tags.</p> <p>Images that appear more than once in a page are retrieved only once.</p> <p>Note: If this option is checked, each image referenced by the target URL contributes to the download time. However, if a image times out during the download process or has a problem during the download, that time is not added to the total download time.</p>
Retrieve Frames	<p>Select this box if you want SiteScope to retrieve the frames references in a frameset and count their retrieval time in the total time to download this page. Frames include those referenced by FRAME and IFRAME tags.</p> <p>If Retrieve Images is also checked, SiteScope attempts to retrieve all images in all frames.</p> <p>Note: If this option is checked, each frame referenced by the target URL contributes to the download time. However, if a frame times out during the download process or has a problem during the download, that time is not added to the total download time.</p>

GUI Element	Description
<p>Use WinInet</p>	<p>Select this option if you want to use WinInet as an alternative HTTP client for this monitor.</p> <p>Default value: Apache</p> <p>Select this option to use WinInet instead of Apache when:</p> <ul style="list-style-type: none"> ▶ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates while Apache does not. ▶ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.
<p>Error If Match</p>	<p>Type a string of text to check for in the returned page or frameset.</p> <p>If the text is contained in the page, the monitor indicates an error condition.</p> <p>HTML tags are part of a text document, so include them if they are part of the text for which you are searching.</p> <p>Example: < B> Error < /B> Message</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p>Example: /href=Doc\d+\.html/ or /href=doc\d+\.html/i</p> <p>Note: The search is case sensitive.</p>

GUI Element	Description
Check for Content Changes	<p>SiteScope records a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs.</p> <p>If the checksum changes, the monitor has a status of content changed error and go into error. If you want to check for content changes, you usually want to use compare to saved contents.</p> <p>The options for this setting are:</p> <ul style="list-style-type: none"> ➤ no content checking (default). SiteScope does not check for content changes. ➤ compare to last contents. The new checksum is recorded as the default after the initial error content changed error occurs, so the monitor returns to OK until the checksum changes again. ➤ compare to saved contents. The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor gets a content changed error and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents. ➤ reset saved contents. Takes a new snapshot of the page and saves the resulting checksum on the first monitor run after this option is chosen. After taking the snapshot, the monitor reverts to compare to saved contents mode. <p>Default value: Cleared (no content checking)</p>
HTTP Version	<p>Select this box to force SiteScope to use HTTP version 1.0 style request headers.</p> <p>When unselected, SiteScope uses HTTP Version 1.1 in the request header to the target server.</p> <p>Default value: HTTP 1.1</p>
Retries	<p>Type the number of times that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request for is a recoverable error.</p>

GUI Element	Description
Accept Untrusted Certs for HTTPS	If you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope does not have the required server certificates, you can either select this option or import the related certificates. For details on importing server certificates, see SSL Connectivity in “URL Monitor Overview” on page 961.
Accept Invalid Certs for HTTPS	Check this option if you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope has invalid server certificates. This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.
When to Encode Post Data	<p>Determines if the Post Data is encoded. Select from the following options:</p> <ul style="list-style-type: none"> ▶ Use content type. Decide to encode the post data by the content type header. If the header equals urlencoded then encode, otherwise do not encode. ▶ Force URL encoding. Always encode the post data. ▶ Force NO URL encoding. Do not encode the post data.
Authorization User Name	<p>If the URL specified requires a name and password for access, type the user name in this box.</p> <p>Alternatively, you can leave this entry blank and type the user name in the Default Authentication Credentials section on the General Preferences page. Use this alternate method to define common authentication credentials for use with multiple monitors.</p>
Authorization Password	<p>If the URL specified requires a name and password for access, type the password in this box.</p> <p>Alternatively, you can leave this entry blank and type the password in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple monitors.</p>

GUI Element	Description
Authorization Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.</p>
Authorization NTLM Domain	Type the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL.
NTLM V2	Select this option if the URL you are accessing requires authentication using NTLM version 2.

GUI Element	Description
Preemptive Authorization	<p>Select when the Authorization User Name and Authorization Password should be sent if SiteScope requests the target URL.</p> <ul style="list-style-type: none"> ▶ Use Global Preference. Select to have SiteScope use the When to Authenticate setting as specified in the Preemptive Authorization section of the General Preferences page. ▶ Authenticate first request. Select to send the user name and password on the first request SiteScope makes for the target URL. Note: If the URL does not require a user name and password, this option may cause the URL to fail. ▶ Authenticate if requested. Select to send the user name and password on the second request if the server requests a user name and password. Note: If the URL does not require a user name and password, this option may be used. <p>All options use the Authorization User Name and Authorization Password entered for this monitor instance. If these are not specified for the individual monitor, the Default Authentication Username and Default Authentication Password specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p>Note: Preemptive Authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
HTTP Proxy	<p>(Optional) A proxy server can be used to access the URL. Type the domain name and port of an HTTP Proxy Server.</p>
Proxy Server User Name	<p>If the proxy server requires a name and password to access the URL, type the name here.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>

GUI Element	Description
Proxy Server Password	<p>If the proxy server requires a name and password to access the URL, type the password here.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Proxy NTLM V2	<p>Select this option if the proxy requires authentication using NTLM version 2.</p>
Client Side Cert	<p>If you need to use a client side certificate to access the target URL, select the certificate file using the drop down menu. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You type the password for the certificate in the Client Side Cert Password box.</p> <p>Note: Client side certificate files must be copied into the <SiteScope root directory>\templates.certificates directory.</p>
Client Side Cert Password	<p>If you are using a client side certificate and that certificate requires a password, type the password in this box.</p>

GUI Element	Description
Post Data	<p>If the URL is for a POST request, type the post variables, one per line as name=value pairs.</p> <p>This option is used to verify that a form is working correctly by performing the same request that occurs when a user submits a form. See also the Match Content item for a way to verify that the correct form response was received.</p> <p>If this item is blank, a GET request is performed.</p> <p>The POST Data can be used to send cookie data. To send cookies with the request, use the format Set-cookie: cookieName=cookieValue.</p> <p>To change the content type of a post, use the format Content-Type: application/my-format.</p> <p>To hide values in the POST data, add a line like:</p> <pre>_private=_name=mysecret _value=rosebud _private=_name=mypassword _privateValue=sesame</pre> <p>and then use the following form in the POST Data:</p> <pre>s username=\$private-mysecret\$ s password=\$private-mypassword\$ </pre> <p>and SiteScope substitutes the values from the master.config into the POST Data.</p>
URL Content Encoding	<p>SiteScope retrieves the correct encoding from the server response. The default value appearing in this box should not be edited.</p> <p>Examples: Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.</p>

GUI Element	Description
Error If Redirected	Select this box if you want SiteScope to notify you if a URL is redirected. Default value: SiteScope follows redirects without reporting an error.
Show Detailed Measurement	Select this box if you want SiteScope to record a detailed breakdown of the process times involved in retrieving the requested URL. These measurements include the following: <ul style="list-style-type: none">▶ DNS lookup time. The time it takes to send a name resolution request to your DNS server until you get a reply.▶ Connection time. The time it takes to establish a TCP/IP/Socket connection to the Web server.▶ Server response time. The time after the request is sent until the first byte (rather first buffer full) of the page comes back.▶ Download time. The time it takes to download the entire page.

URL Content Monitor Settings

<p>Description</p>	<p>The URL Content Monitor is a specialized variation of the URL Monitor that can match up to ten different values from the content of a specified URL. The matched values are displayed with the status of the monitor in the monitor group table and written to the monitor log.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p>Useful Links</p>	<p>"URL Content Monitor Overview" on page 965</p>

The Add/Edit URL Content Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets)

GUI Element	Description
URL	<p>Type the URL that you want to monitor.</p> <p>Example: http://demo.thiscompany.com</p> <p>If you are monitoring a secure URL, the URL must reflect the correct transfer protocol.</p> <p>Example: https://demo.thiscompany.com</p>
Match Content	<p>Type an expression describing the values to match in the returned page. If the expression is not contained in the page, the monitor displays the message no match on content. A regular expression is used to define the values to match.</p> <p>Example: The expression /Copyright (\d*)-(\d*)/ would match two values, 1996 and 1998, from a page that contained the string Copyright 1996-1998. The returned value could be used when setting an Error if or Warning if thresholds.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	The number of seconds that the URL monitor should wait for a page to begin downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status.
Retrieve Images	<p>Select this box if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by IMG, BODY (from the background property), and INPUT TYPE=IMAGE HTML tags. Images that appear more than once in a page are only retrieved once.</p> <p>Note: If the Retrieve Images option is checked, each image referenced by the target URL contributes to the download time. However, if an image times out during the download process or has a problem during the download, that time is not added to the total download time.</p>
Retrieve Frames	<p>Select this box if you want SiteScope to retrieve the frames references in a frameset and count their retrieval time in the total time to download this page. Frames include those referenced by FRAME and IFRAME tags.</p> <p>If Retrieve Images is also checked, SiteScope attempts to retrieve all images in all frames.</p> <p>Note: If the Retrieve Frames option is checked, each frame referenced by the target URL contributes to the download time. However, if a frame times out during the download process or has a problem during the download, that time is not added to the total download time.</p>

GUI Element	Description
Use WinInet	<p>Select this option if you want to use WinInet as an alternative HTTP client for this monitor.</p> <p>Default value: Apache</p> <p>Select this option to use WinInet instead of Apache when:</p> <ul style="list-style-type: none"> ▶ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates while Apache does not. ▶ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.
Error If Match	<p>Type a string of text to check for in the returned page. If the text is contained in the page, the monitor displays content error found. HTML tags are part of a text document, so include them if they are part of the text for which you are searching.</p> <p>Example: < B> Error < /B> Message</p> <p>You can also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash, to indicate that there is no case sensitive matching.</p> <p>Example: /href=Doc\d+\.html/ or /href=doc\d+\.html/i</p> <p>Note: The search is case sensitive.</p>

GUI Element	Description
Check for Content Changes	<p>SiteScope records a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs.</p> <p>If the checksum changes, the monitor has a status of content changed error and go into error. If you want to check for content changes, you usually want to use compare to saved contents.</p> <p>The options for this setting are:</p> <ul style="list-style-type: none"> ▶ no content checking (default). SiteScope does not check for content changes. ▶ compare to last contents. The new checksum is recorded as the default after the initial error content changed error occurs, so the monitor returns to OK until the checksum changes again. ▶ compare to saved contents. The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor gets a content changed error and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents. ▶ reset saved contents. Takes a new snapshot of the page and saves the resulting checksum on the first monitor run after this option is chosen. After taking the snapshot, the monitor reverts to compare to saved contents mode. <p>Default value: Cleared (no content checking)</p>
Baseline Interval	<p>Type the number of monitor runs to be averaged for use as a Rolling Baseline. Rolling baselines are calculated for an interval equal to the time to complete the number of monitor runs entered here.</p>
HTTP Version	<p>Select this box to force SiteScope to use HTTP version 1.0 style request headers.</p> <p>Default value: HTTP 1.1</p>
Retries	<p>Type the number of times that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request for is a recoverable error.</p>

GUI Element	Description
Accept Untrusted Certs for HTTPS	If you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope does not have the required server certificates, you can either select this option or import the related certificates. For details on importing server certificates, see SSL Connectivity in “URL Content Monitor Overview” on page 965.
Accept Invalid Certs for HTTPS	Check this option if you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope has invalid server certificates. This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.
When to Encode Post Data	Determines if the Post Data is to be encoded. Select from the following options: <ul style="list-style-type: none"> ▶ Use content type. Decide to encode the post data by the content type header. If the header equals urlencoded then encode, otherwise do not encode. ▶ Force URL encoding. Always encode the post data. ▶ Force NO URL encoding. Do not encode the post data.
Authorization User Name	If the URL specified requires a name and password for access, type the name in this box.
Authorization Password	If the URL specified requires a name and password for access, type the password in this box.
Authorization Credentials	Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243. Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.
Authorization NTLM Domain	Type the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL in this step.

GUI Element	Description
NTLM V2	Select this option if the URL you are accessing requires authentication using NTLM version 2.
Preemptive Authorization	<p>Select when the Authorization User Name and Authorization Password should be sent if SiteScope requests the target URL.</p> <ul style="list-style-type: none"> ▶ Use Global Preference. Select to have SiteScope use the When to Authenticate setting as specified in the Preemptive Authorization section of the General Preferences page. ▶ Authenticate first request. Select to send the user name and password on the first request SiteScope makes for the target URL. Note: If the URL does not require a user name and password, this option may cause the URL to fail. ▶ Authenticate if requested. Select to send the user name and password on the second request if the server requests a user name and password. Note: If the URL does not require a user name and password, this option may be used. <p>All options use the Authorization User Name and Authorization Password entered for this monitor instance. If these are not specified for the individual monitor, the Default Authentication Username and Default Authentication Password specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p>Note: Preemptive Authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
HTTP Proxy	(Optional) A proxy server can be used to access the URL. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	<p>If the proxy server requires a name and password to access the URL, type the name here.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>

GUI Element	Description
Proxy Server Password	<p>If the proxy server requires a name and password to access the URL, type the password here.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Proxy NTLM V2	<p>Select this option if the proxy requires authentication using NTLM version 2.</p>
Client Side Cert	<p>If you need to use a client side certificate to access the target URL, select the certificate file using the drop down menu. Normally, this is a .pfx (.p12) type certificate that usually requires a password. You type the password for the certificate in the Client Side Cert Password box.</p> <p>Note: Client side certificate files must be copied into the SiteScope/templates.certificates directory.</p>
Client Side Cert Password	<p>If you are using a client side certificate and that certificate requires a password, type the password in this box.</p>
POST Data	<p>If the URL is for a POST request, type the post variables, one per line as name=value pairs. This option is used to verify that a form is working correctly by performing the same request that occurs when a user submits a form.</p> <p>See also the Match Content box for a way to verify that the correct form response was received.</p> <p>If this item is blank, a GET request is performed.</p> <p>Note: This item can also be used to pass cookies with the request.</p> <p>Example: "Set-cookie:<cookieName>=<cookieValue>"</p>
URL Content Encoding	<p>SiteScope retrieves the correct encoding from the server response. The default value appearing in this box should not be edited.</p> <p>Example: Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.</p>
Error If Redirected	<p>Select this box if you want SiteScope to notify you if a URL is redirected.</p> <p>Default value: SiteScope follows redirects without reporting an error.</p>

GUI Element	Description
Show Detailed Measurement	<p>Select this box if you want SiteScope to record a detailed breakdown of the process times involved in retrieving the requested URL. These times include the following:</p> <ul style="list-style-type: none"> ▶ DNS lookup time. The time it takes to send a name resolution request to your DNS server until you get a reply. ▶ Connection time. The time it takes to establish a TCP/IP/Socket connection to the Web server. ▶ Server response time. The time after the request is sent until the first byte (rather first buffer full) of the page comes back. ▶ Download time. The time it takes to download the entire page.
Match Value Labels	<p>Use this option to type labels for the matched values found in the content. The match value labels are used as variables to access retained values from the Content Match expression for use with the monitor threshold settings.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ Separate multiple labels with a comma (,). ▶ You can set up to four labels. <p>The labels are used to represent any retained values from the Content Match regular expression in the parameters available for the status threshold settings (Error if, Warning if, and Good if). These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.</p>

URL List Monitor Settings

Description	<p>The URL List Monitor is used to check a large list of URLs. This monitor is commonly used by Web hosting providers to measure the availability and performance of their customer's Web sites.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"URL List Monitor Overview" on page 968

The Add/Edit URL List Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets)

GUI Element	Description
URL List Name	<p>Type the path for the file containing the list of URLs to be monitored. This file should be a plain text file and contain only one URL per line.</p> <p>Examples:</p> <p>http://www.website.com/index.html http://www.website.com/main/customer/order.html http://www.website.net/default.htm http://www.Web pages.com/tech/support/ws/intro.html</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets)

GUI Element	Description
Server	Type the optional Server name to specify which URLs to check in the URL list. If the URLs are stored in a map format, this item is used to check a subset of the URLs from the list. Default value: All URLs in the list are checked.
Log	Type the path for the log file for this monitor. For each URL checked, an entry is added to this log file. If this item is blank, a log is not created.
Error Log	Type the path for the error log file for this monitor. For each error retrieving a URL, an entry is added to this log file. If this item is blank, a log is not created.
Threads	Type the number of threads to retrieve URLs. This is the number of simultaneous checks to perform. Increasing this number shortens the time for all of the URLs to be checked but also increases the load on the server.
Pause	Type the pause, in milliseconds, between each URL check. Decreasing this number shortens the total time required to check all of the URLs but also increases the load on the server.
Retries	Type the number of times you want SiteScope to try to reach URLs that are returning an error.
HTTP Proxy	(Optional) A proxy server can be used to access the URLs in the list. Type the domain name and port of an HTTP Proxy Server.
HTTP Proxy User Name	If the proxy server requires a name and password to access the URL, type the name here. Note: Your proxy server must support Proxy-Authenticate for these options to function.

GUI Element	Description
HTTP Proxy Password	<p>If the proxy server requires a name and password to access the URL, type the password here.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Authorization User Name	<p>If the URLs in the list require a name and password for access, type the name in this box.</p>
Authorization Password	<p>If the URLs in the list require a name and password for access, type the password in this box.</p>
Authorization Credentials	<p>Select a credential profile from the drop-down list to have SiteScope automatically supply the user name and password for the monitor. If you are creating a new template monitor, you must type the name of the credential profile. You configure credential profiles in Credential Preferences. For details, see “Configure Credential Preferences” on page 243.</p> <p>Note: If you select or type a credential profile, you do not need to type a user name and password. A credential profile takes priority over user name and password entries.</p>

GUI Element	Description
Timeout	<p>The number of seconds that the URL monitor should wait for a page to complete downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status.</p> <p>If you have checked the Retrieve Frames or Retrieve Images option, SiteScope waits for these items to be retrieved before considering the page to be fully downloaded.</p>
Use WinInet	<p>Select this option if you want to use WinInet as an alternative HTTP client for this monitor.</p> <p>Default value: Apache</p> <p>Select this option to use WinInet instead of Apache when:</p> <ul style="list-style-type: none"> ➤ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates whereas Apache does not. ➤ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.

URL Sequence Monitor Settings

Description	<p>The URL Sequence Monitor simulates a user's actions across a series of Web pages and URLs. This is particularly useful for monitoring and testing multi-page e-commerce transactions and other interactive online applications.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	<p>Monitors must be created in a group in the monitor tree.</p>
Included in Tasks	<p>"Create a URL Sequence" on page 994</p>
Useful Links	<p>"URL Sequence Monitor Overview" on page 971</p> <p>"Create a URL Sequence" on page 994</p>

The Add/Edit URL Sequence Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	<p>Type a text name for this URL Sequence Monitor instance. This text is displayed in the System Availability Management Administration and other places in the SiteScope interface.</p> <p>Default value: SiteScope creates a name based on the host, system, or URL being monitored.</p>
Frequency	<p>Select how often the URL Sequence Monitor should perform the Web Transaction. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days.</p> <p>Default value: 10 minutes.</p> <p>Minimum value: 15 seconds</p> <p>Note: Many URL sequences may take a minute or more to complete. Therefore the Frequency should be set to enable sufficient time for SiteScope to complete the actions of the sequence.</p>
Steps	<p>Use the Add Step button to define the URL sequence steps. For details, see “URL Sequence Steps Settings” on page 1033.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	The number of seconds that the URL Sequence Monitor should wait for the entire sequence to complete before timing-out. Once this time period passes, the URL Sequence Monitor logs an error and reports an error status.
Timeout Is Per Step	Select this box if you want to use the value entered for the Timeout above as the Timeout for each step of the sequence rather than for the entire transaction. If the step takes more than this time to complete, the URL Sequence Monitor logs an error and reports an error status.
Retrieve Images	<p>Select this box if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by IMG, BODY (from the background property), and INPUT TYPE=IMAGE HTML tags.</p> <p>Images that appear more than once in a page are only retrieved once.</p> <p>Note: If this option is checked, each image referenced by the target URL contributes to the download time. However, if an image times out during the download process or has a problem during the download, that time is not added to the total download time.</p>

GUI Element	Description
Retrieve Frames	<p>Select this box if you want SiteScope to retrieve the frames references in a frameset and count their retrieval time in the total time to download this page. Frames include those referenced by FRAME and IFRAME tags. If Retrieve Images is also checked, SiteScope attempts to retrieve all images in all frames.</p> <p>Note: If this option is checked, each frame referenced by the target URL contributes to the download time. However, if a frame times out during the download process or has a problem during the download, that time is not added to the total download time.</p>
Use WinInet	<p>Select this option if you want to use WinInet as an alternative HTTP client for this monitor.</p> <p>Default value: Apache</p> <p>Select this option to use WinInet instead of Apache when:</p> <ul style="list-style-type: none"> ▶ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates while Apache does not. ▶ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.
HTTP Proxy	(Optional) A proxy server can be used to access the URLs in the sequence. Type the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	<p>If the proxy server requires a name and password to access the URLs in the sequence, type the name here.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Proxy Server Password	<p>If the proxy server requires a name and password to access the URLs in the sequence, type the password here.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>

GUI Element	Description
Use Cookie Persistency	Select this option if you want to share cookies between monitor runs and between configured monitors. For details, see “Sharing Cookies Between Monitor Runs and Configured Monitors” on page 982.
Load cookies from persistency	Select this option if you want to load all relevant cookies from the persistency file and add them to the list of cookies to be sent to the server. Cookies are loaded at the beginning of the monitor run.
Save cookies to persistency	Select this option if you want to save all cookies received from the server for the current monitor run to the persistency file. Where a cookie has the same name, and its domain and path attribute string values exactly match those of an existing cookie in the persistency file, the cookie replaces the existing cookie. Cookies are saved at the end of every monitor run and the persistency file is updated.
Cookie Persistency File	Type the path and name of the cookie persistency file.
Proxy NTLM V2	Select this option if the proxy server requires authentication using NTLM version 2.
Resume at Step, If Error	<p>You use this option to specify a URL sequence step to run in the case that a URL Sequence results in an error. This is useful when a URL sequence involves a user or customer login which would result in problems if the sequence ended without logging out.</p> <p>Use the drop-down list to select a URL sequence step to jump to in the case that any step in the sequence returns an error.</p>
Execute resume step and remaining steps	If the Resume at Step option is selected and run, selection of this option causes SiteScope to run that step and continue executing the other, subsequent steps until it reaches the end of the sequence.

GUI Element	Description
Show Detailed Measurements	<p>Select this box if you want SiteScope to record a detailed breakdown of the process times involved in retrieving the requested URL. These include the following:</p> <ul style="list-style-type: none"> ▶ DNS lookup time. The time it takes to send a name resolution request to your DNS server until you get a reply. ▶ Connection time. The time it takes to establish a TCP/IP/Socket connection to the Web server. ▶ Server response time. The time after the request is sent until the first byte (rather first buffer full) of the page comes back. ▶ Download time. The time it takes to download the entire page.
HTTP Version	<p>Some systems may not be designed to accept HTTP 1.1 requests headers. If this is the case, select this option to have SiteScope use HTTP 1.0.</p> <p>Default value: HTTP version 1.1</p>
Retries	<p>Type the number of times that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request for is a recoverable error.</p>
Accept Untrusted Certs for HTTPS	<p>If you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope does not have the required server certificates, you can either select this option or import the related certificates. For details on importing server certificates, see SSL Connectivity in “URL Sequence Monitor Overview” on page 971.</p>
Accept Invalid Certs for HTTPS	<p>Check this option if you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope has invalid server certificates. This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.</p>
NTLM V2	<p>Select this option if the URL you are accessing requires authentication using NTLM version 2.</p>

URL Sequence Steps Settings

The following describes the settings used for each individual sequence step in the URL Sequence step dialog box. The scope of each of these settings is limited to the request action for the step. For example, the **User Name** and **Password** settings are only sent as part of the request being made in the step that they are defined.

GUI Element	Description
Reference Type	<p>Use these options to select how SiteScope progresses from one step of a URL sequence to the next. For details, see “Defining Sequence Steps” on page 974.</p> <p>The options include:</p> <ul style="list-style-type: none"> ▶ URL. Go to a particular URL directly. Type the URL you want SiteScope to go to in the URL box. ▶ Link. Follow a hyperlink on the page received from the previous step. Click to display all available links on the current page. Click the label or HTML text corresponding to the hyperlink that you want SiteScope to follow. If you know a link is available on the subject page but it does not appear in the drop-down list, it may that the page uses a client-side program. In this case, you may have to specify the URL manually. ▶ Form. Type data into a form received from the previous step and submit the form data to an application. Click to display the list of available form buttons. Click the name or HTML text corresponding to the form button that you want SiteScope to use. If you know a form is available on the subject page but it does not appear in the drop-down list, see “URL Sequences and Dynamic Content” on page 977. ▶ Frame. Request the content of a specific frame if the previous step returned an HTML frameset. Click the arrow on the right of the box to display all available filenames displayed in the current FRAMESET and then click the file that you want SiteScope to retrieve. ▶ Refresh. Follow an automated redirection defined by a META HTTP-EQUIV="Refresh" tag. Click the arrow on the right of the box to display all available Refresh filenames, and select the file that you want SiteScope to retrieve. Normally there is only one filename.

GUI Element	Description
POST Data (for Form)	<p>If the URL at this step issues a POST request for a form and the user has used the Form reference type (indicating that the user wants to send the form), type the post variables, one per line as name=value pairs. This option is used to verify that a form is working correctly by performing the same request that occurs when a user manually submits a form. When the form is submitted, SiteScope fills in any items that are not specified with data here with the same defaults as a browser would have chosen.</p> <p>A single name=value pair may be used to hide any data that is passed to the form, such as a password. The values entered in the POST Data text box are not encrypted and are visible to anyone. If you want to secure the value by encrypting it, use the Post Data Password Key and Post Data Password Value boxes to secure the monitor as described below.</p> <p>Note: There may be more than one form on the page.</p>
Post Data Password Key	<p>Type the name of the box that was supplied by the URL in the POST Data box. It is the name component of the name=value pair.</p>
Post Data Password Value	<p>Type the value that is required when accessing the form. This is the value component of the name=value pair. The value is encrypted using the TDES algorithm.</p> <p>For example, you want to define an encrypted password to the form that the URL monitor, gmail.com sends. The site gmail.com automatically supplies information in the POST Data text box of the URL Sequence dialog box. The Post Data Password Key may vary from site to site. The Post Data Password Key provided by gmail.com is Passwd. The Post Data Password Value is the password that you provide.</p> <p>For details on how to type an encrypted or unencrypted password, see “Enter an Encrypted or Unencrypted Password (if required)” on page 995.</p>
URL Content Encoding	<p>SiteScope retrieves the correct encoding from the server response. The default value appearing in this box should not be edited.</p> <p>Example: Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.</p>

GUI Element	Description
Match Content	<p>Type a string of text to check for in the returned page or frameset. If the text is not contained in the page, the monitor displays the message content match error.</p> <p>HTML tags are part of a text document, so include them if they are part of the text for which you are searching. This works for XML pages as well. Example: < B> Hello< /B> World</p> <p>You can also perform a regular expression match by enclosing the string in forward slashes, with a letter <i>i</i> after the trailing slash indicating case-insensitive matching. Example: /href=Doc\d+\.html/ or /href=doc\d+\.html/i</p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression. Example: /Temperature: (\d+). This returns the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</p> <p>Note: The search is case sensitive.</p>
Error If Match	<p>Type a string of text to check for in the returned page for this step. If the text is contained in the page, the monitor display the message content error found for this step's URL. The search is the same as for the Match Content box described above.</p>
User Name (for URL)	<p>If the URL specified for this step requires a name and password for access, type the user name in this box. Alternately, you can leave this entry blank and type the user name in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.</p>
Password (for URL)	<p>If the URL specified for this step requires a name and password for access, type the password in this box. Alternately, you can leave this entry blank and type the password in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.</p>

GUI Element	Description
Authorization NTLM Domain	Type the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL in this step.
Preemptive Authorization	<p>Select when the Authorization User Name and Authorization Password should be sent if SiteScope requests the target URL.</p> <ul style="list-style-type: none"> ▶ Use Global Preference. Select to have SiteScope use the When to Authenticate setting as specified in the Preemptive Authorization section of the General Preferences page. ▶ Authenticate first request. Select to send the user name and password on the first request SiteScope makes for the target URL. Note: If the URL does not require a user name and password, this option may cause the URL to fail. ▶ Authenticate if requested. Select to send the user name and password on the second request if the server requests a user name and password. Note: If the URL does not require a user name and password, this option may be used. <p>All options use the Authorization User Name and Authorization Password entered for this monitor instance. If these are not specified for the individual monitor, the Default Authentication Username and Default Authentication Password specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p>Note: Preemptive Authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
Delay	(Optional) Type how long SiteScope should wait before executing the next step of the sequence.
Step Title	(Optional) Type the text for the title of this step within the sequence monitor. The title is only displayed in the Edit URL Sequence form.

GUI Element	Description
When to Encode Post Data	<p>Determines if the Post Data is encoded. Select from the following options:</p> <ul style="list-style-type: none"> ▶ Use content type. Decide to encode the post data by the content type header. If the header equals urlencoded then encode, otherwise do not encode. ▶ Force URL encoding. Always encode the post data. ▶ Force NO URL encoding. Do not encode the post data.
Client Side Cert	<p>If you need to use a client side certificate to access the target URL, select the certificate file using the drop down menu. Client side certificate files must be copied into the SiteScope\templates.certificates directory. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You type the password for the certificate in the Client Side Cert Password box.</p>
Client Side Cert Password	<p>If you are using a client side certificate and that certificate requires a password, type the password in this box.</p>
Show Source	<p>Click to open a new browser window that displays the source code of the URL returned by the previous request. You can use this window to copy data, such as a session ID or form data, from the Web page for use in the current step. The HTML Source folding panel at the bottom of the step page can also be used to view the source of the Web page. However, some browsers do not support copying data from this panel.</p>
Show Page	<p>Click to open a new browser window that displays the URL in a regular browser view. You can use this window to match the Link and Form data displayed in the URL Sequence Monitor step dialog form with the elements as displayed on the Web page.</p>

Web Script Monitor Settings

<p>Description</p>	<p>The Web Script Monitor gives you a flexible solution for virtual end-user monitoring of all your Web-based Applications. It can monitor dynamic content, test various authentication methods, and capture each step in a transaction between virtual user and Web site. This can help identify performance and availability issues before they affect end users.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<ul style="list-style-type: none"> ▶ The Web Script Monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information. ▶ Note to HP Business Availability Center users: The Web Script Monitor is not available when working in HP Business Availability Center and cannot be configured in System Availability Management. The monitor's data cannot be reported to HP Business Availability Center. ▶ Monitors must be created in a group in the monitor tree.
<p>Useful Links</p>	<p>"Web Script Monitor Overview" on page 984</p>

The Add/Edit Web Script Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	Type a text name for this Web Script Monitor instance. This text is displayed in various locations in the SiteScope interface to identify the monitor.
Frequency	<p>Select how often the Web Script Monitor should run the script. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days.</p> <p>Note: The update interval must be a minimum of 15 seconds or longer.</p>
Web Script URL	<p>Select from the following options:</p> <ul style="list-style-type: none"> ▶ Full path Web script name. Type the full path for the VuGen script. The script must be a .zip file and the path must be a location to which the machine running SiteScope has file system access. ▶ Web script files list. Select from the list of available scripts in the directory storing your VuGen scripts. This could be the default directory <SiteScope root directory>\templates.webscripts or a directory you name in General Preferences. For details, see “SiteScope General Preferences User Interface” on page 248. <p>When the script is selected, it is copied into a SiteScope directory and the monitor no longer accesses the original location or the original script files.</p> <ul style="list-style-type: none"> ▶ If the script is changed in VuGen and you want the monitor to run the newer version of the script, you must edit the monitor and select the script again. ▶ Each script used for a Web Script Monitor must have a unique name.

GUI Element	Description
Web Script Timeout	<p>Type the time in seconds after which you want SiteScope to stop running the script if it has not successfully completed its run.</p> <p>This value must be less than the value you entered for the Frequency setting.</p>
Counters	<p>The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p>
Get Counters	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor. For the list of counters available for the monitor, see “Web Script Performance Counters” on page 1041.</p> <p>The first list of counters applies to all the transactions in the script and is called Total. The Status counter is the only counter that is in the Total list and the only counter that can be applied to all the transactions within the script. The subsequent lists are by transaction. Each transaction list includes all the available counters, enabling you to make specific selections of counters for the different transactions in the script.</p> <p>Note: Not all counters return values for all transactions.</p>

Web Script Performance Counters

The following table lists all the counter metrics available for the monitor. Not all the counters report on all the transactions.

Name	Description
Retry Time	<p>Displays the overall amount of time that passes from the moment an HTTP request is started until the moment an HTTP or TCP error message is returned.</p> <p>Retry time only relates to HTTP or TCP errors that execute a retry after the error.</p>
DNS Time	<p>Displays the average amount of time needed to resolve the DNS name to an IP address, using the closest DNS server.</p> <p>The DNS Lookup measurement is a good indicator of slow DNS resolution or other problems with the DNS server.</p>
Connection Time	<p>Displays the amount of time needed to establish an initial connection with the Web server performing the transaction.</p> <p>The connection measurement is a good indicator of problems along the network or whether the server is responsive to requests.</p>
SSL Handshaking Time	<p>Displays the amount of time taken to establish an SSL connection (includes the client hello, server hello, client public key transfer, server certificate transfer, and other optional stages). After this point, all the communication between the client and server is encrypted.</p> <p>The SSL handshaking measurement is only applicable for HTTPS communications.</p>
Network Time to First Buffer	<p>Displays the amount of time that passes from the moment the first HTTP request is sent until receipt of ACK.</p> <p>The network measurement is a good indicator of network quality (look at the time/size ratio to calculate download rate).</p>

Name	Description
Server Time to First Buffer	<p>Displays the amount of time that passes from the receipt of ACK of the initial HTTP request (usually GET) until the first buffer is successfully received back from the Web server. The server time to first buffer measurement is a good indicator of Web server delay.</p> <p>Note: Because server time to first buffer is being measured from the client, network time may influence this measurement if there is a change in network performance from the time the initial HTTP request is sent until the time the first buffer is sent.</p>
Download Time	<p>Displays the time from the receipt of the first buffer until the last byte arrives.</p> <p>Download time is a combination of server and network time, because each server (as specified by the URLs in the script) sends data over two or four connections, and therefore is usually working while data is being transmitted over the network.</p> <p>As a Web page is retrieved, its various components (images, applets, and so on) travel in data packets from server to client across the connections, so that some data packets may be traveling over the network through one of the connections, while others are being processed by the server through another connection.</p>
Client Time	Displays the time during the script run when the client is not sending or receiving data from the server.
Duration	The time in milliseconds for the transaction to be run.
Status	Displays whether the transaction passed or failed. A value of 0 is passed, a value of 1 is failed. A failed transaction could be caused by a content matching error, as set up in the VuGen script, or an http error from the server.
Size	The size in bytes received from the Web sites being monitored by the transaction.
Number of Errors	Number of errors that occurred during the transaction run.
Number of Pages	Number of pages accessed when running the transaction.

Part VI

Integration Monitors

22

Working with SiteScope Integration Monitors

Integration Monitors enable you to capture and forward data from several Enterprise Management Systems (EMS) applications and servers into HP Business Availability Center.

This chapter includes:

Concepts

- ▶ Integration Monitors Overview on page 1046
- ▶ Topology Settings on page 1049

Tasks

- ▶ Deploy Integration Monitors on page 1055

Reference

- ▶ List of Deprecated Integration Monitors on page 1057

Troubleshooting and Limitations on page 1059

Integration Monitors Overview

Integration Monitors are run by the SiteScope data collector and are used to integrate data from third-party applications (typically EMS systems) into HP Business Availability Center.

Note: Access to Integration Monitor types requires that a special SiteScope Optional License be entered on the SiteScope server.

There are two levels of configuration for collecting the data and forwarding that data to HP Business Availability Center:

- ▶ **Required:** The monitors must be configured to properly map to the monitored system and collect the required samples, whether in the form of events, measurements, or tickets. The field mapping from the monitored system is done by selecting a sample type in the Field Mapping setting and editing the corresponding script template in a text editor.
- ▶ **Optional:** The data can also be mapped to a topology to forward data to the correct CI hierarchy in HP Business Availability Center. This enables the monitor to accurately report status to the required CIs within HP Business Availability Center for use by the different applications in the product. The topology settings are configured using a Jython script that is loaded depending on the type of topology you want to create.

This section includes the following topics:

- ▶ “Integration Monitor Categories” on page 1047
- ▶ “Field Mapping Sample Types” on page 1048
- ▶ “Topology Settings” on page 1049

Integration Monitor Categories

Integration monitors can be divided into two categories.

Application-Specific Monitors

These integration monitors are designed for use with specific EMS applications. These monitors are predefined with the required field mapping and topology settings.

The monitors include:

- ▶ HP OVO Event Monitor
- ▶ HP Service Center Monitor
- ▶ NetScout Event Monitor

The scripts for both the field mapping and the topology settings can be further configured to suite the needs of your specific environment.

Note: Topology Settings are not available for the NetScout Event Monitor.

Generic Integration Monitors

Technology Integration Monitors designed for use with most EMS applications that support extraction of data from a database, log file, SNMP trap, or Web service interface.

The field mapping and topology settings for these monitors must be configured by loading the applicable scripts and editing them in a separate text editor during monitor creation.

The monitors include:

- ▶ Technology Database Integration Monitor
- ▶ Technology Log File Integration Monitor
- ▶ Technology SNMP Trap Integration Monitor
- ▶ Technology Web Service Integration Monitor

Field Mapping Sample Types

The integration monitors use field mapping scripts to correctly map the data they collect to a format recognizable by HP Business Availability Center. For the generic integration monitors, you configure and customize these mappings as required. When you select a field mapping type, you must copy the script into a text editor, make your changes, and then copy the script back into the field mapping text box.

The mappings for the application-specific monitors are not editable while configuring the monitor and it is recommended to use the out-of-the-box integration mappings already configured for those monitors.

When configuring the generic integration monitors, select from the following types of sample scripts:

- ▶ **Measurements.** Used to collect time-based data. Data collected by Integration Monitors that use the measurements sample type is integrated into HP Business Availability Center as typical SiteScope data and can be viewed in all contexts that support viewing SiteScope data (for example, Dashboard, Service Level Management, System Availability Management, user reports, and so on). Topology settings are not available when selecting the **Measurements** field mapping.
- ▶ **Events.** Used to collect data on specific events. Data collected by Integration Monitors that use the event sample type is integrated into HP Business Availability Center using the UDX framework and can be viewed in contexts that support the display of UDX data (Event Log, Dashboard, trend reports). The data can also be accessed using the HP Business Availability Center API.
- ▶ **Tickets.** Used to collect incidents and events from ticketing systems. Data collected by integration monitors that use the ticketing sample type is integrated into HP Business Availability Center and can be viewed in Dashboard and Service Level Management.

The Database, Log File, SNMP Trap, and Web Service Technology Integration Monitors can be configured to work with these sample types. You use the field mapping script templates that come prepackaged with SiteScope as a basis for creating a customized configuration required for your specific environment. When you configure an integration monitor, you select the sample type to load the required script template and edit the script template in a text editor. You then copy back the edited version of the script into the monitor's field mapping setting.

For details on customizing the field mapping scripts, see “Integration Monitor Field Mapping” on page 1161.

Topology Settings

To establish the full integration with Business Availability Center if you selected **Events** or **Tickets** as the field mapping for the monitor, you select a topology template for your integration monitor. You do this while creating an integration monitor in the Topology Settings area. The topology templates for **Hosts**, **Hosts-Applications**, and **Tickets** are specially configured with the necessary values to forward data to the required CIs in Business Availability Center's CMDB.

The topology is written as a Jython script. Jython is a language based on Python and powered by Java. For details on how to work in Jython, you can refer to these Web sites:

- <http://www.jython.org>
- <http://www.python.org>

The script includes the basis of the functions necessary to retrieve the required topology data from the monitored application. To build the topology, the script uses the sample that was created as a result of the monitor's field mapping. The script includes the mapping to forward the retrieved data to the relevant CIs in Business Availability Center.

SiteScope forwards the topology to create or update a CI under the following conditions:

- ▶ When the CI is created in SiteScope for the first time as a result of the monitor retrieving data, regardless of whether the CI exists in the CMDB.
- ▶ If there were any changes to any of the CI's properties.
- ▶ The initial monitor run after SiteScope is restarted.

This prevents overloading the CMDB with CI updates coming from the monitor.

Selecting a Topology

When working with application-specific monitors, you do not select a topology and the topology is preconfigured with the necessary data for the integration. If you selected **Measurements** as the monitor's field mapping, you also do not select a topology.

When working with generic integration monitors with field mapping of either events or tickets, you select from the following topology settings:

- ▶ **Custom.** You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or application CIs.

Note: It is recommended not to select **Custom** as this does not load a script and you must enter the entire script yourself. It is recommended to begin with either **Hosts** or **Hosts-Applications** and edit one of those scripts.

- ▶ **Hosts.** Creates a host CI with an EMS monitor CI as a leaf node.
- ▶ **Hosts-Applications.** Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI under the application CI. The host CI can also have an EMS monitor CI as a leaf node.
- ▶ **Tickets.** Creates a business service CI with an EMS monitor CI as a leaf node.

Note: The topology script must include the EMS monitor CI as the lowest leaf in the topology created by the integration.

Hosts Topology

The default topology created includes a Host CI with an EMS Monitor CI as its leaf node.



The Host CI has a monitored by relationship with the EMS Monitor CI. The EMS Monitor CI passes status onto the Host CI.

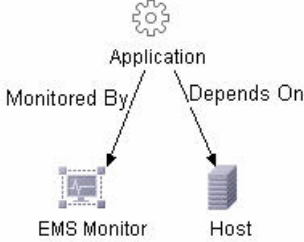
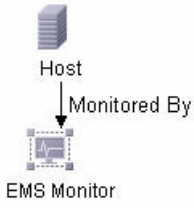
Hosts-Applications Topology

In this topology, there are two types of data that can be retrieved from the monitored system: **application** events and **system** events.

- ▶ **Application events.** This data is recognized as data affecting business services. (This event is mapped to the Application KPI for the relevant CIs.)
- ▶ **System events.** This data is all other data retrieved from the monitored application that does not affect business services. This data passes status onto the Host CI. The status may propagate to the Application CI if there is a relationship between the Host CI receiving the system event and the Application CI. (This event is mapped to the System KPI for the relevant CIs.)

If the samples forwarded belong to the category of business application events, then the status from the event is assigned to the Application CI and the Host CI does not get the status from the EMS monitor CI.

The following table illustrates the topology created for each type of event:

Topology Created for Application Event	Topology Created for System Event
 <pre> graph TD Application[Application] -- Monitored By --> EMS_Monitor[EMS Monitor] Application -- Depends On --> Host[Host] </pre>	 <pre> graph TD Host[Host] -- Monitored By --> EMS_Monitor[EMS Monitor] </pre>

If the events do not belong to the category of business application events, then the event is considered a system event.

You can configure which data is considered business application data and which data is not. You configure these instructions by editing the topology script as follows:

Search for the following strings in the topology script:

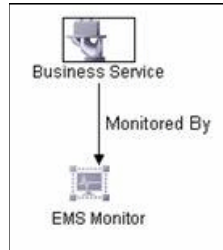
```

### EDIT THIS: Application CIs are created for all applications except
"system"
if (subject != "system"):
    
```

The variable **subject** represents the subject field in the retrieved sample (as defined in the field mapping for events). The value **system** is an example of possible values representing the data from an application that is considered 'system' data and not forwarded to the Application CI. This 'system' data is forwarded to the Host CI.

Tickets

The default topology created includes a Business Service CI with an EMS Monitor CI as its leaf node. The Business Service CI has a monitored by relationship with the EMS Monitor CI.



The EMS Monitor CI passes status onto the Business Service CI.

Editing the Topology Script

To configure the topology, you must edit the Jython script that appears in the Topology Settings area when creating an integration monitor. It is highly recommended that you copy the contents of the script into your preferred text editor, edit the script in the text editor, and then copy back the contents into the Topology Settings field for the monitor.

The **Hosts**, **Hosts-Applications**, and **Tickets** topologies are already configured with the necessary information. Following are the guidelines for editing the script if you want to create your own topology.

- It is highly recommended that you familiarize yourself with the Jython language before attempting to edit this script.
- The Jython language is sensitive to spaces and tabs and you must be careful while editing the script.
- You must leave the import section as is and only add to it.
- The main body of the script is mandatory and consists of:

```
def DiscoveryMain(Framework)
```

This main function is responsible for creating Object State Holder Vector (OSHV) results. This holds the CI data and how to map the incoming samples to the CIs.

- ▶ Each CI should have only one EMS Monitor CI as a leaf node.
- ▶ For event scripts, the following expressions must appear as the last lines in the script:

```
Framework.setUserObject("result_object",monitoredCiType)
return OSHVResult
```

The variable `monitoredCiType` is the CI type being monitored by the EMS Monitor CI that receives the event.

If the script creates more than one EMS Monitor CI for one retrieved event, you must determine to which of the CIs that event belongs and passes status. You do this by assigning the correct value to the `monitoredCiType`. For example, if the script creates one EMS Monitor CI for an Application CI and one for a Host CI, and you want the event to pass status to the Host CI, the value of the variable `monitoredCiType` should be "host".

- ▶ Use the built-in "logger" to debug the topology scripts when samples arrive. You do this by modifying the level and type of information reported to the log file. Change the log file settings in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties** file as follows:

- a Open the **log4j.properties** file in a text editor and locate the following lines in the file:

```
# Jython prints
log4j.category.PATTERNS_DEBUG=${loglevel}, integration.appender
```

Change the argument of **log4j.category.PATTERNS_DEBUG** from **`\${loglevel}** to **DEBUG**, as follows:

```
log4j.category.PATTERNS_DEBUG=DEBUG, integration.appender
```

- b Save the file. It may take a few seconds for the changes to take effect.

The results are logged to the **bac_integration.log** file.

Jython Properties File

The <SiteScope root directory>\conf\ems\jython.properties file controls many aspects of the Jython script. Generally, you do not need to edit this file. It already includes all the properties necessary for running the Jython script.

If you working in a secure Business Availability Center installation that has a certificate, you may have to modify one of the properties in this file. In this case, you must insert the following line into the file:

```
appilog.agent.Probe.BasicAuth.Realm=MyPrivateFile
```

Where myPrivateFile is a variable for the certificate realm. If you want to find out what realm a given URL belongs to, you can open the URL with a Web browser and see the first line in the popup box.

Note: When you modify the **jython.properties**, you must restart SiteScope to enable your changes to take effect.

Deploy Integration Monitors

This task describes the steps involved in deploying an integration monitor.

You can deploy integration monitors while working in:

- ▶ System Availability Management Administration
- ▶ EMS Integrations Admin which opens System Availability Management Administration
- ▶ A standalone SiteScope that reports to Business Availability Center

1 Select a SiteScope

When in System Availability Administration, select the SiteScope server from which you want to deploy the integration monitor. For details on the user interface, see “System Availability Management Administration” on page 57.

Note: This step is relevant only for users accessing SiteScope from HP Business Availability Center.

2 Create a Group for the Integration Monitor

It is highly recommended that you create special groups for the integration monitors. This enables you to more easily recognize the data that is reported to Business Availability Center as coming from the integrations.

For details on the New SiteScope Group user interface, see “New SiteScope Group Page” on page 462.

3 Configure the Integration Monitor

You must configure the monitor and add the required data for the monitor’s settings. You can choose from the following application-specific integrations:

- HP OVO Event Monitor
- HP Service Center Monitor
- NetScout Event Monitor

You can choose from the following generic integration monitors:

- Technology Database Integration Monitor
- Technology Log File Integration Monitor
- Technology SNMP Trap Integration Monitor
- Technology Web Service Integration Monitor

4 Edit Field Mappings and Topology Script

For generic integration monitors or any special customizations, you must also:

- Edit the fields mapping. For details on this topic, see “Integration Monitor Field Mapping” on page 1161.
- Edit the topology settings. For details on this topic, see “Topology Settings” on page 1049.

List of Deprecated Integration Monitors

In SiteScope version 8.5, a number of Integration Monitors were deprecated and are no longer supported.

The following Technology Integration Monitors can be used instead of the deprecated monitors:

Deprecated Monitor	Recommended Monitor
Avalon Event	Technology SNMP Trap
BMC Patrol Event	Technology SNMP Trap, Technology Log File
BMC Patrol	Technology Log File
CA Unicenter Event (1)	Technology SNMP Trap
Compaq Insight Manager Event (2)	Technology Database
HP Systems Insight Manager Event	Technology Database
Netcool Event	Technology SNMP Trap
NetIQ (3)	Technology Database
Remedy Ticketing	Technology Database
Tivoli TEC Event	Technology Database
Tivoli DM	Technology Database
WhatsUp Event (4)	Technology Log File

The following are examples of how a Technology monitor can be configured to replace a deprecated monitor:

(1) Configure CA Unicenter agents to send SNMP traps to a SiteScope host machine where a Technology replacement monitor has been configured.

(2) For Compaq Insight Manager version 7.0, configure the replacement SiteScope monitor to read from the following tables: `Notices`, `NoticeType`, `Devices`, `StringResource`, and `StringTableLarge`.

(3) For NetIQ versions 5.0 and 5.1, configure the replacement SiteScope monitor to query tables `Data` (contains raw data) and `DataHeader` (contains metadata about the objects that NetIQ monitors).

(4) For WhatsUp version 8.0, configure the replacement SiteScope monitor to read from the log file `EV-<date>.tab`.

Note: Beginning with SiteScope 8.x, the monitor configuration file `main.config` is no longer used. All functions that were supported in `main.config` are now supported in `event.config` and available in the **Fields Mapping** setting.

Troubleshooting and Limitations

The information below describes basic troubleshooting techniques and information regarding log files that may be useful when working with Integration Monitors.

Integration Monitor Logs

Integration Monitor activity is logged to `<SiteScope root directory>\logs\RunMonitor.log` and `lbac_integration.log`.

You can modify the level and type of information reported to the log file by changing the log file settings in the `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties` file. You can instruct the logging mechanism to:

- ▶ report logged information in less or greater detail than is reported by default
- ▶ log all samples sent by Integration Monitors to HP Business Availability Center
- ▶ log all received events from external EMS systems

To modify log settings:

- 1** Open the `log4j.properties` file in a text editor.
- 2** To specify that samples sent by Integration Monitors to HP Business Availability Center be logged:
 - a** Locate the following lines in the file:


```
log4j.category.EmsSamplePrinter=${loglevel}, integration.appender
log4j.additivity.EmsSamplePrinter=false
```
 - b** Change the argument of `log4j.category.EmsSamplePrinter` from `${loglevel}` to `DEBUG`, as follows:


```
log4j.category.EmsSamplePrinter=DEBUG, integration.appender
```
 - c** Save the file. It may take a few seconds for the changes to take effect.

The results are logged to the `bac_integration.log` file.

- 3 To specify that all received events from external EMS systems be logged:
 - a Locate the following lines in the file:

```
log4j.category.EmsEventPrinter=${loglevel}, monitors.appender
log4j.additivity.EmsEventPrinter=false
```
 - b Change the argument of `log4j.category.EmsEventPrinter` from `${loglevel}` to `DEBUG`, as follows:

```
log4j.category.EmsEventPrinter=DEBUG, monitors.appender
```
 - c Save the file. It may take a few seconds for the changes to take effect.

The results are logged to the `RunMonitor.log` file.

Other Log and Troubleshooting Issues

- ▶ Look for errors in `<SiteScope root directory>\logs\error.log` and in `<SiteScope root directory>\logs\bac_integration.log`.
- ▶ If samples are created and sent from SiteScope but cannot be seen in HP Business Availability Center Dashboard, Event Log, or SiteScope reports, search for the string `ERROR` or `WARN` in the `wde.logl` and `loader.logl` files in the `<HP Business Availability Center root directory>\log\mercury_wde\` directory to make sure the samples were not dropped due to missing fields or values.
- ▶ Increase the level of Dashboard logging in `<HP Business Availability Center root directory>\conf\core\Tools\log4j\EJB\ble.properties` file to verify that Dashboard is receiving samples. Locate the following parameter and change the log level status to `DEBUG`:

```
log4j.category.Trinity.BLE_SAMPLES=DEBUG, trinity.samples.appender
```

The results are logged to the `<HP Business Availability Center root directory>\log\EJBContainer\TrinitySamples.log`.

Note: Once you have determined the cause of the problem, it is recommended that you set log levels to their default settings so as not to overload the system.

Additional troubleshooting information is located in the HP Software Self-solve knowledge base (<http://h20230.www2.hp.com/selfsolve/documents>) (you must log in to the knowledge base with your HP Passport ID) and in the following sections of the documentation:

- ▶ For Technology Database Integration monitor, see “Troubleshooting the Technology Database Integration Monitor” on page 1114.
- ▶ For Technology Log File monitor, see “Troubleshooting the Technology Log File Integration Monitor” on page 1129.
- ▶ For Technology SNMP Trap monitor, see “Troubleshooting the Technology SNMP Trap Integration Monitor” on page 1142.
- ▶ For Technology Web Service Integration monitor, see “Troubleshooting the Technology Web Service Integration Monitor” on page 1156.

23

HP OVO Event Monitor

The HP OVO Event Monitor allows you to integrate an existing Hewlett-Packard OVO Server with HP Business Availability Center by transferring HP OVO events from HP OVO Server to an HP Business Availability Center server.

Note: This monitor supports:

- ▶ HP OVO/UNIX versions 8.x (x >= 24) when installed on Solaris or on HP UX platforms.
 - ▶ HP OVO/Windows versions 7.5x when installed on Windows platforms.
 - ▶ English only. It does not support I18N mode.
-

This chapter includes:

Concepts

- ▶ HP OVO Event Monitor Overview on page 1064

Tasks

- ▶ HP OVO Integration Add-on – Workflow on page 1067

Reference

- ▶ HP OVO Event Monitor User Interface on page 1075

HP OVO Event Monitor Overview

The HP OVO Event Monitor depends on an HP OVO Integration Add-on module to collect events from the HP OVO Server. The Add-on, when installed on the HP OVO Server, listens to events received by the HP OVO system and sends them to the HP OVO Event Monitor. The HP OVO Event Monitor transfers the events to an HP Business Availability Center server. The HP OVO Integration Add-on and the HP OVO Event Monitor communicate using TCP/IP networking (with a customizable TCP port).

Configuration Files

The HP OVO Event monitor uses a predefined configuration file, `<SiteScope root directory>\conf\ems\hp\event.config`, to define the processing of incoming data and to define the output sample forwarded to HP Business Availability Center. Do not modify this configuration file.

The following configuration file allows mapping between HP OVO event fields and HP Business Availability Center KPIs and can be modified: `<SiteScope root directory>\conf\ems\hp\spi2kpi.config`.

Note: If you customized this file in previous versions of SiteScope, you must manually copy this file to your SiteScope version 9.50 installation. Use the same file path as in the previous version.

There are 4 sections in this file: **system**, **network**, **application**, and **security**. These sections correspond to four predefined KPIs in HP Business Availability Center for HP OVO events. You can modify this file to meet the needs of your site.

Below is a sample `spi2kpi.config` file:

```
[system]

[network]
Application1=.*SNMP*

[application]
Application1=.*MS SQL.*
Application2=.*Oracle.*
Application3=.*Informix.*
Application4=.*Sybase.*
Application5=.*Apache.*
Application6=.*iPlanet.*
Application7=.*SUN One.*
Application8=.*MSExchange.*
Application9=.*Microsoft Exchange Server.*
Application10=.*Active Directory.*
Application11=.*IIS.*
Application12=.*WebLogic.*
Application13=.*WebSphere.*
Application14=.*Biztalk.*
Application15=.*SharePoint.*
Application16=.*R3.*

[security]
Group1=.*SECURITY.*
```

Every HP OVO event is processed and matched against the regular expression pattern:

- Application<number> pattern means that an application field from the event should be matched against the regular expression pattern.
- Group<number> pattern means that the group field from the event should be matched against the regular expression pattern.

The matching process starts at the beginning of the file and proceeds line by line until the first match is found. When a match is found, the process stops and the value of the resulting KPI is assigned to the `attr1` field of the event sample. If there is no match, the system KPI is assigned to the `attr1` field.

The order in which you list the applications and groups in this file is important because, in the event that there may be more than one match, the parser stops after the first match. For details, see “Integration Monitor Field Mapping” on page 1161.

Important: After you modify `spi2kpi.config` file, right-click the HP OVO monitor in the monitor tree, select **Edit**, and then click **OK** to close the edit monitor page. If this is not done, your changes in the configuration file are not implemented in the monitor.

Status

The status returned by the monitor is the current value of the monitor, such as:

```
Status: GOOD
Status Summary: 10 events received, connected Add-ons: 1
```

The status is logged as either **GOOD**, **WARNING**, or **ERROR**. A warning status is returned if no Add-on is connected to the monitor.

The status can be configured further using advanced options in the HP OVO Alert Monitor Configuration Form.

For information about Integration Monitor logging and troubleshooting, see “Integration Monitor Logs” on page 1059 and “Troubleshooting and Limitations” on page 1059.

For details on configuring this monitor, see “HP OVO Event Monitor User Interface” on page 1075.

HP OVO Integration Add-on – Workflow

The purpose of the HP OVO Integration Add-on is to connect to the HP OVO message infrastructure, to receive events from the HP OVO, and to forward these events to the SiteScope machine.

Note: The HP OVO Integration Add-on module is platform specific. Modules are provided for all platforms supported by OVO/UNIX version 8.24 or OVO/Windows version 7.5.

This task includes the following steps:

- “Installing the HP OVO Integration Add-on” on page 1067
- “Configuring the HP OVO Integration Add-on” on page 1069
- “Tuning the HP OVO Integration Add-on” on page 1070
- “Starting and Stopping the HP OVO Integration Add-on” on page 1072
- “Uninstalling the HP OVO Integration Add-on files from the HP OVO Server” on page 1073
- “Support in HP OVO Cluster Installation” on page 1074
- “Log File Messages” on page 1074

Installing the HP OVO Integration Add-on

Installation packages for the various platforms used below is in <SiteScope root directory>\conf\ems\hp\addon\OVO-BAC.zip file.

To install on HP-UX 11.11:

- 1** Log in as superuser to the HP OVO Server. Alternatively, use the `su` command to gain superuser permissions.
- 2** Copy **HPOvOBac-01.00.000-HPUX11.0-release.depot** installation package to `\tmp`.
- 3** Do the following command:

```
swinstall -s /tmp/HPOvOBac-01.00.000-HPUX11.0-release.depot \*
```

To install on HP-UX 11.23:

- 1** Log in as superuser to the HP OVO Server. Alternatively, use the `su` command to gain superuser permissions.
- 2** Copy `HPOvOBac-01.00.000-HPUX11.22_IPF32-release.depot` installation package to `\tmp`.
- 3** Do the following command:

```
swinstall -s /tmp/HPOvOBac-01.00.000-HPUX11.22_IPF32-release.depot \*
```

To install on Solaris 5.7 or later:

- 1** Log in as user `root` to the HP OVO Server. Alternatively, use the `su` command to gain super-user permissions.
- 2** Copy `HPOvOBac-01.00.000-SunOS5.7-release.sparc` installation package to `\tmp`.
- 3** Do the following command:

```
pkgadd -d /tmp/HPOvOBac-01.00.000-SunOS5.7-release.sparc HPOvOBac
```

To install on Windows:

- 1** Log in as user `administrator` to the HP OVO Server.
- 2** Copy `HPOvXpl-02.61.120-WinNT4.0-release.msi` and `HPOvOBac-01.00.000-WinNT4.0-release.msi` installation packages to `C:\tmp`. Do the following commands:
 - a** `msiexec /I C:\tmp\HPOvXpl-02.61.120-WinNT4.0-release.msi /qn`
 - b** `msiexec /I C:\tmp\HPOvOBac-01.00.000-WinNT4.0-release.msi /qn`

Configuring the HP OVO Integration Add-on

Once installed, the HP OVO Integration Add-on must be configured on the HP OVO Server before it can be used.

To configure the HP OVO Integration Add-on on the HP OVO Server:

- 1 Configure the host name or IP address of the SiteScope machine on which the HP OVO Event Monitor is installed:
`ovconfchg -ns opc.bac -set TargetHost <host name>`
- 2 Configure the port if you are using a port other than the default (9000):
`ovconfchg -ns opc.bac -set TargetHost <host name> -set TargetPort <port>`

Note: If you change this setting, make sure to update the HP OVO Event Monitor.

HP OVO Integration Add-on for UNIX provides a function that improves performance of internal message processing. Enabling this function improves the performance of the HP OVO Integration Add-on (and other OVO components, such as the OVO Java GUI). This function is disabled by default.

To enable improved HP-OVO Add-on performance on UNIX feature:

On the HP OVO Server, perform the following commands:

- 1 `opcsv -stop`
- 2 `ovconfchg -ovrg server -ns opc -set OPCMSGM_USE_GUI_THREAD NO_RPC`
- 3 `opcsv -start`

Tuning the HP OVO Integration Add-on

You can tune the HP OVO Integration Add-on by running utilities from the command line on the HP OVO Server.

To check the current settings:

```
ovconfget opc.bac
```

To change a parameter:

```
ovconfchg -ns opc.bac -set <variable name> <value>
```

where <variable name> and <value> are in the following table:

Variable Name	Default Value	Description
TargetHost	<empty>	Host name of the SiteScope receiver. No connection is attempted if this is empty.
TargetPort	9000	Port number of the SiteScope receiver. No connection is attempted if this is 0.
CacheMax	1000	Maximum number of messages stored in cache memory to avoid database lookups.
CacheKeep	500	If cache size reaches CacheMax , only the most-recently-used messages in CacheKeep are kept in the cache. All others are removed from the cache.
Connection Timeout	300	If no new messages or message changes are transmitted to the SiteScope receiver, the connection is closed after this number of seconds.
MinWaitTime	15	If the connecting to the SiteScope receiver failed, the HP OVO Integration Add-on waits this many seconds the first time after connection failure before retrying to connect. The wait time is doubled after each retry, up to MaxWaitTime .

Variable Name	Default Value	Description
MaxWaitTime	120	Maximum number of seconds to wait after connection failures before retry. When doubling the wait time after connection failures exceeds MaxWaitTime, the wait time is no longer doubled and MaxWaitTime is used instead.
MaxQueueLen	1000	If the connection to the SiteScope receiver has been lost and new messages or message changes come in, these messages and message changes are buffered in a memory queue. If the number of entries in that queue reaches MaxQueueLen, the oldest entries are removed from the queue.
NodeKeepTime	900	The HP OVO Integration Add-on looks up IP addresses from host names. In addition, OVO/Windows host names also need to be looked up from the OVO database. These IP addresses (and host names on OVO/Windows) are stored in a memory cache. Because host names and IP addresses of systems can be changed, entries in that cache are invalidated (and afterwards looked up again) after NodeKeepTime seconds.

Changing any of these variables automatically updates the HP OVO Integration Add-on. There is no need to stop and restart the HP OVO Integration Add-on process.

Starting and Stopping the HP OVO Integration Add-on

The HP OVO Integration Add-on must be started after it is installed.

To start and stop the HP OVO Integration Add-on on UNIX platforms:

On UNIX platforms, the HP OVO Integration Add-on is controlled by OpenView Control Daemon (ovcd). Using the command line tool **ovc** on the HP OVO Server, perform the command:

```
ovc -stop <or start> opc2bac
```

If the HP OVO Integration Add-on disconnects from SiteScope during operation, it tries to reconnect to the SiteScope at regular intervals. In the meantime, events are stored within the HP OVO Integration Add-on.

If the HP OVO Integration Add-on terminates from SiteScope during operation, the events not yet sent to SiteScope are lost.

Note: Because the Integration Add-on is linked with HP OVO API libraries, it may be necessary to stop the Integration Add-on before installing HP OVO patches, and start it after the patch installation.

To start or stop the HP OVO Integration Add-on on Windows platforms:

On Windows platforms, the HP OVO Integration Add-on runs as a Windows service.

- 1** On the HP OVO Server, click **Start > Settings > Control Panel > Administrative Tools > Services**.
- 2** Select the service **HP OpenView Operations Message Forwarder to BAC**.
- 3** Click **Start** or **Stop**.

Uninstalling the HP OVO Integration Add-on files from the HP OVO Server

If you must uninstall the HP OVO Integration Add-on files from the HP OVO Server, perform the following procedure:

To remove the HP OVO Integration Add-on files from an HP OVO Server on HP-UX platform:

- 1 Log in as superuser.
- 2 Perform the command:
`swremove HPOvOInt.HPOVOBAC`

To remove the HP OVO Integration Add-on files from an HP OVO Server on Solaris platform:

- 1 Log in as superuser.
- 2 Perform the command:
`pkgrm HPOvOBac`

To remove the HP OVO Integration Add-on files from an HP OVO Server on Windows platform:

- 1 On the HP OVO Server, click **Start > Settings > Control Panel > Administrative Tools > Services**.
- 2 Remove the following installed programs:
 - HP OpenView Operations, BAC Integration
 - HP OpenView Cross Platform Components (unless used by other installed programs). If this program is in use, you receive an error message and the removal fails.

Support in HP OVO Cluster Installation

The HP OVO Integration Add-on is supported in an HP OVO cluster environment. You can do the following tasks:

- Install HP OVO Integration Add-on on each cluster node separately.
- Configure HP OVO Integration Add-on on each cluster node separately. All configuration settings on all cluster nodes must be identical.
- Uninstall HP OVO Integration Add-on on each cluster node separately.

Log File Messages

On UNIX platforms, the HP OVO Integration Add-on writes log messages into the log file `/var/opt/OV/logSystem.txt`.

On Windows platforms, `System.txt` is in directory `<DataDir>\log` where `<DataDir>` is the data directory chosen during OVO/Windows installation (for example, `C:\Program Files\HP OpenView\Data`).

Log file entries use the process name `opc2bac` for messages logged by the HP OVO Integration Add-on.

HP OVO Event Monitor User Interface

Description	<p>The HP OVO Event Monitor allows you to integrate an existing HP OpenView installation with HP Business Availability Center by transferring HP OVO messages from HP OVO Server to an HP Business Availability Center server.</p> <p>This monitor supports:</p> <ul style="list-style-type: none">▶ HP OVO versions 8.24 or later, when installed on Solaris 5.7 and later or when installed on HP UX 11.11 or HP UX 11.23▶ HP OVO versions 7.5 or later when installed on Windows <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none">▶ In the monitor tree, right-click a group and select Add Monitor.▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"HP OVO Event Monitor" on page 1063

The Add/Edit Integration HP OVO Event Monitor configuration file templates page includes the following areas:

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Frequency	<p>Set how often SiteScope attempts to run the action defined for the monitor instance. Each monitor run updates the status of the monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p>Default value: 10 minutes</p> <p>Minimum value: 15 seconds</p>
HP OVO Add-on TCP Port	<p>Type the TCP port number as configured in the HP OVO Integration Add-on.</p> <p>Default value: 9000</p>
Field Mapping	<p>The out-of-the-box integration script that enables the monitor to correctly map the data it collects from the OVO installation to a format recognizable by the monitor and HP Business Availability Center.</p> <p>It is recommended to use the field mapping as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the file in the following location and edit it in your preferred text editor: <SiteScope root directory>\conf\ems\hp\event.config. To enable any changes, you must edit the monitor to reload the edited script.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1161.</p>

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Script	<p>The out-of-the-box integration script that creates a topology in Business Availability Center that is based on the data collected from the OVO installation. The script is based on the Jython scripting language (Python enabled by Java) and enables the integration between the data the monitor collects from the OVO system and Business Availability Center’s applications.</p> <p>It is recommended to use the topology settings as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the following file: <SiteScope root directory>\conf\ems\scripts\EMS_hpovo.py and edit it in your preferred text editor. To enable any changes, you must edit the monitor to reload the edited script.</p> <p>For more details on editing the script, see “Topology Settings” on page 1049.</p>

24

HP ServiceCenter Monitor

The HP ServiceCenter Monitor enables you to integrate Incident Management data from an HP ServiceCenter installation with HP Business Availability Center.

Note: This monitor supports ServiceCenter version 6.2.1.

This chapter includes:

Concepts

- ▶ HP ServiceCenter Monitor Overview on page 1080

Tasks

- ▶ HP ServiceCenter Integration – Workflow on page 1081

Reference

- ▶ HP ServiceCenter Monitor User Interface on page 1084

HP ServiceCenter Monitor Overview

Use the HP ServiceCenter monitor in SiteScope to integrate the incident data from HP ServiceCenter' Incident Management to HP Business Availability Center.

Incident Management automates reporting and tracking an incident, or groups of incidents, associated with a business enterprise. Incident Management enables you to identify types of incidents, such as software, equipment, facilities, network, and so on, and track the resolution process of these incidents.

The HP ServiceCenter monitor forwards business service-related incidents to HP Business Availability Center to create configuration items (CIs) based on those incidents. By default, CIs are created only for those incidents that are considered business service incidents in HP ServiceCenter. If necessary for your environment, you can configure the integration scripts to map other incidents as well.

The integration maps the incidents to the business service CIs created and creates a monitored by relationship between the HP ServiceCenter monitor CI and the business service CI. The monitor integrates the incident data into samples which are forwarded to HP Business Availability Center applications, such as Dashboard and Service Level Management.

Example Integration

When an incident is opened in ServiceCenter on a service, reporting that the service is unavailable, it is forwarded to HP Business Availability Center by the SiteScope monitor. The following happens in Business Availability Center:

- ▶ The Business Service CI is created with an EMS Monitor CI if it did not already exist.
- ▶ If the Business Service CI did exist, the incident is added to the existing CI along with an EMS Monitor CI.
- ▶ You can view the service CI with this open incident in Dashboard.
- ▶ You can drill down to access HP ServiceCenter.

For more detailed information on the CIs and related KPIs, see “Integration with HP ServiceCenter” in *Using Service Level Management*.

For details on configuring this monitor, see “HP ServiceCenter Monitor User Interface” on page 1084.

HP ServiceCenter Integration – Workflow

The following are the steps necessary to configure the integration:

- “Define HP ServiceCenter Tables for External Access” on page 1081
- “Edit Clocks and Incident Management Configuration Files” on page 1082
- “Create the JAR File” on page 1082
- “Create a Corresponding HP ServiceCenter User” on page 1083
- “Configure an HP ServiceCenter Monitor in SiteScope” on page 1083

1 Define HP ServiceCenter Tables for External Access

To enable the integration, you must provide external access to the clocks table and the probe_summary table in HP ServiceCenter. This can be done:

- Manually within HP ServiceCenter if the tables are used for other external internal integrations. For details, refer to the HP ServiceCenter documentation.
- Using the configuration file supplied with HP Business Availability Center. For details on how to perform this task, see “Enable External Access to the clocks and probe_summary Tables” on page 1083.

2 Edit Clocks and Incident Management Configuration Files

If any changes were made to the clocks table and/or the incident management tables in HP ServiceCenter, then the same changes must be made to the corresponding configuration files in SiteScope. The configuration files included with the integration are configured with the same parameters as the default tables in HP ServiceCenter. However, if these tables were changed in any way, they must be edited on the SiteScope side as follows:

- a** Access the files from the following location:
 - **<SiteScope root directory>\conf\ems\peregrine\incidentAttributesMapping.config**
 - **<SiteScope root directory>\conf\ems\peregrine\clockAttributesMapping.config**
- b** Edit the files using a text editor. Follow the mapping directions as documented in the files.

3 Create the JAR File

This batch file creates and compiles the files needed for the HP ServiceCenter monitor. The result of this batch is a **peregrine.jar** that is placed in the **WEB_INF\lib** directory. To create the JAR file:

- a** Stop the SiteScope service on the SiteScope machine.
- b** Ensure that JDK version 1.4.1 or higher is installed.
- c** Set **JAVA_HOME** system variable to the JDK directory (for example **C:\j2sdk1.4.1_03**).
- d** Update the **build.properties** file with the wsdl locations.
- e** Double-click the **<SiteScope root directory>\conf\ems\peregrine\create-peregrine-jar.bat** file to run the batch.
- f** If you are running SiteScope on a UNIX system, the file extension is **.sh** and you must run the file from the full path in a terminal window.
- g** Restart the SiteScope service on the SiteScope machine.

4 Create a Corresponding HP ServiceCenter User

You must create a dedicated user in HP ServiceCenter that should be used solely for the purposes of this HP Business Availability Center/SiteScope integration.

The user created in HP ServiceCenter must share the same time zone as the SiteScope machine. This user must also use the same date format that SiteScope uses: **dd/mm/yy**.

Use the value for the **Username** and **Password** fields when configuring the monitor as you created in HP ServiceCenter.

5 Configure an HP ServiceCenter Monitor in SiteScope

You can create this monitor:

- ▶ directly in SiteScope
- ▶ using the System Availability Management Administration portal in HP Business Availability Center
- ▶ using the EMS Integrations Administration portal in HP Business Availability Center

Enable External Access to the clocks and probe_summary Tables

The following are the steps necessary to enable external access to the clocks and probe_summary tables.

To use the configuration file to enable external access to the clocks and probe_summary tables:

- 1** Locate the configuration file **Ticketing_Integration_extaccess_def.unl** on the HP Business Availability Center DVD and copy it to a local directory.
- 2** Open the HP ServiceCenter client that is attached to the server used for the the integration.
- 3** Select **Toolkit > Database Manager**.
- 4** In the menu on the upper right side of the Database Manager, select **Import/Load**.

- 5 Select the **Ticketing_Integration_extaccess_def.unl** file.
- 6 Click the **Load FG** button.

HP ServiceCenter Monitor User Interface

Description	<p>This monitor enables you to integrate HP ServiceCenter incidents with HP Business Availability Center. The incidents in ServiceCenter are forwarded to Business Availability Center as samples by this SiteScope monitor. The samples are used in reporting data to the Business Availability Center applications, such as Service Level Management and Dashboard.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ➤ In the monitor tree, right-click a group and select Add Monitor. ➤ In the Contents tab for the group, click Add Monitor.
Important Information	<p>Monitors must be created in a group in the monitor tree. It is recommended to create a special group for the ServiceCenter integration.</p>
Included in Tasks	<p>"HP ServiceCenter Integration – Workflow" on page 1081</p>
Useful Links	<p>"HP ServiceCenter Monitor" on page 1079</p>

The Add/Edit Integration HP ServiceCenter Monitor settings page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
HP ServiceCenter Web Service Endpoint	<p>The URL for the HP ServiceCenter Web Service. Use the following format: <code><protocol>://<host_name>:<port>/</code> where host_name is the name of the ServiceCenter server and port is the port number of the ServiceCenter server.</p> <p>Example: <code>http://HOST:12670/sc61server/ws</code> (for HP ServiceCenter 6.2) and <code>http://HOST:13080/sc62server/ws</code> (for HP ServiceCenter 7.0)</p> <p>Note: This field replaces the Host and Port fields that were in previous versions of SiteScope. When upgrading to SiteScope 9.50, you must change all instances of HP ServiceCenter monitors to specify the HP ServiceCenter URL instead.</p>
Username	The designated user name created in HP ServiceCenter for the purpose of this integration monitor.
Password	The password of the designated user created in HP ServiceCenter for the purpose of this integration monitor.

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Field Mapping	<p>The out-of-the-box integration script that enables the monitor to correctly map the data it collects from the ServiceCenter installation to a format recognizable by the monitor and HP Business Availability Center.</p> <p>It is recommended to use the field mapping as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the following file: <SiteScope root directory>\conf\ems\peregrine\ticket.config and edit it in your preferred text editor. To enable any changes, you must edit the monitor to reload the edited script.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1161.</p>
Test Script	<p>Click to test the field mapping script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events are forwarded to Business Availability Center.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>
Synch Flag	<p>Select to enable the monitor to query ServiceCenter to retrieve all Incidents Changes from the time specified in the Synch Time setting.</p> <p>Default value: Cleared</p> <p>Note: This flag is reset to cleared after each time the monitor retrieves the data from ServiceCenter.</p>

GUI Element	Description
Synch Time	Type a value indicating the time from which the monitor retrieves incidents. Type a value only when Synch Flag is selected.
Incident Management (probsummary table) query	<p>Type the text to add to the query that the monitor sends to ServiceCenter. You can add to the query to determine which Incidents the monitor retrieves.</p> <p>Default value: type="bizservice". The query is set to retrieve only those incidents opened on CIs of type bizservice.</p> <p>Note: The syntax for the query must be specified by the ServiceCenter application. It is recommended that you consult the ServiceCenter help to create the text to add to the query and to test the query using the advanced search found in the ServiceCenter application.</p>
Incident Open State	<p>Indicates the initial state as defined in ServiceCenter for the incident lifecycle.</p> <p>Default value: Open</p>

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<p>Script</p>	<p>The out-of-the-box integration script that creates a topology in Business Availability Center that is based on the data collected from the ServiceCenter installation. The script is based on the Jython scripting language (Python enabled by Java) and enables the integration between the data the monitor collects from the ServiceCenter system and Business Availability Center's applications.</p> <p>It is recommended to use the topology settings as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the following file: <SiteScope root directory>\discovery\scripts\ems\EMS_peregrine.py and edit it in your preferred text editor. To enable any changes, you must edit the monitor for SiteScope to reload the edited script.</p> <p>For more details on editing the script, see “Topology Settings” on page 1049.</p>
<p>Test Script</p>	<p>Click to test the topology script. This test gives you the results of what events are forwarded to Business Availability Center and what topology is mapped.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

25

NetScout Event Monitor

The NetScout Event Monitor monitors alerts received from the NetScout nGenius server and forwards them to HP Business Availability Center. This provides a way to centralize data collection, display, and alerting for the conditions for which you may otherwise be unaware until something more serious happens.

This chapter includes:

Concepts

- NetScout Event Monitor Overview on page 1090
- System Requirements on page 1091

Tasks

- NetScout Integration – Workflow on page 1092

Reference

- NetScout Event Monitor User Interface on page 1093

NetScout Event Monitor Overview

The NetScout Event Monitor is designed to collect SNMP Trap data from NetScout nGenius servers. Each time that the monitor is run, SiteScope checks traps that have been received since the last time the monitor ran and reports the results to HP Business Availability Center.

The NetScout Event Monitor forwards alerting instances to HP Business Availability Center to create configuration items (CIs) based on application or host alarms in NetScout.

The integration maps the alarms to the NetScout CIs created and creates a monitored by relationship between the NetScout Event monitor CI and the the relevant host, interface, or application CI. The monitor integrates the incident data into samples that are forwarded to HP Business Availability Center applications, such as Dashboard and Service Level Management.

Note: For information about Integration Monitor logging and troubleshooting, see “Integration Monitor Logs” on page 1059 and “Troubleshooting and Limitations” on page 1059.

For details on configuring this monitor, see “NetScout Event Monitor User Interface” on page 1093.

System Requirements

The following are important guidelines and requirements for using the NetScout Event Monitor to forward alerts to HP Business Availability Center.

- ▶ The NetScout nGenius server must be configured to send traps to the SiteScope server.

Note: The NetScout Event Monitor uses port 162 for receiving traps. If another application or process on the machine where SiteScope is running has bound this port, the monitor reports an **Address in use** error and the monitor type is unavailable.

- ▶ SiteScope must be registered with an HP Business Availability Center installation. The SiteScope must have a profile defined in the HP Business Availability Center installation prior to enabling the registration in the SiteScope interface. To verify registration or to re-register SiteScope with HP Business Availability Center, see the Integration Preferences page in the Preferences container.
- ▶ The NetScout Event Monitor must be set to synchronize integration monitor data with HP Business Availability Center. You can use the configuration file for the NetScout Event Monitor to control the data that is sent from SiteScope to HP Business Availability Center. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 1161.

NetScout Integration – Workflow

The following are the tasks necessary to integrate data from a NetScout system and view the NetScout data in a way that is customized to your needs.

This task includes the following steps:

- “Configure a NetScout Event Monitor in SiteScope” on page 1092
- “Activate NetScout EMS Integration in Business Availability Center” on page 1092

1 Configure a NetScout Event Monitor in SiteScope

You can create this monitor:

- directly in SiteScope
- using the System Availability Management Administration portal in HP Business Availability Center

2 Activate NetScout EMS Integration in Business Availability Center

Activate the assignment rules in Business Availability Center. For details on how to perform this task, see “NetScout nGenius Integration” in *Solutions and Integrations*.

NetScout Event Monitor User Interface

Description	<p>The NetScout Event Monitor monitors alerts received from the NetScout nGenius server and forwards them to HP Business Availability Center. This provides a way to centralize data collection, display, and alerting for the conditions for which you may otherwise be unaware until something more serious happens.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"NetScout Event Monitor" on page 1089

The Add/Edit NetScout Event Monitor page includes the following areas:

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Frequency	<p>Set how often SiteScope attempts to run the action defined for the monitor instance. Each monitor run updates the status of the monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p>Default value: 10 minutes</p> <p>Minimum value: 15 seconds</p>

GUI Element	Description
Field Mapping	<p>The out-of-the-box integration script that enables the monitor to correctly map the data it collects from the NetScout installation to a format recognizable by the monitor and HP Business Availability Center.</p> <p>This script is not editable.</p>
Run Alerts	<p>Select the method for running alerts:</p> <ul style="list-style-type: none"> ▶ If for each event received from NetScout system is chosen, then the monitor triggers alerts for every matching entry found. <p>Note: If for each event received from NetScout system is selected as the alert method, when the NetScout Monitor is run, the monitor never reports a status of error or warning, regardless of the results of the content match or even if the target SNMP Trap is not found.</p> ▶ If the once, after all events from NetScout system were received method is selected, then the monitor counts up the number of matches and triggers alerts based on the Error if and Warning if thresholds defined for the monitor in the Threshold Setting section.
EMS Time Difference	<p>Type a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded.</p> <p>Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.</p>

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Script	<p>The out-of-the-box integration script that creates a topology in Business Availability Center that is based on the data collected from the NetScout installation. The script is based on the Jython scripting language (Python enabled by Java) and enables the integration between the data the monitor collects from the NetScout system and Business Availability Center's applications.</p> <p>It is recommended to use the topology settings as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the following file: <SiteScope root directory>\discovery\scripts\ems\ems_netscout.py and edit it in your preferred text editor. To enable any changes, you must edit the monitor to reload the edited script.</p> <p>For more details on editing the script, see "Topology Settings" on page 1049.</p>

26

Technology Database Integration Monitor

The Technology Database Integration Monitor allows you to collect event and time series data from database tables used by Enterprise Management Systems (EMS) by performing a query through a JDBC connection. The data retrieved is then processed and sent to HP Business Availability Center as samples (one sample for each row that was returned by a SQL query).

This chapter includes:

Concepts

- ▶ Technology Database Integration Monitor Overview on page 1098
- ▶ Setup Requirements on page 1099

Tasks

- ▶ Integrate Database Data into HP Business Availability Center on page 1102

Reference

- ▶ Technology Database Integration Monitor User Interface on page 1105
- ▶ Troubleshooting and Limitations on page 1114

Technology Database Integration Monitor Overview

Use the Technology Database Integration Monitor to integrate database records into HP Business Availability Center. The following are examples of data that can be integrated into HP Business Availability Center using the Technology Database Integration Monitor:

- ▶ Events from monitoring applications event tables or views.
- ▶ Open tickets from ticketing systems applications.
- ▶ Time series from monitoring applications measurement tables.

Each time the Technology Database Integration Monitor runs, it returns the monitors status, the time it took to perform the query, the number of rows in the query result set, and the first two fields in the first row of the result and writes them in the monitoring log file.

What Data Is Forwarded

The Technology Database Integration Monitor uses a user-defined query and enumerating field name, field type, and initial value. While the query provided by the user is used to define a search criterion on the database, the enumerating field is used so that events are forwarded only once. Using an initial value allows you to specify an initial threshold value for the events that should be forwarded.

For example, if **Enumerating Field Type** uses DATE and **Start from value** uses 2003-20-03 12:00:00, only events that happened after the specified date are forwarded in the first run of the monitor. In subsequent monitor runs, the highest value for the DATE field found is used to verify that only new events are forwarded.

You use the field mapping script selected for the Technology Database Integration Monitor to control the data that is sent from SiteScope to Business Availability Center. See the section on “Integration Monitor Field Mapping” on page 1161 for more details on the file structure and syntax.

Before setting up the Technology Database Integration Monitor, you should be clear about the purpose and usage of the data in HP Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

For details on configuring the monitor, see “Technology Database Integration Monitor User Interface” on page 1105.

Setup Requirements

The steps for setting up a Technology Database Integration Monitor vary according to what database software you are trying to query. The following is an overview of the requirements for using the Technology Database Integration Monitor:

- ▶ You must use one of the database drivers supplied by default, or install or copy a compatible database driver or database access API into the required SiteScope directory location. The supplied drivers include:
 - ▶ **com.inet.tds.TdsDriver.** TDS driver is from i-net Software for Microsoft SQL databases. This driver is deployed with SiteScope.
 - ▶ **com.mercury.jdbc.sqlserver.SQLServerDriver.** DataDirect driver is from DataDirect Technologies. It is an alternative to the TDS driver for those Microsoft SQL databases that use Windows NT authentication. This driver is deployed with SiteScope.
 - ▶ **com.inet.ora.OraDriver.** OraDriver driver is from Oracle for Oracle databases. This driver is deployed with SiteScope.

Other database driver packages are available as compressed (zipped) archive files or .jar files. Database drivers in this form must not be extracted. Rather, put them into the **<SiteScope root directory>\java\lib\ext** subdirectory.

- ▶ You must know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers.

Database Connection URLs for this monitor are:

- ▶ **`jdbc:inetdae:<hostname>:<port>`**
where `<hostname>` is the name of the host where the database is running and `<port>` is the port on which the database interfaces with the driver.
- ▶ **`jdbc:mercury:sqlserver://<hosthost>:1433;DatabaseName=master;AuthenticationMethod=type2`**
where `<hostname>` is the name of the host where the database is running.
- ▶ **`jdbc:oracle:thin:@<hostname>:<port>:<dbname>`**
where `<hostname>` is the name of the host where the database is running, `<port>` is the port on which the database interfaces with the driver, and `<dbname>` is the name of the Oracle database instance.
- ▶ The database you want to query must be running, have a database name defined, and have at least one named table created in the database. In some cases, the database management software needs to be configured to enable connections by using the middleware or database driver.
- ▶ You need a valid user name and password to access and perform a query on the database. In some cases, the machine and user account that SiteScope is running on must be given permissions to access the database.
- ▶ You must know a valid SQL query string for the database instance and database tables in the database you want to query. Consult your database administrator to work out required queries to use.
- ▶ When adding the monitor to SiteScope, in the Main Settings area, you must select a field mapping script and load the script for the monitor. Copy the contents of the script into your preferred text editor, and edit the script to define the event handlers for this monitor instance. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 1161.

Notes and Limitations

- ▶ When Windows authentication is used to connect to the database, configure SiteScope using the following settings:
 - ▶ JDBC Connection string: **jdbc:mercury:sqlserver://<hosthost>:1433; DatabaseName=master;AuthenticationMethod=type2**
 - ▶ JDBC driver: **com.mercury.jdbc.sqlserver.SQLServerDriver**.
 - ▶ Leave the **Database User name** and **Database Password** fields empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.
- ▶ When referring to data arriving from the Technology Database Integration Monitor in the config file, use the column name prefixed by the dollar sign (\$).

For example, for the following database query:

```
SELECT height,width FROM some_table WHERE width > 0
```

You can refer to the columns returned using the labels \$height and \$width. The names of the columns are case sensitive.

Integrate Database Data into HP Business Availability Center

This section provides the overall flow for setting up the Technology Database Integration Monitor to work with HP Business Availability Center. If you need more information on performing any of the steps, see the sections on “Setup Requirements” on page 1099, and “Technology Database Integration Monitor User Interface” on page 1105.

To integrate database data into HP Business Availability Center:

- 1 Use a database client to connect to the relevant software database. Identify which tables contain the required events/metrics (the software schema documentation may help you with this).
- 2 A JDBC database driver is a prerequisite for setting up the monitor. It is recommended to use the following JDBC drivers:

- For SQL Server:

Database Connection URL=

jdbc:inetdae:<DatabaseHostName>:<Port>?database=<Database Name>

Database Driver=com.inet.tds.TdsDriver

- For Oracle:

Database Connection URL=

jdbc:inetora:<DatabaseHostName>:<Port>:<Database Instance Name>

Database Driver=com.inet.ora.OraDriver

- 3 Use the SiteScope Database Connection tool as follows:
 - Verify the driver can be loaded and that it successfully connects.
 - Add a username and password to verify that a connection can be established to the database.
 - Add a naive query. Refine the query until you get all the required events/metrics required for usage in HP Business Availability Center.

- 4 Add a Technology Database Integration Monitor in HP Business Availability Center, as described in “Technology Database Integration Monitor User Interface” on page 1105. Note the following:
 - When adding the new monitor to a group, it is recommended that you use a dedicated group for integration monitors only.
 - If you do not see the **Integration Monitors** category, make sure you have an EMS Option License for your SiteScope.
- 5 While editing the settings for the Technology Database Integration Monitor, note the following:
 - **Main Settings.** Make sure that a value is specified for all parameters in the **Main Settings** area.
 - **Name.** It is recommended that the monitor name include the name of the integrated software.
 - **Connection parameters.** Fill all connection parameters for connecting to the database: **Database Connection URL**; **Database User Name**; **Database Password**; **Database Driver**
 - **SELECT/FROM/WHERE query clauses.** **SELECT** and **FROM** are mandatory. It is recommended that you build your query with the SiteScope Database Connection tool *before* defining the monitor. When specifying the **SELECT** clause, the value given for **Enumerating Field** must appear in the clause.
 - **Frequency.** Define how often the monitor should query the database. The maximum number of rows that the monitor can retrieve on each cycle is 5000; this is to prevent an out-of-memory exception. The frequency should therefore be set so that the monitor retrieves a maximum of 5000 rows per cycle.

You can edit the maximum number of rows in the **Advanced Settings** section for the monitor.
 - **Enumerating Field parameters.** Fill in details for the enumerating field.

- ▶ **Field Mappings.** Copy the content of the field mapping script you select into a text editor, edit the script to retrieve data from the monitored application, and copy the script back into the field mapping script area. For details on editing the script, see “Integration Monitor Field Mapping” on page 1161.
 - ▶ **Topology Settings.** Optionally, you can configure the topology setting by creating a Jython script that creates a topology in HP Business Availability Center to match your EMS system. For details on this topic, see “Topology Settings” on page 1049.
- 6 View the data in HP Business Availability Center:
- ▶ **Events integration.** You can view events in Dashboard (add a Generic EMS source, then add the Generic EMS NodeFactory to a view), System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
 - ▶ **Metrics integration.** You can view the data in any application that supports SiteScope data, including SiteScope reports.
 - ▶ If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <HP Business Availability Center root directory>\bin.

To troubleshoot problems with data arriving to HP Business Availability Center, see “Troubleshooting and Limitations” on page 1114.

 **Technology Database Integration Monitor User Interface**

Description	<p>The Technology Database Integration Monitor allows you to collect event and time series data from database tables used by Enterprise Management Systems (EMS) by performing a query through a JDBC connection. The data retrieved is then processed and sent to HP Business Availability Center as samples (one sample for each row that was returned by a SQL query).</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Technology Database Integration Monitor" on page 1097

The Add/Edit Technology Database Integration Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Database Connection URL	Type a URL to a database connection (sometimes referred to as an Authentication string). One way to create a database connection is to use ODBC to create a named connection to a database. For example, first use the ODBC control panel to create a Data Source Name (DSN) called <code>test</code> under the system DSN tab. Then, type <code>jdbc:odbc:test</code> in this box as the connection URL. Alternatively, use the supplied Microsoft SQL or Oracle driver to connect to the Database.
Database Driver	Type the driver used to connect to the database. Use the Fully Qualified Class Name of the JDBC driver you are using.
SELECT	Type the SELECT clause to be used in the SQL query. Type <code>*</code> for all fields or a comma separated list of column names to be retrieved from the database. When specifying the SELECT clause, the column used as the enumerating field must appear in the clause.
FROM	Type the FROM clause to be used in the SQL query. Type a table name or a comma separated list of tables from which the selected columns should be extracted.
WHERE	Type the WHERE clause to be used in the SQL query. This is an optional field which allows you to define the select criteria. Leaving it empty results in retrieving all the rows from the table defined in the FROM option.

GUI Element	Description																				
OS Integrated Security	<p>Check this check box if you want to use the user name and password from Windows' user authentication to access the database. Entries in the Database Username and Database Password are ignored.</p> <p>If this parameter is checked, you must use the DataDirect driver as your database driver.</p>																				
Database User Name	Type the user name used to login to the database.																				
Database Password	Type a password used to login to the database.																				
Enumerating Field	<p>Type a name for a database field that can be used to order the events that are returned from the database query.</p> <p>Note: The column used as enumerating field must be included in the SELECT clause.</p>																				
Enumerating Field Type	<p>Type the type of field used to order the result set. This can be a DATE field, an INTEGER field, a DOUBLE floating point numeral field, or a LONG field.</p> <p>The following table maps SQL types to the required enumerating field type.</p> <table border="1" data-bbox="621 894 1163 1310"> <thead> <tr> <th data-bbox="621 894 849 928">SQL Type</th> <th data-bbox="849 894 1163 928">Enumerating Field Type</th> </tr> </thead> <tbody> <tr> <td data-bbox="621 928 849 963">SMALLINT</td> <td data-bbox="849 928 1163 963">INTEGER</td> </tr> <tr> <td data-bbox="621 963 849 998">INTEGER</td> <td data-bbox="849 963 1163 998">INTEGER / LONG</td> </tr> <tr> <td data-bbox="621 998 849 1032">BIGINT</td> <td data-bbox="849 998 1163 1032">LONG</td> </tr> <tr> <td data-bbox="621 1032 849 1067">NUMERIC</td> <td data-bbox="849 1032 1163 1067">LONG</td> </tr> <tr> <td data-bbox="621 1067 849 1102">DOUBLE</td> <td data-bbox="849 1067 1163 1102">DOUBLE</td> </tr> <tr> <td data-bbox="621 1102 849 1137">DECIMAL</td> <td data-bbox="849 1102 1163 1137">DOUBLE</td> </tr> <tr> <td data-bbox="621 1137 849 1171">FLOAT</td> <td data-bbox="849 1137 1163 1171">DOUBLE</td> </tr> <tr> <td data-bbox="621 1171 849 1206">TIMESTAMP</td> <td data-bbox="849 1171 1163 1206">TIMESTAMP</td> </tr> <tr> <td data-bbox="621 1206 849 1241">DATE</td> <td data-bbox="849 1206 1163 1241">TIMESTAMP</td> </tr> </tbody> </table>	SQL Type	Enumerating Field Type	SMALLINT	INTEGER	INTEGER	INTEGER / LONG	BIGINT	LONG	NUMERIC	LONG	DOUBLE	DOUBLE	DECIMAL	DOUBLE	FLOAT	DOUBLE	TIMESTAMP	TIMESTAMP	DATE	TIMESTAMP
SQL Type	Enumerating Field Type																				
SMALLINT	INTEGER																				
INTEGER	INTEGER / LONG																				
BIGINT	LONG																				
NUMERIC	LONG																				
DOUBLE	DOUBLE																				
DECIMAL	DOUBLE																				
FLOAT	DOUBLE																				
TIMESTAMP	TIMESTAMP																				
DATE	TIMESTAMP																				

GUI Element	Description
<p>Initial Enumerating Value</p>	<p>Type an initial value to be used as a condition for the initial run of this monitor instance. For example, if you specify the Enumerating Field Type as a field type DATE and you type a value of 2000-31-01 12:00:00 in the Start from value field, only records that were added to the database after the specified date are forwarded.</p> <p>Note: The value of this field cannot be edited.</p>
<p>Sample Type</p>	<p>Select from the following sample types for this integration:</p> <ul style="list-style-type: none"> ▶ Events. For details, see “Configuring Field Mapping for Event Samples” on page 1164. ▶ Measurements. For details, see “Configuring Field Mapping for Measurement Samples” on page 1170. ▶ Tickets. For details, see “Configuring Field Mapping for Ticket Samples” on page 1173.
<p>Load File</p>	<p>Click to load the script that is applicable to the sample type selected above.</p>

GUI Element	Description
Field Mapping	<p>The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring.</p> <p>The mapping itself is not editable in the UI. You must copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1161.</p>
Test Script	<p>Click to test the field mapping script. It is highly recommended that you test the script before running the monitor. This test gives you the results in a separate window of what events or measurements are forwarded to Business Availability Center.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
EMS Server Name	<p>If you are reporting monitor data to an installation of HP Business Availability Center, type a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in an HP Business Availability Center report.</p> <p>Syntax exceptions: Use only alphanumeric characters for this entry. You can type the name of the monitored server or a description of the database to be used to identify the host.</p>
Max Rows	<p>Specify the maximum number of rows the monitor retrieves from the database for each monitor cycle.</p> <p>Default value: 5000 rows</p> <p>If the number of result rows exceeds the set maximum, the monitor retrieves the remaining rows (those that exceeded the maximum) on future cycles, until all result rows are retrieved.</p> <p>The value should be sufficient to keep up with database table growth, yet small enough to avoid <code>java.lang.OutOfMemoryException</code> errors. Further, monitor run frequency should also be considered. Make sure that the rate at which data is collected by the monitor—which is dependent on both monitor run frequency and network/system speed—is greater than, or equal to, the rate of data insertion on the monitored system.</p>

GUI Element	Description
EMS Time Difference	<p>Type a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded.</p> <p>Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.</p>

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Topology template	<p>Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propagates its status to the CIs mapped in this topology.</p> <p>Select from:</p> <ul style="list-style-type: none"> ▶ Custom. You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the available topology. ▶ Hosts. Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the topology. ▶ Hosts-Applications. Creates a topology with an application CI and a host CI and an EMS monitor CI as the leaf node under each application CI and host CI. <p>Note: It is recommended not to select Custom as this does not load a script and you must enter the entire script yourself. It is recommended to begin with either Host or Host and Application and edit one of those scripts. When editing the topology, you must ensure that an EMS Monitor CI is created as the leaf node to any CI that receives samples from the integration.</p> <p>For more details, see “Topology Settings” on page 1049.</p>
Load Script	<p>Click to load the required Jython script for the topology you selected in the Topology template option. If you selected Custom, there is no script to load.</p>

GUI Element	Description
Script	<p>The contents of the script are visible in this box. However, it is highly recommended not to edit the contents of the script here. You must copy the contents of the script into your preferred text editor, edit the script as needed, and then copy the contents back into this box.</p> <p>Note: The Jython script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see “Topology Settings” on page 1049.</p>
Test Script	<p>Click to test the topology script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is created. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Troubleshooting and Limitations

- ▶ Check for errors in `<SiteScope root directory>\logs\RunMonitor.log` and in `<SiteScope root directory>\logs\error.log`.
- ▶ Change the log level to DEBUG in `<SiteScope root directory>\conf\core\Tools\log4j\PlanJava\log4j.properties`, to watch outgoing samples.

Change the line:

```
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
```

to:

```
log4j.category.EmsEventPrinter= DEBUG, ems.appender.
```

The log file to look at is:

```
<SiteScope root directory>\logs\RunMonitor.log
```

- ▶ If samples are created and sent from SiteScope, but the data is not seen in **Dashboard/Event Log/SiteScope reports**, look in `<HP Business Availability Center root directory>\log\mercury_wde\wdeIgnoredSamples.log` to make sure the samples were not dropped due to missing fields or values.
- ▶ Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine:
`<HP Business Availability Center root directory>\conf\core\tools\log4j\mercury_wde\wde.properties`

Change the log level parameter to DEBUG in the following lines:

- ▶ `log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender`
- ▶ `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender`

Look at the corresponding log files:

- ▶ `<HP Business Availability Center root directory>\logs\mercury_wde\wdeIgnoredSamples.log`
- ▶ `<HP Business Availability Center root directory>\logs\mercury_wde\wdePublishedSamples.log`

27

Technology Log File Integration Monitor

The Technology Log File Integration Monitor watches for specific entries added to a log file of an Enterprise Management System (EMS) application by trying to match against a regular expression. From each matched entry, one sample is created and sent to HP Business Availability Center. Each time the monitor runs, it examines log entries added since the last time it ran.

This chapter includes:

Concepts

- ▶ Technology Log File Integration Monitor Overview on page 1116
- ▶ Setup Requirements on page 1117

Tasks

- ▶ Integrate Log File Data into HP Business Availability Center on page 1118

Reference

- ▶ Technology Log File Integration Monitor User Interface on page 1120

Troubleshooting and Limitations on page 1129

Technology Log File Integration Monitor Overview

The Technology Log File Integration Monitor is useful for automatically extracting data from log files and sending the data to HP Business Availability Center. For example, you can use this monitor to forward information from Hewlett Packard Network Node Manager to Business Availability Center.

Each time that it runs this monitor, SiteScope starts from the point in the file where it stopped reading the last time it ran. This insures that you are notified only of new entries and speeds the rate at which the monitor runs.

When using a regular expression to match against a specific line in the log, it is possible to use regular expression back references to select the data to be forwarded to Business Availability Center. For details on using back references, see “Retaining Content Match Values” on page 1505.

What Data Is Collected

The Technology Log File Integration monitor sends to Business Availability Center data that is extracted from any row that matched against the **Content Match** regular expression.

Before setting up the Technology Log File Integration Monitor, you should be clear about the purpose and usage of the data in HP Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

The specific data that is forwarded to HP Business Availability Center is controlled by the field mapping script. You use this script to specify the preferred value fields that you want forwarded. For more details on selecting the script and the file structure and syntax, see “Integration Monitor Field Mapping” on page 1161.

For details on configuring the monitor, see “Technology Log File Integration Monitor User Interface” on page 1120.

Setup Requirements

The following are requirements for using the Technology Log File Integration Monitor to forward data to Business Availability Center:

- ▶ You must have the format and syntax of the log file that you want to monitor. You must construct a **Content Match** regular expression to match on the entries in the log file that contain the data you want to monitor and forward to Business Availability Center. For examples of regular expressions, see “Examples for Log File Monitoring” on page 1511.
- ▶ When adding the monitor to SiteScope, in the Main Settings area, you must select a field mapping script and load the script for the monitor. Copy the contents of the script into your preferred text editor, and edit the script to define the event handlers for this monitor instance. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 1161.

Note: When referring to data arriving from the Technology Log File Integration monitor in the configuration file, use the number corresponding to the back reference returned prefixed by the label `$group`.

For example, for the **Content Match** expression:

```
/([0-9]{2})\s([A-Z]*) ([a-z]*) /
```

and the corresponding Log file text that contains:

```
21 HELLO world
```

you can refer in the config file to three retained values (back references) as follows, where the number appended to the end of the `$group` label corresponds to the order of the parentheses in the expression:

```
$group0 = (21)
```

```
$group1 = (HELLO)
```

```
$group2 = (world)
```

Integrate Log File Data into HP Business Availability Center

This section provides the overall flow for setting up the Technology Log File Integration Monitor to work with HP Business Availability Center. If you need more information on performing any of the steps, see the sections on “Setup Requirements” on page 1117, or “Technology Log File Integration Monitor User Interface” on page 1120.

To integrate log file data into HP Business Availability Center:

- 1** Open the relevant software log file, and identify which lines describe events or metrics. Build your regular expression with the SiteScope Regular Expression tool. Use the tool to:
 - match against the line you wish to use.
 - make sure that values extracted correctly from the line.
- 2** Add a Technology Log File Integration Monitor in HP Business Availability Center. Note the following:
 - When adding the new monitor to a group, it is recommended that you use a dedicated group for integration monitors only.
 - If you do not see the **Integration Monitors** category, make sure you have an EMS Option License for your SiteScope.
- 3** While editing the settings for the Technology Log File Integration Monitor, note the following:
 - **Main Settings.** Make sure that a value is specified for all parameters in the **Main Settings** area.
 - **Name.** It is recommended that the monitor name include the name of the integrated software.

- ▶ **Log File Pathname and Server:**
 - ▶ The file name can include a variable name (for example: `s/c:\temp\EV-$year$-$0month$-$0day$.tab/`).
 - ▶ When reading a file on a remote UNIX machine, define a remote UNIX connection; you can then select the UNIX machine from the **Server** list.
 - ▶ When reading a file on a remote Windows machine, type the UNC path in the **Log File Pathname** box (SiteScope should run under a privileged user for the machine that holds the file), and leave the **Server** box empty.
 - ▶ **Frequency.** Specify how often the monitor should query the log file.
 - ▶ **Content Match (regular expression).** Surround values you wish to extract with parenthesis. It is recommended that you build your content match with the SiteScope Regular Expression tool before defining the monitor.
 - ▶ **Field Mappings.** Copy the content of the field mapping script you select into a text editor, edit the script to retrieve data from the monitored application, and copy the script back into the field mapping script area. For details on editing the script, see “Integration Monitor Field Mapping” on page 1161.
 - ▶ **Topology Settings.** Optionally, you can configure the topology setting by creating a Jython script that creates a topology in HP Business Availability Center to match your EMS system. For details, see “Topology Settings” on page 1049.
- 4** It is recommended that you perform optimization of the regular expression after completing setup of the Technology Log File Integration Monitor (for example, to check for problems with use of quantifiers such as `.*`). Optimization is done with the SiteScope Regular Expression tool. Update the monitor with any corrections.

5 View the data in HP Business Availability Center:

- ▶ **Events integration.** You can view events in Dashboard (add a Generic EMS source, then add the Generic EMS NodeFactory to a view), System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- ▶ **Metrics integration.** You can view the data in any application that supports SiteScope data, including SiteScope reports.
- ▶ If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <HP Business Availability Center root directory>bin.

To troubleshoot problems with data arriving to HP Business Availability Center, see “Troubleshooting and Limitations” on page 1129.

Technology Log File Integration Monitor User Interface

<p>Description</p>	<p>Technology Log File Integration Monitor watches for specific entries added to a log file of a Enterprise Management System (EMS) application by trying to match against a regular expression. From each matched entry, one sample is created and sent to HP Business Availability Center. Each time the monitor runs, it examines log entries added since the last time it ran.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p>Useful Links</p>	<p>“Technology Log File Integration Monitor” on page 1115</p>

The Add/Edit Technology Log File Integration Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Frequency	<p>Select how often the Technology Log File Integration Monitor checks the log file for data to forward to HP Business Availability Center.</p> <p>Default value: 10 minutes</p> <p>Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ The update interval must be a minimum of 15 seconds or longer. ▶ It is possible to define a monitor with zero frequency. However this monitor runs only if activated manually or according to the frequency of the composite or e-business transaction monitor including it.
Servers	<p>Choose the server where the log file you want to monitor is located. Use the drop-down list to select a server from the list of UNIX remote servers that are available to SiteScope.</p>

GUI Element	Description
Log File Pathname	<p>Type the path to the log file you want to extract data from.</p> <ul style="list-style-type: none"> ▶ Remote UNIX. For reading log files on remote UNIX machines, the path must be relative to the home directory of UNIX user account being used to login to the remote machine. Select Preferences > UNIX Servers for information about which UNIX user account is being used. ▶ Remote Windows NT/2000 through NetBIOS. You can also monitor log files by including the UNC path to the remote log file. For example, <code>\\remoteserver\sharedfolder\filename.log</code>. This requires that the user account under which SiteScope is running has permission to access the remote directory using the UNC path. If a direct connection using the operating system is unsuccessful, SiteScope tries to match the <code>\\remoteserver</code> with servers currently defined as remote NT connection profiles (displayed in the Microsoft Windows Remote Preferences servers list). If an exact match is found for <code>\\remoteserver</code> in the remote NT connection profiles, SiteScope tries to use this connection profile to access the remote log file. If no matching server name is found, the monitor reports that the remote log file can not be found. ▶ Remote NT through SSH. You must select the remote server using the Server selection above. It is not necessary to select a remote Windows server if you are using NetBIOS to connect to remote Windows servers. <p>Optionally, you can use a regular expression to insert date and time variables. For example, you can use a syntax of <code>s/ex\$shortYear\$\$0month\$\$0day\$.log/</code> to match date-coded IIS log file names.</p>

GUI Element	Description
Content Match	<p>Type the text to look for in the log entries. You can also use regular expression in this entry to match text patterns.</p> <p>Unlike the content match function of other SiteScope monitors, the Log File Monitor content match is run repeatedly against the most recent content of target log file until all matches are found. This means the monitor not only reports if the match was found but also how many times the matched pattern was found.</p> <p>To match text that includes more than one line of text, add an s search modifier to the end of the regular expression.</p>
Sample Type	<p>Select from the following sample types for this integration:</p> <ul style="list-style-type: none"> ▶ Events. For details, see “Configuring Field Mapping for Event Samples” on page 1164. ▶ Measurements. For details, see “Configuring Field Mapping for Measurement Samples” on page 1170. ▶ Tickets. For details, see “Configuring Field Mapping for Ticket Samples” on page 1173.
Load File	<p>Click to load the script that is applicable to the sample type selected above.</p>
Field Mapping	<p>The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring.</p> <p>The mapping itself is not editable in the UI. You must copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1161.</p>

GUI Element	Description
Test Script	<p>Click to test the field mapping script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
No Error if File Not Found	Select this box if you want this monitor to remain in good status, if the file is not found.
Log File Encoding	If you are reading a log file whose encoding is different than the SiteScope machine's default encoding, specify the log file encoding.

GUI Element	Description
Run Alerts	<p>Select the method for running alerts for this monitor:</p> <ul style="list-style-type: none"> ▶ Select for each log entry matched to have the monitor trigger alerts for each and every matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error). <p>Note: When the Technology Log File Integration Monitor is run with this alert method selected, the monitor never displays an error or warning status in the SiteScope interface, regardless of the results of the content match or even if the target log file is not found. The monitor triggers alerts if one or more matching entries are found and the Error if or Warning if thresholds are defined accordingly in the Advanced Options section (for example, setting Error if to the default of matchCount > 0).</p> ▶ Select once, after all log entries have been checked to have the monitor count up the number of matches and trigger alerts one time based on the Error if and Warning if thresholds defined for the monitor in the Advanced Options section. <p>Note: By default, selecting this option causes SiteScope to send one alert message if one or more matches are found, but the alert does not include any details of the matching entries. To have SiteScope include the matching entries, you must associate the monitor with an alert definition that has the property <matchDetails> in the alert template. This special template property is used to populate the alert with the details of all the matching entries. You use this for e-mail alerts or other alert types that work with template properties.</p> <p>E-mail alert templates are stored in the <SiteScope root directory>\templates.mail directory.</p>

GUI Element	Description
<p>EMS Time Difference</p>	<p>Type a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.</p>

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Topology template	<p>Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propagates its status to the CIs mapped in this topology.</p> <p>Select from:</p> <ul style="list-style-type: none"> ▶ Custom. You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or EMS monitor CIs. ▶ Hosts. Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the topology. ▶ Hosts-Applications. Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI as leaf nodes of the application CI. The host CI also has an EMS monitor CI as a leaf node. <p>Note: It is recommended not to select Custom as this does not load a script and you must enter the entire script yourself. It is recommended to begin with either Host or Host and Application and edit one of those scripts.</p> <p>For more details, see “Topology Settings” on page 1049.</p>
Load Script	<p>Click to load the required Jython script for the topology you selected in the Topology template option. If you selected Custom, there is no script to load.</p>

GUI Element	Description
Script	<p>The contents of the script are visible in this box. However, it is highly recommended not to edit the contents of the script here. You must copy the contents of the script into your preferred text edit, edit the script as needed, and then copy the contents back into this box.</p> <p>Note: The Jython script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see “Topology Settings” on page 1049.</p>
Test Script	<p>Click to test the topology script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is mapped. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Troubleshooting and Limitations

- ▶ Check for errors in **<SiteScope root directory>\logs\RunMonitor.log** and in **<SiteScope root directory>\logs\error.log**.
- ▶ Change the log level to DEBUG in **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties**, to watch outgoing samples.

Change the line:

```
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
to:
```

```
log4j.category.EmsEventPrinter= DEBUG, ems.appender.
```

The log file to look at is:

<SiteScope root directory>\logs\RunMonitor.log

- ▶ If samples are created and sent from SiteScope, but the data is not seen in **Dashboard/Event Log/SiteScope reports**, look in **<HP Business Availability Center root directory>\log\mercury_wde\wdeIgnoredSamples.log** to make sure the samples were not dropped due to missing fields or values.
- ▶ Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine:
<HP Business Availability Center root directory>\conf\core\tools\log4j\mercury_wde\wde.properties

Change the log level parameter to DEBUG in the following lines:

- ▶ `log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender`
- ▶ `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender`

Look at the corresponding log files:

- ▶ **<HP Business Availability Center root directory>\logs\mercury_wde\wdeIgnoredSamples.log**
- ▶ **<HP Business Availability Center root directory>\logs\mercury_wde\wdePublishedSamples.log**

28

Technology SNMP Trap Integration Monitor

The Technology SNMP Trap Integration Monitor watches for SNMP traps received by SiteScope from third-party Enterprise Management Systems (EMS). For each SNMP trap that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the SNMP trap values.

The third-party EMS systems must be configured to send traps to the SiteScope server.

This chapter includes:

Concepts

- ▶ Technology SNMP Trap Integration Monitor Overview on page 1132
- ▶ Setup Requirements on page 1133

Tasks

- ▶ Integrate SNMP Trap Data into HP Business Availability Center on page 1134

Reference

- ▶ Technology SNMP Trap Integration Monitor Settings on page 1136

Troubleshooting and Limitations on page 1142

Technology SNMP Trap Integration Monitor Overview

The Technology SNMP Trap Integration Monitor is useful for integrating traps that your external devices create into the HP Business Availability Center framework. For example, you can use this monitor to forward information from Hewlett Packard Network Node Manager to Business Availability Center. See “Integration with HP Network Node Manager” on page 1157 for more information.

What Data Is Collected

The Technology SNMP Trap Integration Monitor collects data that is extracted from any SNMP trap received by SiteScope and sends notifications to HP Business Availability Center containing preferred values from the original SNMP trap.

Before setting up the Technology SNMP Trap Integration Monitor, you should be clear about the purpose and usage of the data in HP Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

The specific data that is forwarded to HP Business Availability Center is controlled by the field mapping script. You use this script to specify the preferred value fields that you want forwarded. For more details on selecting the script and the file structure and syntax, see “Integration Monitor Field Mapping” on page 1161.

For details on configuring the monitor, see “Technology SNMP Trap Integration Monitor Settings” on page 1136.

Setup Requirements

The following are requirements for using the Technology SNMP Trap Integration Monitor to forward data to Business Availability Center:

- ▶ When adding the monitor to SiteScope, in the Main Settings area, you must select a field mapping script and load the script for the monitor. Copy the contents of the script into your preferred text editor and edit the script to define the event handlers for this monitor instance. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 1161.

Note: All the received traps are saved to **snmptrap.log** in **<SiteScope root directory>\logs**. When referring to data arriving from the Technology SNMP Trap Integration Monitor in the config file, use the names from the **snmptrap.log** file, prefixed with the dollar sign (\$).

For example:

Use the **\$oid** to refer to the **oid** value of the trap, **\$var1** to refer to the variable bound as the first variable in trap, and **\$var2** for variable bound as second variable in trap.

-
- ▶ The SNMP agents you want to monitor must be configured to send SNMP traps to the SiteScope host. Consult with the system administrator or applicable product documentation for more about SNMP configuration.

Note: The Technology SNMP Trap Integration Monitor uses port 162 for receiving traps. If another application or process on the machine where SiteScope is running has bound this port, the monitor reports an **Address in use** error and the monitor type is unavailable. You must terminate the process or service that is using the port, and restart SiteScope afterwards.

Integrate SNMP Trap Data into HP Business Availability Center

This section provides the overall flow for setting up the Technology SNMP Trap Integration Monitor to work with HP Business Availability Center. If you need more information on performing any of the steps, see the sections on “Setup Requirements” on page 1133, and “Technology SNMP Trap Integration Monitor Settings” on page 1136.

To integrate SNMP trap data into HP Business Availability Center:

- 1 Configure the relevant software to send SNMP traps to the SiteScope machine.
- 2 Open the SiteScope SNMP Trap tool and watch if the traps are received.

If you do not see any traps, make sure that the SNMP trap port is available for the SiteScope: Stop SiteScope, and verify that the SNMP trap port (162) is available—`netstat -na | find "162"` shows no output. (To see which process uses this port, you can download `tcpview` from www.sysinternals.com.)

If the port is busy, locate the program that uses it (often the Microsoft SNMP Trap Service) and terminate it. Restart SiteScope.
- 3 Add a Technology SNMP Trap Integration Monitor in HP Business Availability Center, as described in “Technology SNMP Trap Integration Monitor Settings” on page 1136. Note the following:
 - ▶ When adding the new monitor to a group, it is recommended that you use a dedicated group for integration monitors only.
 - ▶ If you do not see the **Integration Monitors** category, make sure you have an EMS Option License for your SiteScope.
- 4 While editing the settings for the Technology SNMP Trap Integration Monitor, note the following:
 - ▶ **Main Settings.** Make sure that a value is specified for all parameters in the **Main Settings** area.
 - ▶ **Name.** It is recommended that the monitor name include the name of the integrated software.

- ▶ **Field Mappings.** Copy the content of the field mapping script you select into a text editor, edit the script to retrieve data from the monitored application, and copy the script back into the field mapping script area. For details on editing the script, see “Integration Monitor Field Mapping” on page 1161.
 - ▶ **Topology Settings.** Optionally, you can configure the topology setting by creating a Jython script that creates a topology in HP Business Availability Center to match your EMS system. For details, see “Topology Settings” on page 1049.
- 5** You can view SNMP traps in the **Tools** link or in `<SiteScope root directory>\logs\snmptrap.log`. (For a better understanding of what SNMP traps are, refer to: www.snmpblink.org.)
- 6** View the data in HP Business Availability Center:
- ▶ **Events integration.** You can view events in Dashboard (add a Generic EMS source, then add the Generic EMS NodeFactory to a view), System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
 - ▶ **Metrics integration.** You can view the data in any application that supports SiteScope data, including SiteScope reports.
 - ▶ If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under `<HP Business Availability Center root directory>\bin`.

To troubleshoot problems with data arriving to HP Business Availability Center, see “Troubleshooting and Limitations” on page 1142.

Technology SNMP Trap Integration Monitor Settings

<p>Description</p>	<p>The Technology SNMP Trap Integration Monitor watches for SNMP traps received by SiteScope from third-party Enterprise Management Systems (EMS).</p> <p>For each SNMP trap that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the SNMP trap values.</p> <p>The third-party EMS systems must be configured to send traps to the SiteScope server.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ➤ In the monitor tree, right-click a group and select Add Monitor. ➤ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p>Useful Links</p>	<p>"Technology SNMP Trap Integration Monitor" on page 1131</p>

The Add/Edit Technology SNMP Trap Integration Monitor page includes the following areas:

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Frequency	<p>Set how often SiteScope attempts to run the action defined for the monitor instance. Each monitor run updates the status of the monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p>Default value: 10 minutes. Minimum value: 15 seconds</p>
Sample Type	<p>Select from the following sample types for this integration:</p> <ul style="list-style-type: none"> ▶ Events. For details, see “Configuring Field Mapping for Event Samples” on page 1164. ▶ Measurements. For details, see “Configuring Field Mapping for Measurement Samples” on page 1170. ▶ Tickets. For details, see “Configuring Field Mapping for Ticket Samples” on page 1173.
Load File	<p>Click to load the script that is applicable to the sample type selected above.</p>
Field Mapping	<p>The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring.</p> <p>The mapping itself is not editable in the UI. You must copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1161.</p>

GUI Element	Description
<p>Test Script</p>	<p>Click to test the field mapping script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>
<p>Run Alerts</p>	<p>Choose the method for running alerts:</p> <ul style="list-style-type: none"> ▶ If for each SNMP Trap received from EMS system is chosen, then the monitor triggers alerts for every matching entry found. <p>When the Technology SNMP Trap Integration Monitor is run in the for each SNMP Trap received from EMS system alert method, the monitor never reports a status of error or warning, regardless of the results of the content match or even if the target SNMP Trap is not found.</p> <ul style="list-style-type: none"> ▶ If once, after all SNMP Traps from EMS system were received is chosen, then the monitor counts up the number of matches and triggers alerts based on the Error If and Warning If thresholds defined for the monitor in the Advanced Settings section.

GUI Element	Description
EMS Time Difference	<p>Type a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded.</p> <p>Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.</p>

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Topology template	<p>Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propagates its status to the CIs mapped in this topology.</p> <p>Select from:</p> <ul style="list-style-type: none"> ▶ Custom. You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or EMS monitor CIs. ▶ Hosts. Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the topology. ▶ Hosts-Applications. Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI as leaf nodes of the application CI. The host CI also has an EMS monitor CI as a leaf node. <p>Note: It is recommended not to select Custom as this does not load a script and you must enter the entire script yourself. It is recommended to begin with either Host or Host and Application and edit one of those scripts.</p> <p>For more details, see “Topology Settings” on page 1049.</p>
Load Script	<p>Click to load the required Jython script for the topology you selected in the Topology template option. If you selected Custom, there is no script to load.</p>

GUI Element	Description
Script	<p>The contents of the script are visible in this box. However, it is highly recommended not to edit the contents of the script here. You must copy the contents of the script into your preferred text edit, edit the script as needed, and then copy the contents back into this box.</p> <p>Note: The Jython script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see “Topology Settings” on page 1049.</p>
Test Script	<p>Click to test the topology script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is mapped. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Troubleshooting and Limitations

The following sections provide information on troubleshooting for the Technology SNMP Trap Integration Monitor, and verifying the communication paths:

- ▶ “Basic Troubleshooting Guidelines” on page 1142
- ▶ “Verify SNMP Trap Reception to SiteScope” on page 1143
- ▶ “Common Problems and Solutions” on page 1144

Basic Troubleshooting Guidelines

- ▶ Check for errors in `<SiteScope root directory>\logs\RunMonitor.log` and in `<SiteScope root directory>\logs\error.log`.
- ▶ Change the log level to DEBUG in `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties`, to watch outgoing samples.

Change the line:

```
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
```

to:

```
log4j.category.EmsEventPrinter= DEBUG, ems.appender.
```

The log file to look at is: `<SiteScope root directory>\logs\RunMonitor.log`

- ▶ Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine: `<HP Business Availability Center root directory>\conf\core\tools\log4j\mercury_wde\wde.properties`

Change the log level parameter to DEBUG in the following lines:

- ▶ `log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender`
- ▶ `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender`

Look at the corresponding log files:

- ▶ <HP Business Availability Center root directory>\logs\mercury_wde\wdeIgnoredSamples.log
- ▶ <HP Business Availability Center root directory>\logs\mercury_wde\wdePublishedSamples.log

Verify SNMP Trap Reception to SiteScope

You can verify that SiteScope is receiving SNMP traps from other management systems using the SiteScope SNMP Trap Monitor. Use the following steps to verify that SiteScope is receiving traps.

To verify that SiteScope is receiving SNMP traps:

- 1** Add a SNMP Trap Monitor to SiteScope. In case you already have SNMP Trap Monitor defined, you can skip this step.
- 2** Configure the intended SNMP Trap sending entity to send traps to the SiteScope machine. The steps to configure the SNMP host depends on system. Usually, it involves lowering system thresholds to cause normal situations to create traps. On some systems there is a test mode that you can use to create traps on demand. The other way is to use one of the freely available SNMP trap generators, and to send copies of the trap to SiteScope.
- 3** Inspect the SNMP Trap Monitor log file in SiteScope for sent traps. Every SNMP Trap received by the SiteScope is written into the SNMP Trap Monitor's log file, located in <SiteScope root directory>\logs\snmptrap.log.

Common Problems and Solutions

The following table summarizes common problems and suggested solutions:

Problem Symptom	Possible Cause	Solution
The monitor does not appear in the monitor list.	Option License for Integration Monitors had not been provided.	Provide the Option License for Integration Monitors.
The SNMP traps are not forwarded to HP Business Availability Center applications.	The SNMP Agent does not emit SNMP traps.	Verify that the SNMP Agent is configured to emit SNMP traps. Use the <SiteScope>\logs\snmptrap.log file to verify that traps are received by SiteScope. For details, see “Verify SNMP Trap Reception to SiteScope” on page 1143.
	The EMS configuration file contains errors.	Click the Test Script button in the Advanced Settings to verify the EMS configuration file.
	The SNMP trap port is busy.	Make sure that no other SNMP trap service is listening to SNMP traps on the SiteScope machine. Microsoft SNMP Trap Service is common cause on computers running Windows NT or Windows 2000 OS.
	The monitor is not configured to report to these applications.	Make sure that the monitor is configured to report to these applications.
Samples are created and sent from SiteScope, but the data is not seen in Dashboard/Event Log/SiteScope reports.	Samples were dropped due to missing fields or values.	Check in <HP Business Availability Center root directory>\log\mercury_wde\wdeIgnoredSamples.log.

29

Technology Web Service Integration Monitor

The Technology Web Service Integration Monitor enables a Web service entry point to SiteScope. The monitor can be used to report data from third-party Enterprise Management Systems (EMS) to SiteScope through Web service. Both event and metrics entry points into HP Business Availability Center are published for external systems to use. For each event and/or metric that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the event and/or metrics values.

This chapter includes:

Concepts

- ▶ Technology Web Service Integration Monitor Overview on page 1146
- ▶ Setup Requirements on page 1147

Tasks

- ▶ Check Connectivity to the Technology Web Service Integration Monitor on page 1149

Reference

- ▶ Technology Web Service Integration Monitor Settings on page 1150

Troubleshooting and Limitations on page 1156

Technology Web Service Integration Monitor Overview

Use the Technology Web Service Integration Monitor for integrating event data or metrics data from your existing EMS system to HP Business Availability Center. SiteScope supplies a WSDL file which the user can use to create a client code. The client code reports the event and/or metrics data to SiteScope. The client has several ways to report data to HP Business Availability Center:

- report one event
- report an array of events
- report one metric
- report an array of metrics

What Data Is Collected

The Technology Web Service Integration Monitor collects data that is extracted from any message received by SiteScope report data Web service and sends notifications to HP Business Availability Center containing preferred values from the original message.

Before setting up the Technology Web Service Integration Monitor, you should understand and map out the purpose and usage of the data that is forwarded to HP Business Availability Center. You should determine if the data is for presentation in the Dashboard, Service Level Management, and/or reports.

The specific data that is forwarded to HP Business Availability Center is controlled by the field mapping script. You use this script to specify the preferred value fields that you want forwarded. For more details on selecting the script and the file structure and syntax, see “Integration Monitor Field Mapping” on page 1161.

Limitations

If you are working with HP Business Availability Center version 5.1 and lower, you cannot define new Technology Web Service Integration monitors or edit existing ones from within HP Business Availability Center. If you need to define a new Technology Web Service Integration monitor or edit an existing monitor, detach SiteScope from HP Business Availability Center, define the monitor in SiteScope's new user interface, and then attach the SiteScope to HP Business Availability Center again.

For details on configuring the monitor, see “Technology Web Service Integration Monitor Settings” on page 1150.

Setup Requirements

- When adding the monitor to SiteScope, in the Main Settings area, you must select a field mapping script and load the script for the monitor. Copy the contents of the script into your preferred text editor and edit the script to define the event handlers for the monitor instance. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 1161.
- To enable the connection to SiteScope reportMonitorData Web service, you must create a client code (in any language) that makes the connection and handles the reporting of the data to SiteScope through the Web service.

To enable the connection to SiteScope reportMonitorData Web service:

- 1** Open Explorer and go to SiteScope (<http://<SiteScope host>:8080/SiteScope/services>). Take the WSDL file of the service **reportMonitorData**. The WSDL is an interface file which represents the API of the reportMonitorData Web service in SiteScope. The reportMonitorData service is the service that listens to incoming messages and forwards them to HP Business Availability Center. This file is used to create the client stubs that connect to the service and report the data.
- 2** Generate the stubs using the WSDL file. The generation of the stubs can be to any language. The way to create the files depends on the language that you want to use.

For example, if you want to use Java as the client code, you must use the WSDL2JAVA task in AXIS package that can be downloaded from their Web site. Run **Java org.apache.axis.wsdl.WSDL2Java <name of saved WSDL file>**. After running this, you get two packages. One package is **com**, which holds the needed objects for sending the data, and the second is **localhost**, which holds the stubs that makes the connection to SiteScope Web service.

- 3** Write the actual client code which uses the generated classes to send the data to SiteScope. In the code, call the **setreportMonitorDataEndpointAddress(<SiteScope targetHost>)**, which is found in **MonitorDataAcceptorServiceLocator** (one of the generated stubs) to set the SiteScope address to where you want the data reported.
- 4** Run your code and check if you get data in the SiteScope Technology Web Service Integration monitor.

Check Connectivity to the Technology Web Service Integration Monitor

After creating a Technology Web Service Integration monitor in SiteScope, you can check connectivity to the Web service by using the **test_client** which is located in the <SiteScope root directory>\conf\ems\webservice\test_client directory. This tool sends constant messages to SiteScope reportMonitorData Web service. The messages can be either metrics messages or event messages.

To use the client tool to check connectivity:

- 1** In the <SiteScope root directory>\conf\ems\webservice\test_client directory, run the **test_event_client.bat** for events or **test_metrics_client.bat** for metrics, using the following parameters:
 - ▶ **Target Host.** The address of the SiteScope host which receives the messages.
 - ▶ **Number of messages to send.** Number of messages to send to SiteScope.
 - ▶ **System Id.** System Id of the monitor that receives the messages.
 - ▶ **Severity/Quality.** Severity of the event when forwarding events (default is to send 1 to 5). Quality of the metric when forwarding metrics data (default is 0-3).
- 2** If you are forwarding other values to HP Business Availability Center, you must edit the configuration file accordingly.

The tool can also be run with no parameters. In this case, the tool tries to send one message to the local host. The message has the system id: **Test Event System Id**. The severity is 5 (for events) or the quality is 3 (for metrics).

If you use this option, you must activate it on the SiteScope machine and have a Technology SNMP Trap Integration monitor with the system id: **Test Event System Id**.

- 3** After running the tool, go to the required SiteScope monitor and see if the number of messages received equals the number that you sent. In addition, you can go to one of the applications (Dashboard, System Availability Management) and see if the data that you sent is displayed.

Technology Web Service Integration Monitor Settings

<p>Description</p>	<p>The Technology Web Service Integration Monitor enables a Web service entry point to SiteScope. The monitor can be used to report data from third-party Enterprise Management Systems (EMS) to SiteScope through Web service. Both event and metrics entry points into HP Business Availability Center are published for external systems to use. For each event and/or metric that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the event and/or metrics values.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ In the monitor tree, right-click a group and select Add Monitor. ▶ In the Contents tab for the group, click Add Monitor.
<p>Important Information</p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p>Useful Links</p>	<p>"Technology Web Service Integration Monitor" on page 1145</p>

The Add/Edit Technology Web Service Integration Monitor page includes the following areas:

Main Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
System ID	<p>Type a text system id for the Technology Web Service Integration Monitor instance.</p> <p>Each received message from the EMS system holds a system id. Each monitor receives messages only with a system id that matches the system id defined in the monitor. The system id is unique for all monitors. Type the system id that represents the messages that you want this monitor to receive.</p>
Sample Type	<p>Select from the following sample types for this integration:</p> <ul style="list-style-type: none"> ▶ Events. For details, see “Configuring Field Mapping for Event Samples” on page 1164. ▶ Measurements. For details, see “Configuring Field Mapping for Measurement Samples” on page 1170. ▶ Tickets. For details, see “Configuring Field Mapping for Ticket Samples” on page 1173.
Load File	<p>Click to load the script that is applicable to the sample type selected above.</p>

GUI Element	Description
<p>Field Mapping</p>	<p>The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring.</p> <p>The mapping itself is not editable in the UI. You must copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1161.</p>
<p>Test Script</p>	<p>Click to test the field mapping script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Advanced Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Frequency	<p>Select how often the monitor should update its status. The Frequency setting for the monitor controls only the status reports. The Web transaction is forwarded when it is received without any delay.</p> <p>Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days.</p> <p>Default value: 10 minutes</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ The interval must be a minimum of 15 seconds or longer. ➤ It is possible to define a monitor with zero frequency. However this monitor runs only if activated manually or according to the frequency of the composite or e-business transaction monitor including it.

Topology Settings (Monitor Specific)

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Topology template	<p>Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propagates its status to the CIs mapped in this topology.</p> <p>Select from:</p> <ul style="list-style-type: none"> ▶ Custom. You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or EMS monitor CIs. ▶ Hosts. Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the topology. ▶ Hosts-Applications. Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI as leaf nodes of the application CI. The host CI also has an EMS monitor CI as a leaf node. <p>Note: It is recommended not to select Custom as this does not load a script and you must enter the entire script yourself. It is recommended to begin with either Host or Host and Application and edit one of those scripts.</p> <p>For more details, see “Topology Settings” on page 1049.</p>
Load Script	<p>Click to load the required Jython script for the topology you selected in the Topology template option. If you selected Custom, there is no script to load.</p>

GUI Element	Description
Script	<p>The contents of the script are visible in this box. However, it is highly recommended not to edit the contents of the script here. You must copy the contents of the script into your preferred text edit, edit the script as needed, and then copy the contents back into this box.</p> <p>Note: The Jython script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see “Topology Settings” on page 1049.</p>
Test Script	<p>Click to test the topology script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is mapped. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: <SiteScope root directory>\logs\bac_integration.log.</p> <p>Note: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Troubleshooting and Limitations

- ▶ Check for errors in `<SiteScope root directory>\logs\RunMonitor.log` and in `<SiteScope root directory>\logs\error.log`.
- ▶ Change the log level to DEBUG in `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties`, to watch outgoing samples.

Change the line:

```
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
```

to:

```
log4j.category.EmsEventPrinter= DEBUG, ems.appender.
```

The log file to look at is:

```
<SiteScope root directory>\logs\RunMonitor.log
```

- ▶ If samples are created and sent from SiteScope, but the data is not seen in **Dashboard/Event Log/SiteScope reports**, look in `<HP Business Availability Center root directory>\log\mercury_wde\wdeIgnoredSamples.log` to make sure the samples were not dropped due to missing fields or values.
- ▶ Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine:
`<HP Business Availability Center root directory>\conf\core\tools\log4j\mercury_wde\wde.properties`

Change the log level parameter to DEBUG in the following lines:

- ▶ `log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender`
- ▶ `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender`

Look at the corresponding log files:

- ▶ `<HP Business Availability Center root directory>\logs\mercury_wde\wdeIgnoredSamples.log`
- ▶ `<HP Business Availability Center root directory>\logs\mercury_wde\wdePublishedSamples.log`

30

Integration with HP Network Node Manager

HP Business Availability Center can accept events from Hewlett-Packard Network Node Manager (NNM).

This chapter includes:

Concepts

- ▶ Network Node Manager Integration Overview on page 1157
- ▶ Writing Scripts to Export Network Node Manager Data on page 1158

Tasks

- ▶ Configure Events in Network Node Manager on page 1159

Network Node Manager Integration Overview

You can forward from Network Node Manager (NNM) event data by configuring NNM to run a script for each event that you want forwarded to HP Business Availability Center. The script that you write and associate with NNM can do one of the following actions:

- ▶ write the NNM data to a log file
- ▶ send an SNMP trap with the NNM data to a SiteScope server

If your script writes the data to a log you then use a Technology Log File Integration Monitor to read the data and forward it to HP Business Availability Center. If you use a script to send an SNMP trap to a SiteScope server, you use an Technology SNMP Trap Integration Monitor configured to receive it and forward to HP Business Availability Center.

Writing Scripts to Export Network Node Manager Data

The script you use should accept data from Network Node Manager as a command line argument, and process the data so that it can be forwarded to HP Business Availability Center. The following sections describe example scripts that can be used to export NNM data.

Sample Script for Writing to a Log File

The following Perl script receives data from the command line and writes it to a log file as a comma separated vector of values that can be parsed by the Log File Integration Monitor:

```
#!/usr/bin/perl
open LOG, ">>log1.log" or die;
print LOG (join ',', @ARGV) . "\n";
close LOG;
```

Sample Script for Sending SNMP Trap Data

The following Perl script receives data from the command line and sends it as a message in an SNMP trap (using SNMP data generated by Network Node Manager) that can be caught by a Technology SNMP Trap Integration Monitor. It accepts the host name to which the trap is sent as the first parameter and a string description of the alert as the second parameter.

```
#!/usr/bin/perl
$host = $ARGV[0];
$message = $ARGV[1];
system("snmptrap $host \"\" \"\" 6 0 5 system.sysDescr.0 \" . \"octetstringasci
$message");
```

Configure Events in Network Node Manager

Use the following steps to configure Network Node Manager to run a script for the requested events in Network Node Manager. The figure below shows examples of the applicable Network Node Manager pages and dialogs you use.

To configure Network Node Manager to run scripts:

- 1** From the **Options** menu choose **Event Configuration**.
- 2** Select the requested enterprise and event from the **Event Configuration** dialog.
- 3** Select the Actions tab from the Edit > Events > Modify Events dialog.
- 4** Type the command line for the script in the **Command for Automatic Action** text box. You may use NNM variables to pass data to the command line.
- 5** Click **OK** to close the **Modify Events** dialog.
- 6** From the **File** menu in the **Event Configuration** dialog select **Save**.

31

Integration Monitor Field Mapping

You enable capturing event and metrics data from Enterprise Management Systems, automated support systems, and other management applications by configuring integration monitors and their field mapping scripts.

This chapter includes:

Concepts

- ▶ Integration Monitor Field Mapping Overview on page 1162
- ▶ Understanding Field Mapping Structure on page 1163

Reference

- ▶ Configuring Field Mapping for Event Samples on page 1164
- ▶ Configuring Field Mapping for Measurement Samples on page 1170
- ▶ Configuring Field Mapping for Ticket Samples on page 1173
- ▶ Event Handler Structure on page 1177

Integration Monitor Field Mapping Overview

Integration monitors depend on field mappings you customize within the user interface in the settings for the monitor. The mapping defines the processing of incoming data and defines the output sample forwarded to Business Availability Center.

Integration Monitors designed for use with specific EMS applications (these currently include HP OVO, HP Service Center, and NetScout) can be configured without editing their field mapping script. The mappings are predefined by HP and require modification only if specific customizations are required. For details on editing these field mapping scripts, see the description for the field mapping element in the user interface pages for the monitor you are deploying.

For Technology Integration Monitors (Technology SNMP Trap, Technology Log File, and Technology Database monitors), you must select the sample type and the required script template is loaded directly into the field mapping text box. You must edit the field mapping script to suite your organization's needs. The Technology Web Service Integration Monitor field mapping may also need to be customized. You can select from the following sample types:

- ▶ **Events.** Select to forward event data to Business Availability Center.
When you select **Events** and you want to integrate to Business Availability Center using topology settings, it is recommended that you select from the following topology script templates: **Hosts** or **Hosts-Applications**.
- ▶ **Measurements.** Select to forward measurement data to Business Availability Center.
When you select **Measurements**, you can not use topology settings to integrate with Business Availability Center.
- ▶ **Tickets.** Select to forward ticket data to Business Availability Center.
When you select **Tickets** and you want to integrate to Business Availability Center using topology settings, it is recommended that you select the following topology script template: **Tickets**.
For details, on selecting a topology setting, see “Topology Settings” on page 1049.

Note: Use only the mandatory and optional fields defined in the script templates when working with the field mapping. For more information, see the tables for each sample type.

Understanding Field Mapping Structure

The field mapping contains instructions on how to process the data as it arrives to the integration monitors. The instructions that constitute the field mappings are grouped into event handlers—independent sections that contain instructions relevant to specific data. Each event handler contains a **matching condition** by which SiteScope can determine whether to use a particular event handler for an arriving event.

When an event or measurement data arrives at the integration monitor, it iterates over the different event handlers in the field mapping, in the order they appear, testing the **matching condition** of each handler. If a matching handler is found, the monitor uses the instructions within that handler to process the event and perform the action defined for this handler (for example, forward it to Business Availability Center or discard). No further sections are checked after the first match. If no matches are found, the event is discarded.

In addition to the event handlers, the field mapping can contain special entries that affect the integration monitor engine as a whole. These values are grouped into the `[$DEFAULT_PARAMETERS$]` section. This section defines default values for tags that are common for all handlers. Any tag can be set in this section of the field mapping. It is used to create a reported value unless overridden in the matched event handler. For each incoming event, this event handler is always run prior to the matched event handler.

For details on event handler structure, see “Event Handler Structure” on page 1177.

Configuring Field Mapping for Event Samples

The events sample type is used for extracting events collected by external systems and importing them to Business Availability Center. When configuring an integration monitor's field mapping, select the **Events** sample type to load the events script. You can then copy the contents of the **Field Mapping** text box and paste it into a text editor to make your configuration changes. When you are done, copy the contents back into the Field Mapping text box.

This section includes the following topics:

- “Mandatory Values for the Event Script” on page 1165
- “Optional Values for the Event Script” on page 1166
- “Conditional Expression Example 1” on page 1168
- “Conditional Expression Example 2” on page 1168
- “Event Script Example” on page 1169

Mandatory Values for the Event Script

The tables below list mandatory and optional values for the event script.

Field Name	Type	Description	Example
time_stamp	DOUBLE	Time stamp in seconds since Jan 1 1970	time_stamp:DOUBLE=str_to_seconds(\$time,"yyyy-MM-dd HH:mm:ss.SSS"). time_stamp:DOUBLE=time()
severity	INT	Can be one of the following preconfigured severities (based on applicable integer): 0:SEVERITY_UNKNOWN 1:SEVERITY_INFORMATIONAL 2:SEVERITY_WARNING 3:SEVERITY_MINOR 4:SEVERITY_MAJOR 5:SEVERITY_CRITICAL	severity:INT=SEVERITY_MINOR
target_name	STRING	Name of device or host that generated the event	target_name=\$hostName target_name=resolveHostName (String hostname)
status	STRING	Status of event in external EMS terminology	status="OPEN" status="ASSIGNED" status="CLOSED"
subject	STRING	Subject of event (e.g. CPU, SAP application, Hard Disk), middle/high level hierarchy describing the event source.	subject="DISK"

Field Name	Type	Description	Example
instance	STRING	Instance of subject that generated the event (e.g D:\). Lowest level of hierarchy describing the event source	instance="E:\\"
description	STRING	Textual description of event	description="free space on drive e is below 10%"
data_source	STRING	System that generated the event	data_source="HP OVO"

Optional Values for the Event Script

The tables below list optional values for the event script.

Field Name	Type	Description	Example
target_ip	STRING	IP of host or device that generated the event	target_ip=\$IPString
object	STRING	Optional level in the hierarchy describing the event source	object="OS"
event_id	STRING	Unique identifier of this event	event_id=\$id
logical_group	STRING	Logical grouping of this event	logical_group="error messages"
monitor_group	STRING	Monitor group that reported this event	monitor_group="log monitors on \\hostname"
orig_severity_name	STRING	Severity in external EMS terminology	orig_severity_name="Cleared"
acknowledged_by	STRING	Name of user that acknowledged this event	acknowledged_by=\$username
owner	STRING	Name of user who owns this event	owner="admin"

Field Name	Type	Description	Example
value	DOUBLE	Use to transfer numerical values from the event	value=\$thresholdViolated
attr1	STRING	Extra data slot	attr1=\$history
attr2	STRING	Extra data slot	attr2=\$moreHistory
attr3	STRING	Extra data slot	attr3="Design"
attr4	STRING	Extra data slot	attr4=\$MonitorOutput
attr5	STRING	Extra data slot for long strings	attr5=\$Longhistory

Host DNS Resolution for Event Sample

Both the FQDN (fully qualified domain name) and valid IP address are necessary for the fields that are used to create host CIs in HP Business Availability Center integration.

If you do not know the FQDN and/or IP address, then you can use the following functions in the field mapping to resolve the names and access them from the source of the integration:

target_name=resolveHostName(\$SomeHost)

target_ip=resolveHostIP(\$SomeHost)

Note: The variable **\$SomeHost** must be replaced by a variable from the integration source.

These functions are not necessary if:

- ▶ The FQDN and/or IP address is available from the source that the integration is accessing. In this case, you should input the value for **target_name=** as a FQDN and the value for the **target_ip=** without the function.
- ▶ It is not possible for the SiteScope server to resolve the FQDN and/or IP address for the servers from the source that the integration is accessing. In this case, the functions may not provide the valid values.

Conditional Expression Example 1

```
severity:INT=$var6.equals("red") ? SEVERITY_CRITICAL  
: SEVERITY_INFORMATIONAL
```

In this example, the value of sixth variable binding is compared to string red. If the variable binding is indeed equal to string red, then the value of the severity tag is set to SEVERITY_CRITICAL, otherwise it is set to SEVERITY_INFORMATIONAL.

Conditional Expression Example 2

```
severity:INT=$var6.equals("red") ? SEVERITY_CRITICAL :  
$var6.equals("green") ? SEVERITY_INFORMATIONAL : $var6.equals("yellow")  
? SEVERITY_MINOR : SEVERITY_WARNING
```

This example chains the conditional operator into a decision chain. If the sixth variable binding holds string red, then severity tag has the value SEVERITY_CRITICAL. If the sixth variable binding holds string green, then severity tag has the value SEVERITY_INFORMATIONAL. If the variable binding holds string yellow, the tag has the value SEVERITY_MINOR. If none of the above conditions are true, then the tag has the value SEVERITY_WARNING.

Event Script Example

In the example below, two types of events are sent: the first are events of status "OPEN" and the second are events cleared by a user. The data is retrieved from incoming event fields using the \$ notation. All other events are discarded by the last handler.

```
[DEFAULT_PARAMETERS$]
#####
# NOTE: the following parameters are mandatory #
#####
time_stamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS")
severity:INT= SEVERITY_UNKNOWN
target_name=$Device
status=$Status
subject="EMS X Events"
instance=$target
description=$description
data_source="EMS X"

#send an open event with the value in value fields and with the event id
[OPEN events]
$MATCH="OPEN".equals($Status)
$ACTION=TOPAZ_BUS_POST(event)
value:DOUBLE=parseDouble($threshold)
event_id=$uid

#send clear events with the event id and acknowledging username
[clear events]
$MATCH="CLEAR".equals($Status)
$ACTION=TOPAZ_BUS_POST(event)
event_id=$uid
acknowledged_by=$ClearedBy

[event sink]
$MATCH=true
$ACTION=DISCARD
```

Configuring Field Mapping for Measurement Samples

The measurements sample type is used for extracting metrics collected by external systems and importing them to Business Availability Center. When configuring an integration monitor's field mapping, select the **Measurements** sample type to load the measurements script. You can then copy the contents of the **Field Mapping** text box and paste it into a text editor to make your configuration changes. When you are done, copy the contents back into the Field Mapping text box.

Note: If you select the measurement field mapping, you should not use the topology settings for the integration. The topology settings are not supported for the measurement script template type.

This section includes the following topics:

- ▶ “Mandatory Values for the Measurements Script” on page 1171
- ▶ “Measurements Script Example” on page 1171

Mandatory Values for the Measurements Script

The table below lists mandatory values for the measurements script.

Field Name	Type	Description	Example
TimeStamp	DOUBLE	Time stamp in the seconds since Jan 1st 1970 format	TimeStamp:DOUBLE=time ()
Quality	INT	Quality in SiteScope terms. Possible values are:QUALITY_ERROR, QUALITY_WARNING, QUALITY_GOOD	Quality:INT=QUALITY_ERROR
MonitorName	STRING	Logical monitor name	MonitorName="NT cpu Monitor"
MonitorState	STRING	The monitor status, for example, N\A, Good, Error, and so on.	MonitorState="Received " + \$count + " events"
MonitorType	STRING	The monitor type	MonitorType="System Monitor"
TargetName	STRING	The target of this monitor (e.g. host name)	TargetName=\$Device
Measurement Name(N)	STRING	Name the Nth measurement	MeasurementName(1)="C PU Temperature"
Value(N)	DOUBLE	Value of Nth measurement	Value(1):DOUBLE=\$CPU Temperature

Measurements Script Example

In the example below, two measurements are sent: the first one (MeasurementName (1)) takes its name from the \$legend field and takes the value from the \$value field. A second measurement (Measurement Name (2)) uses the constant name CPU Temperature which receives its value from the \$CPUTemp field.

```
#####
#      EMS Integration metricsconfig file #
# use this file to send metrics to HP Business Availability Center #
#####
[$DEFAULT_PARAMETERS$]
# time stamp in the seconds since Jan 1st 1970 format.
TimeStamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS")

# quality in SiteScope terms QUALITY_ERROR, QUALITY_WARNING,
QUALITY_GOOD
Quality:INT=QUALITY_ERROR

# Logical monitor name
MonitorName=$kpName

#target, e.g. host name
TargetName=$parentMachineName

#the status string of the monitor (e.g.: "Log file read, 3 matches found")
MonitorState="The monitor status is: "+ $status

#the monitor type (e.g. "Log Monitor", "CPU Monitor")
MonitorType="NetIQ measurements"

#measurement name
MeasurementName(1)=$legend
#value as double
Value(1):DOUBLE=parseDouble($value)

#measurement name
MeasurementName(2)="CPU Temperature"
#value as double
Value(2):DOUBLE=parseDouble($CPUTemp)
#####
# To send more than one measurement per DB row #
# add pairs #
# MeasurementName (*) = #
# Value (*) :DOUBLE= #
# where * = 1,2,..,n #
#####
[allR]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(ss_t)
```

When specifying more than one measurement in the script, a separate sample is sent with each of the measurements.

Note: When specifying multiple measurements per file, the measurement numbering must be consecutive.

In the case of failure, errors appear in the **RunMonitor.log** but the error does not affect the monitor status.

Configuring Field Mapping for Ticket Samples

The ticket sample type is used for extracting events collected by external systems and importing them to Business Availability Center. When configuring an integration monitor's field mapping, select the **Tickets** sample type to load the tickets script. You can then copy the contents of the **Field Mapping** text box and paste it into a text editor to make your configuration changes. When you are done, copy the contents back into the Field Mapping text box.

This section includes the following topics:

- “Mandatory Values for the Ticket Script” on page 1174
- “Optional Values for the Ticket Script” on page 1175
- “Conditional Expression Example” on page 1176
- “Ticket Script Example” on page 1176

Mandatory Values for the Ticket Script

The tables below list mandatory and optional values for the ticket script.

Field Name	Type	Description	Example
time_stamp	DOUBLE	Time stamp in seconds since Jan 1 1970	time_stamp:DOUBLE=str_to_seconds(\$time,"yyyy-MM-dd HH:mm:ss.SSS").
severity	INT	Can be one of the following preconfigured severities (based on applicable integer): SEVERITY_UNKNOWN SEVERITY_INFORMATIONAL SEVERITY_WARNING SEVERITY_MINOR SEVERITY_MAJOR SEVERITY_CRITICAL	4".equals(\$severity) ? "Low" : ("3".equals(\$severity) ? "Average" : ("2".equals(\$severity) ? "High" : ("1".equals(\$severity) ? "Critical" : "Unknown")))
target_name	STRING	Name of the entity (usually a service) that generated the ticket.	target_name="mail service" (Do not enter static string here, should be retrieved dynamically from the ticket.)
data_source	STRING	System that generated the ticket	data_source="ticketing" (This string should not be edited for HP ServiceCenter integration and must be edited for a generic technology integration monitor.)
ticket_id	STRING	ID of the ticket	ticket_id=112233
ticket_state	STRING	One of the states in the incident lifecycle as defined in the ticketing system.	"Open" / "Closed"

Field Name	Type	Description	Example
ticket_type	STRING	Type of the incident as defined in the ticketing system.	"Incident"
orig_severity_name	STRING	Severity in external EMS terminology	orig_severity_name="Cleared"

Optional Values for the Ticket Script

The script includes comments describing the optional values available for the ticket script. They include those listed here:

Field Name	Type	Description	Example
subject	STRING	Middle/High level hierarchy describing the event source.	CPU, SAP application, hard disk
instance	STRING	Instance of subject that generated the event. The lowest level hierarchy describing the event source.	D:\
object	STRING	Optional level in the hierarchy describing the ticket source	object="OS"
logical_group	STRING	Logical grouping of this ticket	logical_group="error messages"
monitor_group	STRING	Monitor group that reported this ticket	monitor_group="log monitors on \\hostname"
elapsed_time	STRING	Elapsed time of the ticket.	
orig_severity_name	STRING	Severity name as defined in the ticketing system.	
attr1	STRING	Extra data slot	attr1=\$history

Field Name	Type	Description	Example
attr2	STRING	Extra data slot	attr2=\$moreHistory
attr3	STRING	Extra data slot	attr3="Design"
attr4	STRING	Extra data slot	attr4=\$MonitorOutput
attr5	STRING	Extra data slot for long strings. Use for values up to 2000 chars.	attr5=\$Longhistory

Conditional Expression Example

```
4".equals($severity) ? "Low" : ("3".equals($severity) ? "Average" :
("2".equals($severity) ? "High" : ("1".equals($severity) ? "Critical" : "Unknown"))))
```

This example configures the severity of the ticket sample. It matches between the status terms used in the ticketing system to those used in Business Availability Center.

Ticket Script Example

```
[$DEFAULT_PARAMETERS$]
time_stamp:DOUBLE=$time_stamp
ticket_id=$ticket_id
ticket_state=$ticketStatus
severity:INT=$severity
target_name=$target_name
data_source="ticketing"
ticket_type="Incident"
orig_severity_name="4".equals($severity) ? "Low" : ("3".equals($severity) ? "Average" :
("2".equals($severity) ? "High" : ("1".equals($severity) ? "Critical" : "Unknown"))))
```


Event Handler Structure

Each event handler has following structure:

```
[name]
Matching condition
Action directive
Tags
```

The names of **Matching condition**, **Action directive**, and additional directives start with dollar sign symbol (\$). The names of tags should not start with dollar sign.

Comments are allowed in the field mapping. The comment starts with either #, !, or ; character and continues to the end of the line.

Note: Use only the mandatory and optional fields defined in the script templates when working with the field mapping. See the tables in the following sections for more information.

This section includes the following topics:

- “Matching Condition” on page 1178
- “Basic String Expressions” on page 1182
- “Basic Conditional Expression” on page 1182
- “Action Directive” on page 1182
- “Tags” on page 1183
- “Integration Monitor Field Mapping Examples” on page 1184

Matching Condition

The Match Condition must be a valid boolean expression. The expression can contain calls to the operators and functions defined below. The expression can access the contents of the event that is being processed using the dollar sign (\$) notation. For example, if the incoming event is SNMP Trap, then its enterprise OID can be accessed as \$oid. For names specific to a monitor, refer to the documentation of the relevant monitor type.

Note: The Match Condition expression is limited to 4,000 characters.

The matching condition has the form:

```
$MATCH=Boolean expression
```

where the Boolean expression is one of the expressions listed in the table below. When mentioned in the description, the expression can also be used to assign values into tags (see “Tags” on page 1183).

Expressions and Functions	Description	Examples	True if
<, <=, >, >=, ==, !=	Checks the numerical correctness of the expression. Can be used with INT or DOUBLE fields.	\$MATCH=\$numberOfLines == 100	\$numberOfLines equals 100
		\$MATCH=\$numberOfColumns <= 107	\$numberOfColumns equals 107 or less
equals(String)	Checks for string equality.	\$MATCH="ERROR".equals(\$status)	\$status equals the word ERROR
		\$MATCH=\$status.equals("ERROR")	\$status equals the word ERROR

Expressions and Functions	Description	Examples	True if
true, false	Constant Boolean values.	\$MATCH= true	always true.
&&,	To be used to combine any of the above boolean expressions.	\$MATCH= \$status.equals ("ERROR") \$numberOfLines == 100	\$status equals the word ERROR or if \$numberOfLines equals 100
time()	Returns the current time, in seconds, since January 1, 1970 format. Can be used with DOUBLE fields.	\$MATCH= \$timeStampField > (time()-600)	the value of the \$timeStampField is newer than ten minutes ago (in seconds, since January 1, 1970 format)
parseInt (String), parseDouble(String),	Use to convert strings to numeric values. The input string should be a valid representation of an integer or a floating point number. Note: calling this function on a string that cannot be interpreted as a number causes an error and the incoming event is dropped. Can also be used with INT or DOUBLE fields.	\$MATCH= parseInt(\$size) > 10	the string value in \$size is an integer larger than 10.

Expressions and Functions	Description	Examples	True if
str_to_seconds(Str1, Str2)	Calculates the timestamp (in seconds, since January 1, 1970 format) held in the first String using the format in the second string. Can also be used with DOUBLE fields.	<p>\$MATCH= str_to_seconds (\$time,"yyyy-MM-dd HH:mm:ss.SSS") > time()</p> <p>Note: use the following symbols to represent time: Year - 'y' Month - 'M' Day of month - 'd' Hour - 'H' Minute - 'm' Second - 's'</p>	<p>the date specified in \$time in yyyy-MM-dd HH:mm:ss.SSS format is later than the current time.</p> <p>For more information, search the Internet for SimpleDateFormat.</p>
exist(\$field)	Checks for an existence of a field in the processed event and makes sure that it is not an empty value.	\$MATCH= exist(\$status)	\$status exists in the incoming event and is not an empty string.
isInt(String), isDouble (String)	Checks if the input string can be interpreted as an integer or a double number, respectively.	\$MATCH=isDouble(\$size)	the string value in \$size can be converted to a double.

Expressions and Functions	Description	Examples	True if
resolveHostIP (String hostname)	Performs DNS resolution from a server to its IP address. If the DNS resolution fails, the function returns the value unknown host.	target_ip= resolveHostIP (\$host)	
resolveHostName (String hostname)	Performs DNS resolution from an IP address to a fully qualified domain name. If the DNS resolution fails, the function returns the originally input host name.	target_name= resolveHostName (\$host)	

Any of the above expressions can be used and the expression can refer to incoming event fields. The value of the expression, which can be either **true** or **false**, determines whether the event handler is be used to process the event or not.

Basic String Expressions

The following table summarizes the string expressions that can be used in the field mapping:

Operation	Description	Examples
+	String concatenation	"trap type is " + \$trap
substring	Substring of given string	\$var4.substring(3,5)
indexOf	Return indexOf string in another string	\$var4.indexOf(\$var3)

Basic Conditional Expression

One conditional expression is supported; the **?** operator. This operator can be used to compose three expressions into one (for example, <Conditional part> ? <if true part> : <if false part>).

Action Directive

The action directive has the form:

\$ACTION= TOPAZ_BUS_POST or DISCARD

The value of the Action directive defines whether the event is processed and forwarded to Business Availability Center, or discarded. This value takes effect only if the matching condition within the handler had been evaluated to positive value (that is, to **true**). The table below describes the effect of the different actions.

Action	Description	For Use With
TOPAZ_BUS_POST (event)	Send the event to the Business Availability Center bus and database.	HP Business Availability Center
TOPAZ_BUS_POST (ss_t)	Send the metrics to HP Universal CMDB as SiteScope Data.	HP Business Availability Center
DISCARD	Do not send the data to HP Business Availability Center.	events you wish to filter out

Note: If you are using the metrics mapping, TOPAZ_BUS_POST(ss_t), the data is sent to the HP Business Availability Center database as SiteScope data, and thus saved to the database. For details on metrics mapping, see “Configuring Field Mapping for Measurement Samples” on page 1170.

Tags

In addition to directives, the event handler contains **tags**. Each tag represents a field in the event that is forwarded to Business Availability Center. The tag’s value can be evaluated when the event arrives to the integration monitor.

The general format of a tag is `name[:type]=value`.

The `<name>` is any string without spaces or dollar signs (`$`). The `<type>` specifies the type of field as reported to Business Availability Center. It can be either **INT**, **DOUBLE** or **STRING**. The default type is **STRING**.

By defining a tag, you can customize event forwarding to Business Availability Center. Thus getting more value from the external applications that create those events. For example, if the monitor pulls out data from a database table column called `AlertText`, which contains a textual description of an alert, it is possible to send that data to Business Availability Center by adding the following line to an event handler section:

```
[event handler]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
text=$AlertText
```

Note: When adding tags, always add them after the **\$MATCH** and **\$ACTION**.

Integration Monitor Field Mapping Examples

Example 1: Universal Event Handler

```
[post them all]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL
szAlarmText:STRING="post them all handler received an event"
```

Note that the **\$MATCH** directive in the handler is set to **true**. This causes every event to match the handler and therefore every event is sent to the Business Availability Center bus.

Example 2: Different Event Handlers for Different Severities

```
[Error Handler]
$MATCH= $status.equals("ERROR")
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_CRITICAL

[Info Handler]
$MATCH= $status.equals("INFO")
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL

[post them all]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL
```

In this example, an incoming event is matched against the **Error Handler** event handler. If the handler's condition is true (that is, the value in the status field equals **ERROR**), then an event with a field called severity, whose value is **SEVERITY_CRITICAL**, is sent to HP Business Availability Center. An event can be matched only by a single handler. The first match stops the processing and therefore once an event is matched by a section, it is not processed by the next handler.

If the event was not matched by the first handler, the second handler comes into action and its match (which looks for status of **INFO**) is used to decide whether the second handler needs to take action. Finally, if the event does not match the second handler, the third universal handler is evaluated.

Part VII

Templates

32

SiteScope Templates

This chapter includes the main concepts, tasks, and reference information for SiteScope templates.

This chapter includes:

Concepts

- SiteScope Templates Overview on page 1190
- Understanding Templates on page 1192
- Template Examples on page 1194
- Planning Templates on page 1195
- Working with Template Variables on page 1197
- Counter Selection in Monitor Templates on page 1202
- Updating Template Deployments on page 1206

Tasks

- Configure a SiteScope Monitoring Solution Using a Template – Workflow on page 1208
- Publish Template Updates to Related Group Deployments on page 1218
- Modify Counter Selection Strings to Use Regular Expressions on page 1221
- Export and Import a Template on page 1222

Reference

- Reserved Template Group Types on page 1223
- SiteScope Templates User Interface on page 1223

SiteScope Templates Overview

Templates in SiteScope are used to standardize a set of monitor types and configurations into a single structure. This structure can then be repeatedly deployed as a group of monitors targeting multiple elements of the monitored environments.

Templates provide an enterprise solution for standardizing the monitoring of the different IT elements in your enterprise, including servers, applications, databases, network environments, and so forth. Templates speed the deployment of monitors across the enterprise through the single-operation deployment of groups, monitors, alerts, remote servers, and configuration settings.

Templates also provide the ability to view how the actual monitored deployments comply with the standardized deployment as defined in the template. This ensures that any changes in the monitored environment can be quickly updated in the monitoring infrastructure and that the monitoring infrastructure is still compliant with the standards set in the template.

SiteScope provides two types of templates: user-defined templates and solution templates. This chapter discusses user-defined templates. For information on Solution Templates, see “SiteScope Solution Templates” on page 1273.

Template Elements and Features

You create templates within a template container in the monitor tree. These elements are then displayed in the monitor tree where you can access them for changes or deployment. For more information, see “Understanding Templates” on page 1192.

You use templates to deploy a standardized pattern of monitoring to multiple elements in your infrastructure. Effective development and use of templates requires some planning because you can add multiple objects types to the template. For more information, see “Planning Templates” on page 1195.

You create a template by adding and configuring groups, remote server definitions, monitors, alerts, and variables to the template. You use template variables as substitution markers for configuration settings that you want to change dynamically or interactively each time you deploy the template. Creating and referencing variables is an action that is unique to templates. Template variables use a special syntax. For more information, see “Working with Template Variables” on page 1197.

Several SiteScope monitor types use a measurement counter browser function to dynamically query applications and systems for the metrics that are available for monitoring. When you create one of these monitors manually, you use a multiple step procedure to view and select counters. An alternative method is used to select counters when deploying templates. For details, see “Modify Counter Selection Strings to Use Regular Expressions” on page 1221.

After you create and configure templates, you deploy them in the SiteScope hierarchy. If you subsequently want to make changes to the source template, you can automatically publish the changes to SiteScope objects deployed by the template using the Publish Template Changes Wizard. For more information, see “Updating Template Deployments” on page 1206.

Note: For information on configuring internal properties in SiteScope templates, refer to the HP Software Self-solve knowledge base (h20230.www2.hp.com/selfsolve/documents). To enter the knowledge base, you must log in with your HP Passport ID.

Understanding Templates

Templates are objects you use to reproduce groups, servers, monitors, and alerts according to a predefined pattern and configuration. You can deploy all of the items defined in the template in a single operation by copying the template to a location in the SiteScope hierarchy. Templates also use template variables that you use to interactively set certain monitor, server, and alert configuration settings when you deploy the template. Once you have created a template, you can use it to deploy monitors as often as needed.

There are two methods for adding configurations to the created template.

- ▶ You can copy an existing group and monitor hierarchy from a SiteScope to the template and edit the elements for use as a template. For details, see “Create a Template by Copying Existing Configurations” on page 1214.
- ▶ Alternatively, if there are no applicable SiteScope monitor elements in your enterprise or if you want to create new objects or settings, you can manually create template groups, monitors, servers, and alerts in the template. For details, see “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208.








Tip:

- ▶ If SiteScope monitoring has not yet been configured and you are not familiar working with SiteScope monitors and groups, it is recommended that you set up some sample groups, monitors, and alerts before you create templates. This helps familiarize you with the monitor configurations and the relationship between monitors, groups, and alerts. Afterwards, you can copy the structure from the SiteScope and convert the configurations to a template.
 - ▶ To help you get started with templates, SiteScope provides example templates for monitoring in Windows and UNIX HP environments. For details, see “Template Examples” on page 1194.
-

Template Objects

Templates are created and stored in a template container in the monitor tree. The template variable definitions and SiteScope objects configurable using the template are displayed as objects within the template.

The following table describes the objects used in templates:

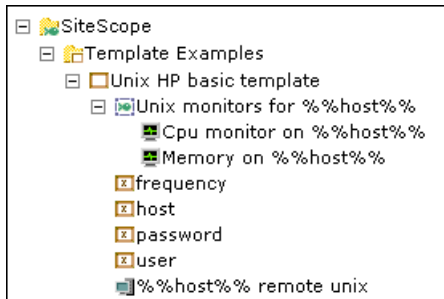
Icon	Object Type	Description
	Template Container	Enables you to manage your template monitoring solutions. You can only add a template to a template container. For details on configuring this object, see “New Template Container Page” on page 1224.
	Template	The template contains the SiteScope group, monitors, remote servers, variable definitions, and alerts that make up the template monitoring solution. For details on configuring this object, see “New Template Page” on page 1225.
	Template Variable	A variable is used to prompt for user input during template deployment. Template variables are either user-defined or predefined system variables. For details on configuring this object, see “New Template Variable Page” on page 1227.
	Template Remote Server	A template remote server is used to define Windows or UNIX remote server preferences that are created when the template is deployed. For details on configuring this object, see “New Template Remote Server Page” on page 1229.
	Template Group	A template group contains the template monitors and associated alerts. You use template groups to manage the deployment of monitors and associated alerts in your infrastructure. For details on configuring this object, see “New Template Group Page” on page 1226.
	Template Monitor	Template monitors are used to define monitors that are created when the template is deployed. For details on configuring this object, see “New Template Monitor Page” on page 1236.
	Template Alert	Template alerts are used to define alerts on groups and monitors that are created when the template is deployed. For details on configuring this object, see “New Template Alert Page” on page 1237.

Template Examples

SiteScope provides template examples for monitoring in Windows and UNIX environments. These templates are available from the **Template Examples** folder in the monitor tree. You can use the template examples to help you become familiar with using SiteScope templates. The template examples show the following:

- ▶ How to use template groups and monitors
- ▶ How to link the template remote server to template monitors
- ▶ How to use default variable values
- ▶ How to use variable ordering

The following example shows the **Unix HP basic template**. The template contains a template group, **Unix monitors for %%host%%**, two template monitors (CPU and Memory), four user-defined variables (host, user, password, and frequency), and a template remote server.



Planning Templates

Template planning is important for effective SiteScope management. You should consider the group and monitor relationships and properties in the template structure and how it fits into the overall monitoring environment.

The following are things to consider as you plan templates:

Object	Consideration
Variable properties	Decide which monitor configuration properties vary from one template deployment to another. For example, the target server address or resource to be monitored is a common variable property. You should also consider what naming conventions you want to use for groups and monitors. You use template variables to enter or select values for variable properties each time you deploy the template. Not all monitor configuration properties can be configured using variables. For more information, see “Working with Template Variables” on page 1197.
Servers	Decide which servers are the target servers, where the objects monitored are located. Template servers are replicated automatically when the template is deployed. You can also define them manually in the Microsoft Windows Remote Preferences or UNIX Remote Preferences section of the monitor tree. For more information, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.
Monitor types	Decide which monitor types you want to replicate using templates. These should be monitor types that monitor multiple systems. For example, CPU, Disk, Memory and Service monitor types are commonly deployed for each server in the infrastructure. You can also include multiple instances of the Service Monitor type in a template to monitor different services or processes running on each server.

Object	Consideration
Common properties	For configuration properties that should be the same from one template deployment to another, you must decide what the values should be. For example, the Frequency setting is a required setting for each monitor type. The default setting is 10 minutes. Depending on what is to be monitored and the overall monitor load, you may want to change this value so that monitors created using the template run more often.
Group structure	Decide the group structure you want to use to organize the monitors. The organization groups and monitors in the template should be compatible with your overall plan for organizing the monitoring in your environment. The group structure you use may affect reporting, alerting, and monitoring.
Alerts	Decide if you want to deploy alerts as part of the template. Consider which alert types and actions you want to associate with the templates and monitors. Alerts deployed as part of a template have their Alert Targets property set to all monitors defined in the template. For example, a template alert added to a template group alerts on any monitor belonging to that group. If this does not fit your alerting plan, you must edit the alert configuration after deployment or add alerts manually.

Working with Template Variables

While you can create templates without using template variables, the use of variables is central to the power and utility of templates. Template variables are substitution markers for monitor configuration settings. You create template variables to represent monitor configuration settings that you want to be able to modify whenever you deploy the template. You reference the variable in a text box in one or more template monitors. Examples of common uses for template variables are: server or host addresses, disk drive designators, file paths, and monitor name descriptions.

There are two steps you use when working with template variables:

1 Create the template variable in the template.

For more information, see “New Template Variable Page” on page 1227.

2 Reference the variable in one or more configuration objects in the template.

For more information, see “Referencing Template Variables” on page 1200.

Each variable that is referenced in a monitor or group object in a template prompts the display of a corresponding entry box when the template is deployed. The variable name is used as a label for the text entry box.

Some monitor configuration settings cannot be set using template variables. With the exception of the remote server selection menu, configuration items that are normally selected using a selection drop-down cannot be defined using template variables. Configuration items that are normally selected using a check box or radio selection cannot be configured using template variables.

Template variables are always child elements of the template container in which they reside. Variables can be referenced and used to define configuration settings for group, monitor, or alert configuration templates within the template. For information about the types of template variables in SiteScope and the specific syntax conventions, see “Variable Syntax” on page 1198.

You should plan and create the template variables before you create other template objects, such as servers and monitors. This way you can enter the references to the variables into the template monitors, groups, or alerts as you add them to the template. Deleting a template variable that has already been referenced in a template object requires that the referencing object be deleted from the template to clear the broken reference.

Tip: You can see examples of how variables are used in templates by viewing the **Template Examples** in the monitor tree. For details, see “Template Examples” on page 1194.

Variable Syntax

There are two types of template variables in SiteScope:

- ▶ **User-defined variables.** User-defined variables are used to enter text-based values during template deployment.
- ▶ **System variables.** System variables are a set of predefined variables you use to access the list of remote servers known to SiteScope and system time information.

Each type of variable has specific syntax conventions which are described in the following sections.

Syntax for User-Defined Variables

User-defined template variables can be alphanumeric characters and may contain the underscore character. They may not contain whitespace, punctuation marks, or other non-alphanumeric characters, except the underscore character. You can create as many variables as you need.

Examples of valid template variable syntax are:

```
description_text  
DiskDrive  
TARGET_URL  
matchExpression
```

You should choose variable names that describe the configuration parameter that is represented. The variable name is used as a label for the variable entry box on the variable value entry window when you deploy the template.

Syntax for System Variables

SiteScope recognizes several pre-defined template variables. These are values that are known by the system, including the list of servers for SiteScope, detected servers such as NetBIOS, as well as user-defined server connection profiles such as remote UNIX. The syntax and description for the pre-defined system variables are:

Syntax for System Variables	Description
SERVER_LIST	Returns a list from which to select one of all the servers known by the platform. Use this to enable selection of remote servers for Server or Host Name properties only.
SERVER_NAME	This variable is derived from the SERVER_LIST variable. Returns the name of the current server with \\ (backslashes) before the name. Use when referencing the server in other boxes.
SERVER_NAME_BARE	This variable is derived from the SERVER_LIST variable. Returns the name of the current server without \\ (backslashes) before the name. Use when referencing the server in a box requiring just the name of the server (for example when deploying CPU monitors or when referencing the name of the server in a description: "Disk space on server Mail.")
DATE	Returns the system date on the server where SiteScope is running. Use to add the date that a monitor was created to a name or description.
TIME	Returns the system time on the server where SiteScope is running. Use to add the time that a monitor was created to a name or description. The value is the time that the template is actually deployed.

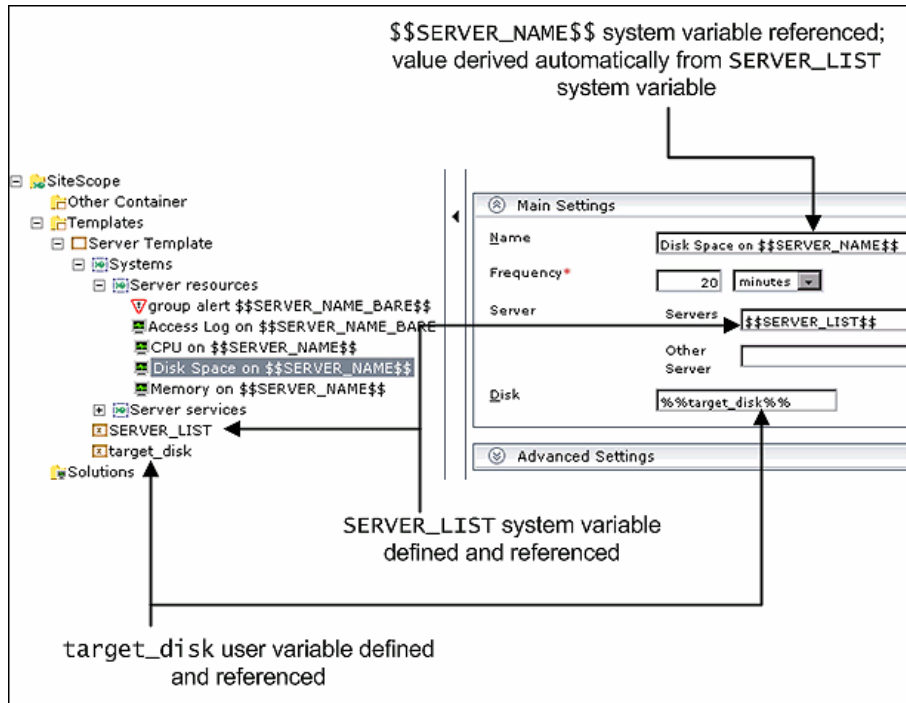
Referencing Template Variables

After you have added template variables to a template, you must create references to them in a monitor or group configuration object. The syntax you use to reference a variable depends on the type of variable.

Variable Type	Syntax	Information
User-Defined	%%variable_name%%	<p>The reference is case sensitive and syntax sensitive. The <code>variable_name</code> reference must match the template variable name and be surrounded by double % symbols.</p> <p>Note: User-defined template variables must be created before they can be referenced in monitor or group configuration templates. Using the %% symbols with a text string that has not already been added to the template as a template variable does not create a reference to a template variable even if a matching variable name is added later.</p>
System	\$\$VARIABLE_NAME\$\$	<p>The reference is case sensitive and syntax sensitive.</p> <p>The <code>SERVER_LIST</code> variable must be defined explicitly as a variable in the template. As long as this variable is defined, the <code>SERVER_NAME</code> and <code>SERVER_NAME_BARE</code> variables may be used in configuration objects by referencing them using the <code>\$\$VARIABLE_NAME\$\$</code> syntax directly in the monitor or group configuration object.</p> <p>The <code>TIME</code> and <code>DATE</code> variables can also be referenced directly.</p> <p>For information about system variables, see “Variable Syntax” on page 1198.</p>

Example

The following diagram shows examples of how to reference user-defined variables and the `SERVER_LIST` and the derived system variables for a monitor template.



Counter Selection in Monitor Templates

SiteScope includes a number of application monitor types that are designed to monitor measurements specific to the target system. These monitor types use a **Get Counters** or **Get Measurements** browser function in their properties panel. Configuring these monitor types manually requires several steps. After selecting the monitor type, you generally have to specify connection properties to the target system and then request SiteScope to retrieve the measurement counters from the remote system. The next step involves selecting the desired counters to be monitored and adding them to the configuration. After this, the monitor can be added to SiteScope.

Deploying monitors using templates does not accommodate a separate step for counter selection. Another mechanism is used to enable the selection of counters for these monitor types using templates. SiteScope uses text matching or regular expression matching to automate the counter selection step for template deployment. You do use a counter selection step when you create the template monitor.

The simplest method for counter selection in templates is to select the specific counters explicitly in the monitor template. This creates an explicit text match used to select the matching counter during deployment. For information about the steps required to add a browsable counter monitor type with explicitly selected counters, see “Add Monitors to a Template” on page 1215.

If the specific counters on the target system vary from one deployment to another, you may be able to use a regular expression to match a pattern that represents the type or category of counter you want to monitor. For more information, see below.

Modifying Counter Selection Strings to Use Regular Expressions

You can modify counter selection strings for template monitors to use regular expressions when you create the monitor or you can edit the monitor later. For more information on modifying a template monitor for regular expression counter matching, see “Modify Counter Selection Strings to Use Regular Expressions” on page 1221.

Counter Selection Using Regular Expressions

Many applications have a number of measurement counters that vary according to the system on which it is running, the configuration of system options, and the components installed. In this case, selecting explicit counters in a monitor template may not be useful across multiple instances of an application or system. Some systems have measurement counters that have a similar pattern but may vary by the name of a node or object context. You can use regular expressions in monitor templates to help automate the selection of multiple measurement counters.

Note: Use of this regular expression counter matching function requires knowledge of the counters on the system to be monitored. You should manually set up a monitor of the type you want to add to the template and carefully review the counters available on the type of system you want to monitor. Creating a "greedy" regular expression that matches large numbers of counters on a remote system may adversely affect SiteScope performance.

The steps you use to create a template monitor to use regular expressions are very similar to the procedure described in the previous section. Instead of selecting all of the counters to be monitored explicitly, you select one or more counters that are representative of all the counters you want to select. The counter selections in monitor templates are stored as text strings. You edit these strings to create patterns that SiteScope uses to find matching counters that are selected when the monitor is deployed.

Examples - Using Regular Expressions

- ▶ **Example 1.** The following is a simple example of how a regular expression can be used for counter selection for a SNMP by MIB Monitor type in a template:

You want to monitor the following three counters from several SNMP agents in your infrastructure:

```
iso/org/dod/internet/mgmt/mib-2/system/sysDescr  
iso/org/dod/internet/mgmt/mib-2/system/sysUpTime  
iso/org/dod/internet/mgmt/mib-2/system/sysName
```

You could select all three counters explicitly in the template monitor. Alternately, you could select one of these and then modify the counter string to be a regular expression such as the following:

```
/iso/org/dod/internet/mgmt/mib-2/system/sys[DUN][a-zT]*/
```

In this example, the counter selection string has been edited to add a pair of / slashes before and after the string. This is necessary to indicate that the string is to be interpreted as a regular expression. Because the selection string included several / slash characters initially, each of these characters must be escaped by adding a \ backslash character immediately preceding it. The [DUN][a-zT]* string includes two character class declarations commonly used in regular expression syntax. For more information on regular expression syntax, see “Using Regular Expressions” on page 1493.

- **Example 2.** The following is an example of how a regular expression can be used for counter selection for a UNIX Resource Monitor type in a template:

You want to monitor daemon processes running on several UNIX or Linux servers in your infrastructure. The list of processing running might include the following:

```
Process\-bash\NUMBER RUNNING
Process\..java/bin/java\NUMBER RUNNING
Process\./ns-admin\NUMBER RUNNING
Process\./ns-proxy\NUMBER RUNNING
Process\./ns-sockd\NUMBER RUNNING
Process\bin/sh\NUMBER RUNNING
Process\etc/init\NUMBER RUNNING
Process\usr/apache/bin/httpd\NUMBER RUNNING
Process\usr/lib/nfs/statd\NUMBER RUNNING
Process\usr/lib/saf/sac\NUMBER RUNNING
Process\usr/lib/saf/ttymon\NUMBER RUNNING
Process\usr/lib/snmp/snmpd\NUMBER RUNNING
Process\usr/lib/ssh/sshd\NUMBER RUNNING
...
```

You can create a regular expression counter selection string to match only those processes that end with the letter "d". The following is an example regular expression to match this pattern:

```
/Process[\\Ww]{5,18}d[\\W]{1,2}NUMBER RUNNING/
```

As with Example 1, the counter selection string includes / slashes before and after the string to indicate that the string is a regular expression. The example process strings on the UNIX server include combinations of \ back slash and / forward slash characters. Because these characters have special meaning in regular expressions, they would have to be escaped. This can be complicated because the process strings have many variations and combinations of these and other symbols. The example regular expression used here simplifies the expression by using character class declarations. The [W] class is used to match punctuation marks. This matches on the \, -, ;, and / characters that appear in some of the process strings without the need to escape the characters individually. For more information on regular expression syntax, see “Using Regular Expressions” on page 1493.

Updating Template Deployments

Using the Publish Template Changes Wizard, you can view how the actual monitored deployments comply with the standardized deployment as defined in the template. This ensures that any changes in the monitored environment can be quickly updated in the monitoring infrastructure and that the monitoring infrastructure is still compliant with the standards set in the template.

Note: Only a SiteScope administrator user can run the Publish Template Changes Wizard.

When you deploy a template, the parent template group is automatically associated to the template. If you subsequently make changes to the template, you can automatically publish the changes to SiteScope objects deployed by the template using the Publish Template Changes Wizard. This enables you to update related deployed groups across the enterprise whenever the template is updated without having to update each object. A deployed group consists of the groups, monitors, alerts, variables, and the remote server configured in the template.

The Publish Template Changes Wizard enables you to update deployed groups in two ways.

- ▶ You can publish only the changes in the template to the deployed groups. This would create added objects, update values of existing objects, but leave other objects not in the template intact.
- ▶ You can publish the changes in the template to the deployed groups and have SiteScope make the above changes and delete all other SiteScope objects from the group that are not in the template groups.

While in the wizard, you perform the following:

- ▶ Select the groups associated with the selected template that you want to update with the template changes and the template update option.
- ▶ View the structural and content differences between the template and the groups in which the template has been deployed.

- View a list of all properties of the selected entity to be updated, including the current and the replacement values, and the type of change.
- Enter values for new variables. You can also modify values for existing variables.
- Publish the changes and view a summary of the results.

Notes

- If you are using groups deployed by templates created in previous versions of SiteScope, root groups are not associated with the source template. You can update these template deployments by manually associating the template groups with the source template by using Global Search and Replace, or by typing the path of the source template in the **Source Template** box in the Advanced Settings for the current group.
- Templates and deployed groups are internally linked by an ID. This means that you can publish changes even if the name of the template or the root group in a deployed group have changed.
- For changes to be published, all changes in the root group hierarchy must succeed. If any changes to a group fail, all changes to that group are rolled back
- You cannot replace an existing monitor target server using the Publish Template Changes wizard or auto deployment update (see “Publishing Template Changes Using the XML” on page 1259), although you can change property values of the target server itself if required.

For details on how to publish template changes, see “Publish Template Updates to Related Group Deployments” on page 1218.

For details on the Publish Template Changes Wizard user interface, see “Publish Template Changes Wizard - Select Deployed Groups Page” on page 1240.

Configure a SiteScope Monitoring Solution Using a Template – Workflow

This task describes the steps for creating a SiteScope monitoring solution using a template. To view a flowchart of this task, see “Configure a SiteScope Monitoring Solution Using a Template – Flowchart” on page 38.

Tip:

- ▶ It is recommended to create these objects in the order listed, although you may not always require all of the objects.
 - ▶ To help you get started with templates, SiteScope provides example templates for monitoring in Windows and UNIX HP environments. For details, see “Template Examples” on page 1194.
-

This task includes the following steps:

- ▶ “Prerequisites” on page 1209
- ▶ “Create a Template Container” on page 1209
- ▶ “Create a Template” on page 1209
- ▶ “Create Template Variables” on page 1209
- ▶ “Create a Template Remote Server” on page 1210
- ▶ “Create a Template Group” on page 1211
- ▶ “Create Template Monitor Instances” on page 1211
- ▶ “Set Up Monitor and Group Alerts” on page 1212
- ▶ “Deploy the Template” on page 1212
- ▶ “Results” on page 1213
- ▶ “Set Up Monitor and Group Reports” on page 1214
- ▶ “Publish Changes to the Monitoring Solution” on page 1214

1 Prerequisites

Check that the post-installation administration tasks have been performed before configuring SiteScope for monitoring. For details, see “Setup and Administration” on page 32.

2 Create a Template Container

Create a template container to enable you to manage your monitoring solution. For details on the user interface, see “New Template Container Page” on page 1224.

3 Create a Template

Add a template to the template container. This is the container for your monitoring solution, in which you will create groups, monitors, remotes, variables, and alerts for the monitoring solution. For details on the user interface, see “New Template Page” on page 1225.

Note: You can also copy an existing group and monitor hierarchy from a SiteScope to the template and edit the elements for use as a template. For details on this task, see “Create a Template by Copying Existing Configurations” on page 1214.

4 Create Template Variables

You can create template variables in the template that enable you to specify a different name for an object every time that you deploy the template. Variables are the first objects that you typically want to create in a template, because these are referred to when you create groups, monitors, servers, and alerts. For details on the user interface, see “New Template Variable Page” on page 1227.

5 Create a Template Remote Server

In the template, you can define a remote Windows NT or UNIX server where the objects monitored are located. A template monitor may run on servers that are defined by template servers at the time of template deployment or on servers defined manually in the Remote Preferences. Template servers are added to the monitor tree under Microsoft Windows Remote Preferences or UNIX Remote Preferences when the template is deployed. For details on the user interface, see “New Template Remote Server Page” on page 1229.

Note: You can add only one remote server to a template. This does not apply to templates created in previous versions of SiteScope.

Example

In the example, you can see that a Windows template remote server has been created with the name `%%host%% remote windows`.

The screenshot shows the 'Properties' dialog for a 'TemplateRemoteNT' server. The title bar reads 'TemplateRemoteNT "%%host%% ...e windows"'. The 'Main Settings' section is visible, containing the following fields:

- Host ***: %%host%%
- Login**: %%user%%
- Password**: *****
- Credentials**: (empty)
- Name**: %%host%% remote windo
- Trace**:
- Method**: NetBIOS (dropdown menu)
- Remote Machine**: Cp1252
- Encoding ***: (empty)

6 Create a Template Group

In the template, create a template group in which you can make the deployment of monitors and associated alerts manageable and effective for your organization. For details on the user interface, see “New Template Group Page” on page 1226.

Note: A template can have only one template group directly under it (the parent group). This does not apply to templates created in previous versions of SiteScope.

7 Create Template Monitor Instances

- a** Select the monitor instances you want to add to the template group. For details on how to perform this task, see “Add Monitors to a Template” on page 1215.

Note: A template monitor may run on servers that are defined by template servers at the time of template deployment or on servers defined manually in the Remote Preferences branch of the monitor tree. Whichever is the case, the value in the **Servers** box must match the host name of an actual server at the time that the template is deployed after values have been substituted for the template variables. If the server name does not match the host name of a real server, the monitor fails.

- b** Set thresholds for monitors by manually setting logic conditions that determine the reported status of each monitor instance. For details on the user interface, see “Threshold Settings” on page 518.

Note: After deploying the template, you can also set thresholds for one or multiple monitors using a baseline. For details on how to set monitor thresholds using a baseline, see “Set Monitor Thresholds Using a Baseline” on page 493.

- c** Build dependencies between groups and key monitors to help control redundant alerting. For details on this topic, see “Monitoring Group Dependencies” on page 473.

8 Set Up Monitor and Group Alerts

Create alerts to send notification of an event or change of status in some element or system in your infrastructure. For details on how to configure alerts, see “Configure an Alert” on page 1409.

9 Deploy the Template

After creating a SiteScope monitoring template, deploy the template to a group within the monitor tree.

- a** Create a group under the SiteScope root where you want to deploy the solution, and deploy the template by copying and pasting it to the destination container.
- b** Type the required variable values in the entry boxes displayed. The entry boxes displayed correspond to the template variables used in the template objects.

Note:

- You can deploy monitors to multiple servers at the same time by entering the server names or addresses separated by a comma (",") when prompted to type the required information for the monitored servers. When doing this, the value in the **Host** property for the template remote referenced by the monitors must consist of a variable value, and only one variable is allowed.
- An error message is displayed if a monitor cannot be deployed. This may occur, for example, when deploying the Disk Space monitor template, if the disk drive does not exist on the deployed server.

Tip: You can also deploy and update the template using an XML file external to the SiteScope user interface. For details on this topic, see “Auto Template Deployment Overview” on page 1254.

Example

If you deploy the **Windows basic template** from the **Template Examples** folder in the monitor tree to a SiteScope group, the following entry boxes are displayed in the Variable Values input window.

The screenshot shows a window titled "Variable Values" with a close button in the top right corner. Below the title bar is a section titled "Main Settings" with a refresh icon. It contains four input fields:

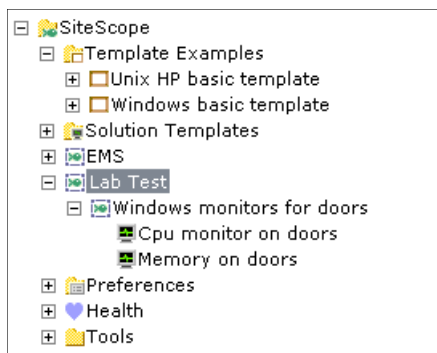
- Host *
- User Name *
- Password *
- Frequency (sec) * (with the value 600 entered)

10 Results

SiteScope adds the monitors and alerts to the specified container in the monitor tree.

Example

In this example, the template example **Windows basic template** was deployed to a group container named **Lab Test**. You can see that the **Windows monitors** template group that contains a **CPU monitor** and **Memory monitor**, was deployed to monitor resource usage on a server named **doors**.



11 Set Up Monitor and Group Reports

Create reports to display information about how the servers and applications you are monitoring have performed over time. For details on how to create reports, see “Create a Report” on page 1444.

12 Publish Changes to the Monitoring Solution

You can make changes to deployed templates, for example, add or remove monitors or modify monitor properties. You do this by editing the template and using the Publish Template Changes Wizard to publish the changes to all the relevant objects deployed by the template. For details on how to perform this task, see “Publish Template Updates to Related Group Deployments” on page 1218.

Create a Template by Copying Existing Configurations

This task describes the steps involved in copying an existing group and monitor hierarchy from a SiteScope to the template and editing the elements for use as a template.

To copy an existing group and monitor hierarchy from a SiteScope to the template:

- 1 Right-click the group, monitor, or alert you want to copy, and select **Copy**.
- 2 Select the template or group within the template folder to which you want to add the copied configurations, and click **Paste**.
- 3 If you are using template variables in the new template, edit each copied object by right-clicking the object and choosing **Edit** to replace the applicable configuration field's value with the required variable syntax. For details on this topic, see “Referencing Template Variables” on page 1200.

Add Monitors to a Template

This task describes the steps involved in creating monitor templates.

This task includes the following steps:

- “Select the Monitor Type” on page 1215
- “Type a Monitor and Host Name” on page 1215
- “Select Counters (for Monitors with Browsable Counters)” on page 1217
- “Configure the Monitor Settings” on page 1217

1 Select the Monitor Type

Select the monitor type you want to configure for the template. For details on the user interface, see “New Template Monitor Page” on page 1236.

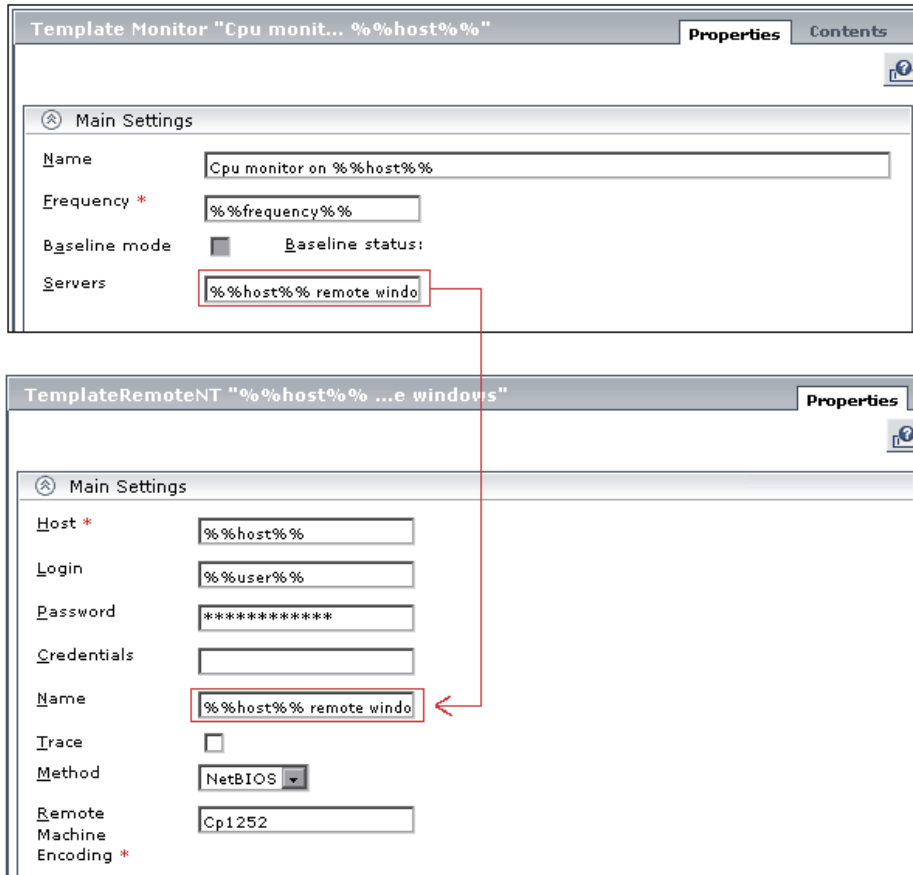
2 Type a Monitor and Host Name

Type a monitor name of your choosing in the **Name** box and the host name in the **Servers** box. If you are using template variables, type the variable syntax for all fields whose values are to be replaced with a variable. This includes use of the `SERVER_LIST` system variable.

If the monitor requires the remote server, enter the same value from the template remote server **Name** field in the **Servers** box for the newly-created template monitor. These names must match for SiteScope to connect the newly-created remote server to the newly-created monitor. For details on the user interface, see “New Template Monitor Page” on page 1236.

Example

In this example, the template monitor (a SiteScope CPU monitor) is configured to run on the template remote server, %%host%% remote windows.



3 Select Counters (for Monitors with Browsable Counters)

Select counters for monitor types designed to monitor measurements specific to the target system.

- a** Click the **Get Measurements** or **Get Counters** button, and select a server or type the connection information for a server that is running the service or application that you want to monitor.
- b** Click the **Get Measurements** or **Get Counters** button again to retrieve the available counters. The counter selection dialog box is updated.
- c** Select the measurements or counters that you want to monitor. If the specific counters on the target system vary from one deployment to another, you can use a regular expression to match a pattern that represents the type or category of counter you want to monitor. For details on how to perform this task, see “Modify Counter Selection Strings to Use Regular Expressions” on page 1221.

4 Configure the Monitor Settings

Configure the other monitor setting values as required. For details on the user interface, see “Common Monitor Settings” on page 510.

Publish Template Updates to Related Group Deployments

This task describes the steps involved in publishing template changes to related group deployments using the Publish Template Changes Wizard.

This task includes the following steps:

- ▶ “Begin Running the Wizard” on page 1218
- ▶ “View the Structural and Content Differences” on page 1219
- ▶ “Add New Variable Values” on page 1220
- ▶ “Review the Publish Template Changes Results” on page 1220




1 Begin Running the Wizard

Run the wizard. On the first page, select the related template groups that you want to update. You can also select the **Enable Delete on Update** option to delete SiteScope objects from the deployed groups that are not in the source template. For details on the user interface, see “Publish Template Changes Wizard - Select Deployed Groups Page” on page 1240.

Example - Select Deployed Groups Page

Select Deployed Groups

Select the groups that are associated with the deployed template to which you want to publish template changes.

-  SiteScope
 -  Lab Test
 -  Lab Test 2

Enable Delete on Update. (Enables you to delete from the deployed templates, all SiteScope objects that are not in the source template.)

2 View the Structural and Content Differences

View the structural differences between the template and the deployed groups. For details on the user interface, see “Review Compliancy Page” on page 1242.

To view content differences in the template objects, click the **View Differences** link to open the Content Changes dialog box. This link only appears if there is a content difference. For details on the user interface, see “Content Changes Dialog Box” on page 1244.

Example - Review Compliancy Page

Review Compliancy

Displays the structural differences between the template and the deployed groups. If there are differences between the template and the deployed group object properties, you can click the View Differences link to display these differences.

Total number of deployed groups for publishing changes: 2

2 deployed groups with structural/content differences

Group Name	Content Differences
<input checked="" type="checkbox"/> SiteScope\Lab Test 2\Lab M1 <ul style="list-style-type: none"> <input type="checkbox"/> Memory View Differences <input type="checkbox"/> CPU on doors - (Does not exist in template) - <input type="checkbox"/> Win Services State - (Does not exist in template) - <input type="checkbox"/> Memory Alert - (Added) - <input type="checkbox"/> Mail Alert - (Added) - <input type="checkbox"/> Windows Remote Servers - <input type="checkbox"/> asasa - (Unused) - 	View Differences
<input checked="" type="checkbox"/> SiteScope\Lab Test\Lab M1 <ul style="list-style-type: none"> <input type="checkbox"/> Memory View Differences <input type="checkbox"/> CPU on doors - (Does not exist in template) - 	View Differences

Example - Content Changes

Content Changes

Review details of the content changes to be performed on the object's properties.

Type : Monitor
Name : Memory

/ 1 Pages

Property Name ▲	Old Value	New Value	Action
Update every	600	900	Modified
Server	SiteScope Server	popeye	Modified

3 Add New Variable Values

Add values for any new variables in the template. Variable values that are mandatory are indicated by a red asterisk (*). You can also edit values of existing variables. Click **Finish** to complete the wizard and publish the template updates. For details on the user interface, see “Modify Variables Page” on page 1246.

Example:

Modify Variables

Total number of deployed groups for publishing changes: 1

1 deployed groups with missing variable values

Enter missing variable values in the Variable Value box below. A red asterisk indicates that the variable value is mandatory.

Group Name	Variable Name	Variable Value
<input type="checkbox"/> <input checked="" type="checkbox"/> SiteScope\Lab Test\Lab M1	Host* Frequency* Server*	<input type="text" value="doors"/> <input type="text" value="600"/> <input type="text"/>

4 Review the Publish Template Changes Results

Review the results of the publish template changes and, if necessary, retry publishing the changes to the deployed groups that failed to update. For details on the user interface, see “Publish Results Summary Page” on page 1247.

Optionally, you can export the publish changes results to a summary report (.pdf file). For details on the summary report, see “Publish Template Changes Summary Report” on page 1248.

Example - Publish Results Summary Page

Publish Results Summary

Displays a summary of the deployed groups affected by the template changes.

1 deployed groups were successfully updated.

1 deployed groups were not updated.

Deployments which were not changed:

Group Name	Reason
SiteScope\Lab Test 2\Lab M1 Resources	Unknown internal error during publish changes.

Modify Counter Selection Strings to Use Regular Expressions

This task describes the steps involved in modifying a template monitor to use a regular expression for measurement counter selection.

To modify a template monitor for regular expression counter matching:

- 1** Right-click the monitor template you want to modify, and click **Edit** to open the template monitor properties view.
- 2** In the **Measurements** or **Counters** section of the Main Settings panel (depending on the monitor type), select a counter selection string that is representative of the pattern of counters you want to configure for the monitor, and click the **Edit** button for the counter string you want to edit. A string edit dialog opens.
- 3** Modify the counter selection string to be a regular expression by adding a slash ("/") character to the beginning and end of the string. Modify the string to use other pattern matching syntax as required. For more information on regular expression syntax, see “Using Regular Expressions” on page 1493.



Note: If the template monitor was configured with explicit counter selections that can be matched using the regular expression that was entered, you can delete the extra counter strings by clicking the **Delete** button to the right of the counter string.

Export and Import a Template

This task describes the steps involved in exporting and importing a template.

This task includes the following steps:

- “Export a Template” on page 1222
- “Import a Template” on page 1222
- “Result” on page 1222

1 Export a Template

Export the template container object that contains the templates you want to use in other SiteScope installations. For details on the user interface, see “Export Template Page” on page 1238.

2 Import a Template

Once you have exported templates, you can copy the export file to another SiteScope server and import the template container object that contains the template or templates you want to use. For details on the user interface, see “Import Template Page” on page 1239.

3 Result

Templates contained in the file are added to the template container. The imported templates can be used directly or modified as required.

Reserved Template Group Types

The following table shows template types used by the SiteScope application. The templates in these directories are reserved, and are not used by alerts. For a list of templates used in alerts, see “SiteScope Alert Templates Directory” on page 1414.

Note: You should not modify the templates in these directories without specific procedures provided in the product documentation or as instructed by HP Software Support.

Template Group	Description	Location
MIB	Text used with SNMP traps	<SiteScope root directory>\ templates.mib
Operating System	Shell commands to be run when monitoring remote UNIX servers	<SiteScope root directory>\ templates.os
Performance Monitor	Used for NT performance monitoring	<SiteScope root directory>\ templates.perfmon
Sound	Audio files used for sound alerts	<SiteScope root directory>\ templates.sound
View	Query and XML/XSL templates	<SiteScope root directory>\ templates.view


SiteScope Templates User Interface

This section describes:

- New Template Container Page on page 1224
- New Template Page on page 1225
- New Template Group Page on page 1226

- ▶ New Template Variable Page on page 1227
- ▶ New Template Remote Server Page on page 1229
- ▶ New Template Monitor Page on page 1236
- ▶ New Template Alert Page on page 1237
- ▶ Export Template Page on page 1238
- ▶ Import Template Page on page 1239
- ▶ Publish Template Changes Wizard - Select Deployed Groups Page on page 1240
- ▶ Generate Auto Deployment XML on page 1250

New Template Container Page


Description	<p>Enables you to define a new template container. You use template containers to store and manage templates. Template containers enable you to group and organize multiple templates in ways that describe their purpose or classification.</p> <p>Templates are displayed with the  icon in the monitor tree. Possible contents of a template container are templates.</p> <p>To access: Right-click the SiteScope node container, and click New Template Container.</p>
Included in Tasks	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208</p> <p>“Create a Template by Copying Existing Configurations” on page 1214</p>
Important Information	<p>Template containers can only be added to the SiteScope node in the monitor tree.</p>
Useful Links	<p>“Understanding Templates” on page 1192</p> <p>“Template Examples” on page 1194</p>

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	Type a name for the template container. Maximum length: 250 characters

New Template Page


Description	<p>Enables you to add a template to a template container. An individual template is comprised of the object definitions of those objects that are created when the template is deployed.</p> <p>Templates are displayed with the  icon in the monitor tree. Possible contents of a template are groups, variables, and a remote server.</p> <p>To access: Right-click a template container, and click New Template.</p>
Included in Tasks	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208</p> <p>“Create a Template by Copying Existing Configurations” on page 1214</p>
Important Information	<p>A template can have only one template group directly under it (the parent group). This does not apply to templates created in older versions of SiteScope.</p>
Useful Links	<p>“Understanding Templates” on page 1192</p> <p>“Template Examples” on page 1194</p>

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	Type a name for the template. The name you enter appears in the monitor tree as a child node of the templates container. Maximum length: 250 characters.

New Template Group Page


Description	Enables you to add a template group to a template or to a template group to create a subgroup. You use template groups to replicate monitoring deployment to multiple locations in the infrastructure. Template groups are displayed with the  icon in the monitor tree. Possible contents of a template group are monitors, alerts, and subgroups. To access: Right-click a template or template group in the monitor tree, and click New Group .
Included in Tasks	“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208
Important Information	A template can have only one template group directly under it (the parent group). This does not apply to templates created in older versions of SiteScope. You can create template monitors, alerts, and subgroups in the parent group or in subgroups only.
Useful Links	“Understanding Templates” on page 1192 “Template Examples” on page 1194

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Group Name	Enter a name for the template group, preferably using a template variable. A template variable enables you to specify a different name for the group every time that you deploy the template. If the group name does not include a variable, multiple deployments of the template in the same directory will fail because the group name is not unique. For details on using template variables, see “Referencing Template Variables” on page 1200.

New Template Variable Page


Description	<p>Enables you to add a template variable to a template. A variable is used to enable prompting for user input during template deployment. Template variables are either user-defined or predefined system variables that provides access to the list of remote server connections known to SiteScope.</p> <p>Template variables are displayed with the  icon in the monitor tree.</p> <p>To access: Right-click a template, and click New Variable.</p>
Included in Tasks	“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208
Useful Links	<p>“Understanding Templates” on page 1192</p> <p>“Working with Template Variables” on page 1197</p> <p>“Template Examples” on page 1194</p>

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	Type a name for the template variable. The name you enter is used to identify the variable in the template in the monitor tree. This is the name that must be used when referring to the variable in other template objects. Note: The name of a variable cannot be edited once the variable has been added. To change a variable name, delete the variable and create a new one with the correct name.
Display Name	Type a display name if you want a different name to be displayed instead of the variable name on deployment. You should still use the variable name when referencing the variable in a template object.
Description	Type a description for the variable.
Default Value	Type a default value to be used for this variable substitution. If you do not enter a value in this box and the box requires a value, you are prompted to enter a value when deploying the template.
Display Order in Template	Type the variable display sequence number. This is the order in which SiteScope prompts you to enter values for a variable on deployment. Variables are displayed in ascending order. Variables that have no display number are displayed at the end. Note: The display order does not change the order of the variables within the template definition.
Mandatory Variable	If selected, the variable field requires a value and prompts you to enter a value when deploying the template. To set a variable with a non-mandatory value, clear the check box. When this option is cleared, SiteScope uses an empty String("") as a value for a non-mandatory variable. Default value: Selected

New Template Remote Server Page

Description	<p>Enables you to create a UNIX or Windows remote server in the template. A template remote server is used to define remote server preferences that are created when the template is deployed.</p> <p>A template remote server is displayed with the  icon in the monitor tree.</p> <p>To access: Right-click a template, and click New Remote NT or New Remote Unix.</p>
Included in Tasks	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208</p>
Important Information	<ul style="list-style-type: none"> ▶ Type the actual values for those fields that remain constant throughout the template deployment. Type template variables in those fields whose values are replaced with a variable value when the template is deployed. For details, see “Referencing Template Variables” on page 1200. ▶ You can add only one remote server to a template. This does not apply to templates created in older versions of SiteScope. ▶ You cannot replace an existing monitor target server using the Publish Template Changes wizard or auto deployment update (see “Publishing Template Changes Using the XML” on page 1259), although you can change property values of the target server itself if required.
Useful Links	<p>“Understanding Templates” on page 1192</p> <p>“Absolute Schedule Preferences” on page 224</p> <p>“Microsoft Windows Remote Preferences” on page 219</p> <p>“UNIX Remote Preferences” on page 220</p> <p>“Template Examples” on page 1194</p>

Main Settings - NT Remote

Note: The variable examples used in the following table are based on examples used in the **Template Examples** in the monitor tree.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Host	<p>Enter the name of a template variable that represents the remote server name, for example, %%host%%. This enables you to add each server as you deploy the template when asked to type the required information for the variables. Each time you type a server name for the variable, a monitor instance is created for that server and the server is added to remote preferences.</p> <p>If the remote servers onto which you want to deploy monitor templates already exist under Remote Preferences, you can reference these servers within the monitor template. You do this by referencing the system variable \$\$SERVER_LIST\$\$ which identifies the servers accessible to the SiteScope. For details, see “Syntax for System Variables” on page 1199.</p> <p>Note: The host name must match an actual server host name after values are substituted for the variables at the time that the template is deployed. If the host name does not match a server name at that time, the monitor fails.</p>
Login	<p>Type the login for the remote server or use a template variable that represents the user login name, for example, %%user%%.</p>
Password	<p>Type the password for the remote server or the passphrase for the SSH key file, or use a template variable that represents the password, for example, %%password%%. When using SSH authentication with public/private key based authentication enter the passphrase for the identity file here.</p>

GUI Element	Description
Name	<p>Type a name by which the remote machine should be known in SiteScope. For example, %%host%% remote windows. For each template monitor that requires this remote server, you must enter this same value in the Servers box for the template monitor.</p> <p>Note: Names must be unique, otherwise the deployment fails.</p>
Trace	<p>Select to trace messages to and from the subject server, recorded to the SiteScope RunMonitor.log file.</p>
Method	<p>SiteScope uses one of two connection types for monitoring Windows server resources. From the drop-down list select:</p> <ul style="list-style-type: none"> ▶ NetBIOS. The default server-to-server communication protocol for Windows NT and 2000 networks. ▶ SSH. Secure Shell, a more secured communication protocol that can be installed on Windows NT/2000 based networks. This connection method normally requires installing SSH libraries on each server to be connected. For more information see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1541.
Remote Machine Encoding	<p>Type the encoding for the remote server, if the remote server is running an operating system version that uses a different character encoding than the server on which SiteScope is running. This enables SiteScope to display encoded content correctly.</p> <p>Default value: Cp1252 encoding</p> <p>Other encodings: Cp1251, Cp1256, Shift_JIS, EUC_JP</p>

Main Settings - Unix Remote

Note: The variable examples used in the following table are based on examples used in the **Template Examples** in the monitor tree.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element	Description
Host	<p>Enter the name of a template variable that represents the remote server name, for example, %%host%. This enables you to add each server as you deploy the template when asked to type the required information for the variables. Each time you type a server name for the variable, a monitor instance is created for that server and the server is added to remote preferences.</p> <p>If the remote servers onto which you want to deploy monitor templates already exist under Remote Preferences, you can reference these servers within the monitor template. You do this by referencing the system variable \$\$SERVER_LIST\$\$ which identifies the servers accessible to the SiteScope. For details, see “Syntax for System Variables” on page 1199.</p> <p>Note: The host name must match an actual server host name after values are substituted for the variables at the time that the template is deployed. If the host name does not match a server name at that time, the monitor fails.</p>
Login	<p>Type the login for the remote server or use a template variable that represents the user login name, for example, %%user%.</p>
Password	<p>Type the password for the remote server or the passphrase for the SSH key file, or use a template variable that represents the password, for example, %%password%. When using SSH authentication with public/private key based authentication enter the passphrase for the identity file.</p>

GUI Element	Description
Name	<p>Type a name by which the remote machine should be known in SiteScope. For example, %%host%% remote unix. For each template monitor that requires this remote server, you must enter this same value in the Servers box for the template monitor.</p> <p>Note: Names must be unique, otherwise the deployment fails.</p>
Trace	<p>Select to trace messages to and from the remote server in the RunMonitor.log file.</p>
OS	<p>The operating system that is running on a remote server. This is required so that the correct information can be obtained from that server.</p> <p>The following operating systems are supported when defining Remote Unix servers: AIX, FreeBSD, HP, HP64, Linux, MacOSX, OPENSERVICES, RHESlinux, SCO, SGI, Sun, Tru64, Tru64 4.x. For servers running versions of UNIX which are not included in the list, see “UNIX Operating System Adapters” on page 1529.</p>
Method	<p>The currently supported methods are:</p> <ul style="list-style-type: none"> ▶ Telnet. Log in to the remote server using Telnet. ▶ SSH. Log in to the remote server using the SSH protocol. This may require additional software and setup depending on the version of UNIX. For more information on SSH requirements, see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1541. ▶ Rlogin. Log in to the remote server using the Rlogin protocol. ▶ HTP. Connect to an HTTP server on the remote server and run the command by using a CGI. For this method the Login and Password are optional and are used for authorizing SiteScope to log on to the remote machine if required. <p>For more information, see “Connection Methods for Remote UNIX” on page 299.</p>

GUI Element	Description
Prompt	This is the prompt output when the remote system is ready to handle a command. Default value: #
Login Prompt	This is the prompt output when the system is waiting for the login to be entered. Default value: login:
Password Prompt	This is the prompt output when the system is waiting for the password to be entered. Default value: password:
Secondary Prompt	Type the secondary prompts if the telnet connection to the remote server causes the remote server to prompt for more information about the connection. Separate multiple prompt string by commas (,).
Secondary Response	Type the responses to any secondary prompts required to establish connections with this remote server. Separate multiple responses with commas (,).


GUI Element	Description
Initialize Shell Environment	<p>Type any shell commands to be run at the beginning of the session. Separate multiple commands with a semicolon (;). This option specifies shell commands to be run on the remote machine directly after a Telnet or SSH session has been initiated. These commands can be used to customize the shell for each SiteScope remote. Some examples include:</p> <ul style="list-style-type: none"> ▶ The remote shell may not have the correct path set for SiteScope scripts to run. The following command adds the directory /usr/local/bin into the PATH of the current shell on the remote machine: <code>export PATH=\$PATH:/usr/local/sbin</code> ▶ The remote shell may not be initializing the pseudo terminal correctly. Type the following command to increase the terminal width to 1024 characters: <code>stty cols 1024;\${SHELL}</code> <p>Note: Commands after a shell invocation are not run.</p> <ul style="list-style-type: none"> ▶ There have been cases where the remote Telnet Server does not echo back the command line properly. This may cause strange behavior for monitors that rely on this behavior. Type the following command to force the remote terminal to echo: <code>stty echo</code> ▶ Certain UNIX shells have been known to behave erratically with SiteScope. This includes bash, ksh, and csh. Type the following command to change the shell to sh for the SiteScope connection: <code>/bin/sh</code>
Remote Machine Encoding	<p>Type the encoding for the remote server if the remote server is running an operating system version that uses a different character encoding than the server on which SiteScope is running. This enables SiteScope to display encoded content correctly.</p> <p>Default value: Cp1252 encoding</p> <p>Other encodings: Cp1251, Cp1256, Shift_JIS, EUC_JP</p>

New Template Monitor Page

Description	<p>Enables you to add a template monitor to a template or template group. Template monitors are used as the basis for the creation of actual monitors at the time that the template is deployed.</p> <p>Template monitors are displayed with the  icon in the monitor tree. You can create template monitors only in a template group. Possible contents of a template monitor are alerts.</p> <p>To access: Right-click a template, and click New Monitor. Select the monitor type you want to configure for the template.</p>
Included in Tasks	“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208
Important Information	Template monitors are not active monitor instances. Monitors are created and activated based on these template configurations only when you deploy the template.
Useful Links	<p>“Understanding Templates” on page 1192</p> <p>“Template Examples” on page 1194</p>

For descriptions of the elements found in the New SiteScope Monitor page, see “New SiteScope Monitor Page” on page 508.

New Template Alert Page

Description	<p>Enables you to define alerts for a template, a template group, or a template monitor. Template alerts are used to define alerts on monitors that are created when the template is deployed.</p> <p>Template alerts are displayed with the  icon in the monitor tree. You can create template alerts only in a template group.</p> <p>To access: Right-click the template, template group, or template monitor for the alert. Click New Alert.</p>
Included in Tasks	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1208</p>
Important Information	<p>You cannot select the Disable or Enable Monitors alert action when creating an alert template. Template alerts are enabled for all the monitors belonging to the object for which they were defined. For example, if an alert is defined for a monitor, then it is activated on that monitor only. If an alert is defined for a template, then it is activated for all the monitors in the template.</p>
Useful Links	<p>“Understanding Templates” on page 1192</p> <p>“Template Examples” on page 1194</p>

For descriptions of the elements found in the New Template Alert page, see “SiteScope Alerts - Add/Edit Alert” on page 1415.

Export Template Page

Description	Enables you to export templates for use in other SiteScope installations. This allows you to replicate standardized monitor configurations across the enterprise. To access: Right-click the template container object in the monitor tree that contains the template or templates you want to export, and click Export .
Included in Tasks	“Export and Import a Template” on page 1222
Important Information	SiteScope templates are stored as binary data. This is different from the text-based monitor sets used in earlier versions of SiteScope. Any changes to templates must be performed using the SiteScope interface.
Useful Links	“Understanding Templates” on page 1192 “Import Template Page” on page 1239

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Export File Name	Type a name that is descriptive of the template or templates to be exported.
File Path	The location to which the template file is saved for export. Accept the default location, or enter a different location. Default value: <SiteScope_install_path>\SiteScope\export
Templates to export	Select the templates you want to export. Default value: All templates within the template container are exported.

Import Template Page

Description	Enables you to import template configurations from other SiteScope installations. This allows you to efficiently replicate standardized monitor configurations across the enterprise. To access: Right-click the template container in the monitor tree into which you want to import the template or templates, and click Import .
Included in Tasks	“Export and Import a Template” on page 1222
Useful Links	“Understanding Templates” on page 1192 “Export Template Page” on page 1238

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Import File Name	Type the name of the file you want to import.
File Path	The location of the template file to be imported. Accept the default location, or enter a different location. Default value: <SiteScope_install_path>\SiteScope\export

Publish Template Changes Wizard - Select Deployed Groups Page

Description	<p>The first page in the Publish Template Changes wizard. Use the Publish Template Changes wizard to check deployed groups for template compliancy and to update SiteScope objects deployed by templates whenever the source template is updated.</p> <p>To access: In the monitor tree, right-click a template, and click Publish Changes.</p> <p>Use the Select Deployed Groups Page to select groups associated with the source template for which you want to apply template changes.</p>
Important Information	<p>The wizard opens only if there are deployments associated with the selected template.</p>
Included in Tasks	<p>“Publish Template Updates to Related Group Deployments” on page 1218</p>
Wizard Map	<p>The Publish Template Changes wizard contains:</p> <p>Publish Template Changes Wizard - Select Deployed Groups Page > Review Compliancy Page > Content Changes Dialog Box > (Modify Variables Page) > Publish Results Summary Page > Publish Template Changes Summary Report</p>
Useful Links	<p>“Updating Template Deployments” on page 1206</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<List of groups associated with the selected template>	Select the groups associated with the selected template that you want to update with the template changes. Default value: All associated groups and subgroups are selected.
Enable Delete on Update	If selected, enables you to delete from the deployed groups, all SiteScope objects that are not in the source template. This enables you to ensure template compliancy.

Review Compliance Page

Description	Displays the structural differences between the source template and the deployed groups, and provides links to content differences in the deployed group objects.
Included in Tasks	“Publish Template Updates to Related Group Deployments” on page 1218
Wizard Map	The Publish Template Changes wizard contains: Publish Template Changes Wizard - Select Deployed Groups Page > Review Compliance Page > (Content Changes Dialog Box) > (Modify Variables Page) > Publish Results Summary Page > Publish Template Changes Summary Report
Useful Links	“Updating Template Deployments” on page 1206

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<N> deployed groups with structural/content differences	Displays the deployed groups and group objects (subgroups, monitors, alerts, and remotes) that have structural or content differences to the source template.
<N> deployed groups with no structural/content differences	Displays the deployed groups that have no structural or content differences to the source template. Groups with no deployment differences are displayed collapsed.

GUI Element	Description
Group Name	<p>Displays the name of the deployed group and all its objects—subgroups, monitors, alerts, alert actions, and remote servers. Structural differences in the objects are displayed in the group tree hierarchy with the following text and color coding:</p> <ul style="list-style-type: none"> ▶ Added. Indicates a new object to be added to the deployed group. The object is displayed in green. ▶ Does not exist in template (only available when the Enable Delete on Update option is not selected in the Select Groups page). Indicates an object that does not exist in the source template. The object is displayed in blue. ▶ Removed (only available when the Enable Delete on Update option is selected in the Select Groups page). Indicates an object to be deleted from the deployed group. The object is displayed in red. ▶ Unused. Indicates that the template remote server is not being used. An unused remote server is displayed in gray. <p>When there are no differences in an object, the object is displayed in black.</p>
Content Differences	<p>Click the View Differences link to open the Content Changes dialog box and view differences in the property level for the deployed group or object. This link is displayed only for objects that contain content differences in properties, thresholds, and any other non-structural differences. For details on the user interface, see “Content Changes Dialog Box” on page 1244.</p> <p>Template remote servers that have been deployed are displayed in the Microsoft Windows Remote Servers or UNIX Remote Servers section. If a remote server already exists in Microsoft Windows/UNIX Remote Preferences, it is not deployed again when the template is deployed.</p>

Content Changes Dialog Box

Description	Use the Content Changes dialog box to view a list of all properties of the selected object that will be updated, the values that will be changed, and the property action status.
Included in Tasks	“Publish Template Updates to Related Group Deployments” on page 1218
Wizard Map	The Publish Template Changes wizard contains: Publish Template Changes Wizard - Select Deployed Groups Page > Review Compliancy Page > (Content Changes Dialog Box) > (Modify Variables Page) > Publish Results Summary Page > Publish Template Changes Summary Report
Useful Links	“Updating Template Deployments” on page 1206

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Type	The selected object type (Group, Monitor, Alert, Alert Action, Remote).
Name	The name of the selected object.
Property Name	The name of the property affected by publishing the change.
Current Value	The existing property value in the deployed group. This value is empty if the property is going to be added to the deployed group. Note: Existing password properties are displayed encrypted.

GUI Element	Description
Replacement Value	<p>The property value in the template. This value is empty if the property is going to be deleted from the deployed group.</p> <p>Note:</p> <ul style="list-style-type: none">▶ Replacement password properties are displayed encrypted.▶ If you make changes to the Depends On property in a template monitor, the full path of the template monitor to which there is a dependence is displayed (for example, SiteScope\etc\template\group\CPU).
Property Action Status	<p>The status of the action (Modified, Added, Deleted, Ignored). Ignored status is used for baseline monitors if there are no changes to the baseline thresholds.</p>

Modify Variables Page

Description	Use the Modify Variables page to add values for new variables in the deployed group. You can also edit existing variable values.
Included in Tasks	“Publish Template Updates to Related Group Deployments” on page 1218
Wizard Map	The Publish Template Changes wizard contains: Publish Template Changes Wizard - Select Deployed Groups Page > Review Compliancy Page > (Content Changes Dialog Box) > (Modify Variables Page) > Publish Results Summary Page > Publish Template Changes Summary Report
Useful Links	“Updating Template Deployments” on page 1206


The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Group Name	The name of the deployed group associated with the template. Note: You can expand groups with variable values already filled, and modify the variables as required. You cannot expand groups that do not contain variables.
Variable Name	The name of a new or existing variable in the deployed group.
Variable Value	Type a value for new variables added to the deployed group. A red asterisk indicates that a variable value is mandatory. You can also edit existing variable values. Note: <ul style="list-style-type: none"> ▶ The variable value for the remote server is read only and cannot be changed. ▶ Hypertext tags in a variable string cause the string to be truncated and it is incorrectly displayed in the Variable Value box (part of the string is displayed in the text label).

Publish Results Summary Page

Description	Displays a summary of the published template updates.
Included in Tasks	“Publish Template Updates to Related Group Deployments” on page 1218
Wizard Map	The Publish Template Changes wizard contains: Publish Template Changes Wizard - Select Deployed Groups Page > Review Compliancy Page > (Content Changes Dialog Box) > (Modify Variables Page) > Publish Results Summary Page > Publish Template Changes Summary Report
Useful Links	“Updating Template Deployments” on page 1206

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click to export the results of publishing for each root group to a PDF file. For details, see “Publish Template Changes Summary Report” on page 1248.
Deployed groups that were not updated	Displays the group name and the reason that the group failed to update in the Reason column. Note: For changes to be published, all changes in the root group hierarchy must succeed. If any changes to a group object fail, all changes to that group are rolled back.

Publish Template Changes Summary Report

The following is an example of the Publish Template Changes Summary Report.

Publish Template Changes Summary Report				
Total number of deployed groups for publishing changes: 1				
Total number of deployed groups that were not updated: 0				
Total number of deployed groups that were successfully updated: 1				
Successfully Changed Deployed Groups				
Deployed Root Group: SiteScope\docs\Windows monitors for doors				
Type	Name	Reason	Message	
Monitor	SiteScope\docs\Windows monitors for doors\Memory on doors	Unchanged		
Alert	SiteScope\docs\Windows monitors for doors\Memory on doors\Memory alert	Successfully added		
Alert Action	Memory E-Mail Alert	Successfully added		
Monitor	SiteScope\docs\Windows monitors for doors\Cpu monitor on doors	Successfully modified		
	Property Name	Deployment Value (previous)	Template Value (current)	Action on Property Value
	Depends On		SiteScope\docs\Windows basic template\Windows monitors for doors\ping test	Successfully added
	Depends Condition	good	available	Successfully modified
Monitor	SiteScope\docs\Windows monitors for doors\ping test	Successfully added		
Remote Server	doors	Unchanged		

Description	Displays information about the template changes published to the deployed groups. It also displays information for group objects that failed to update. Results are at the object level (Group, Monitor, Alert, Alert Action, Remote Server).
Included in Tasks	“Publish Template Updates to Related Group Deployments” on page 1218

Wizard Map	The Publish Template Changes wizard contains: Publish Template Changes Wizard - Select Deployed Groups Page > Review Compliancy Page > (Content Changes Dialog Box) > (Modify Variables Page) > Publish Results Summary Page > Publish Template Changes Summary Report
Useful Links	“Updating Template Deployments” on page 1206

Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Report summary>	The report summary shows the total number of root groups selected for publishing changes, including the number of groups that were successfully and unsuccessfully changed.
Deployed Root Group	The name of the deployed group and all group objects that were successfully/unsuccessfully updated with the template changes. The deployed groups that were not updated are displayed first. Note: For changes to be published, all changes in the root group hierarchy must succeed. If any changes to a group object fail, all changes to that group are rolled back.
Type	The object type (Group, Monitor, Alert, Alert Action, Remote Server)
Name	The name of the object and its path.
Status	The publish status for the object (Successfully added, Successfully modified, Successfully deleted, Failed to add, Failed to modify, Failed to delete, Unchanged).

GUI Element	Description
Message	For deployed group objects that were not updated by the template changes, the reason for the failure to publish the changes.
<Property details>	<p>For deployed group objects that had content changes:</p> <ul style="list-style-type: none"> ▶ Property Name. The name of the property that was updated. ▶ Deployment Value (previous). The previous property value in the deployed group. This value is empty for a property that was added to the deployed group. Previous password variables are displayed encrypted. ▶ Template Value (current). The replacement property value in the deployed group. This is the current property value in the template. This value is empty if the property was deleted from the deployed group. Replacement password variables are displayed decrypted. ▶ Action on Property Value. The type of change made to the property value (Modified, Added, Deleted).

Generate Auto Deployment XML

Description	<p>Enables you to create an XML file to use for automatically deploying the templates in the highlighted template container. Once you generate the XML file, you can edit the file and use it to deploy the templates from the file directory and not in the SiteScope user interface.</p> <p>To access: Right-click the template container in the monitor tree for which you want to create an auto deploy XML file, and click Generate XML.</p>
Included in Tasks	“Deploy a Monitoring Structure Using an XML File” on page 1262
Useful Links	“Auto Template Deployment Overview” on page 1254

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
Generated File Name	Type the name of the XML file to create. This is the file you can edit and use to automatically deploy the templates in this template container.
File Path	<p>The location where the XML file is saved. Accept the default location, or enter a different location.</p> <p>Default value: <SiteScope_install_path>\SiteScope\persistence\autodeployment\drafts</p> <p>Note: If an XML file has been generated previously using the same Generated File Name and File Path, the previously saved XML file is not overwritten. The previous file is renamed with the following addition _bck<number of backup>. For example, if you enter CPUtemplate as the Generated File Name and accept the default location, the existing file in the default folder becomes CPUtemplate.xml_bck1 and the current XML file being generated is saved as CPUtemplate.xml.</p>
Templates to Generate XML	Select the templates for which to create the XML file. The XML file's contents are based on the objects in the template you select. For each template selected, the generated XML includes a separate deploy section.

33

Auto Template Deployment

This chapter includes the main concepts, tasks, and reference information for SiteScope auto template deployment.

This chapter includes:

Concepts

- ▶ Auto Template Deployment Overview on page 1254
- ▶ Creating and Working with the XML File on page 1254
- ▶ XML File Example and Variables on page 1255
- ▶ XML Validator on page 1259
- ▶ Publishing Template Changes Using the XML on page 1259
- ▶ Deployment Results on page 1262

Tasks

- ▶ Deploy a Monitoring Structure Using an XML File on page 1262
- ▶ Encrypt Text on page 1266
- ▶ Update a Deployment on page 1267

Reference

- ▶ XML Tag Reference on page 1269

Troubleshooting and Limitations on page 1272

Auto Template Deployment Overview

SiteScope enables you to automatically deploy a SiteScope template or solution template using an XML file external to the SiteScope user interface. The XML file deploys the objects defined in the template, which must include a parent group and can include subgroups, monitors, a remote server, alerts, and variable definitions. You can edit the XML file to assign variable definitions for mandatory, global, and instance variables.

For details on creating templates, see “SiteScope Templates Overview” on page 1190. For details on working with solution templates, see “Solution Templates Overview” on page 1273.

You can also use the auto template deployment to publish template changes to deployed groups using the same functionality as the Publish Template Changes Wizard. For details, see “Updating Template Deployments” on page 1206.

Auto template deployment is an alternative to using the user interface to deploy templates and publish template changes to deployed groups. It is more suitable than the user interface for working with scripts and deploying onto multiple SiteScopes.

Creating and Working with the XML File

Use one of the following options to create the XML file:

- ▶ Generate and edit your XML in any tool that supports text. The file must be based on the XSD file supplied in the SiteScope file directory. The XSD file is a basic XML file which already includes the appropriate tags, elements, and attributes for creating your own version of the deployment XML.
- ▶ Generate the deployment XML file using the SiteScope interface from a template container or solution template. Each template container and solution template includes the option to generate this auto template deployment XML file. For details, see “Generate Auto Deployment XML” on page 1250.

The XML you use, whether generated from the template or solution template or generated manually, must be a valid XML and match the ATD schema (XSD). You can use the dedicated tool to validate your XML file.

The XML file is dependent on the target SiteScope having the relevant template or solution template in its monitor tree. You deploy the template or solution template by copying the XML file into the persistency folder of the target SiteScope with the relevant template or solution template. You can group several deployments into a single XML file.

XML File Example and Variables

For a reference detailing all the XML tags, elements, and attributes included in the auto template deployment file, see “XML Tag Reference” on page 1269.

Each auto template deployment XML must begin with the following declarations:

- `<?xml version="1.0" encoding="UTF-8" ?>` This states that this is an XML with UTF-8 character encoding.
- `<sitescope:sitescopeRoot ...>` This is the schema declarations. Despite the URLs mentioned, this will not try to connect to any location outside of your SiteScope at any time.

Each section of the XML file begins with one of the following tags with the instruction to perform one of the following options:

- `<sitescope:templateDeploy>` Deploys a template or solution template. You can have multiple instances within the same XML file.
- `<sitescope:templateDeployUpdate>` Publishes changes to an existing deployment.

Within each action, you must specify the following:

- `<deploy:fullPathtoTemplate>` The path to the template within the SiteScope tree in the user interface, not including the SiteScope root node. In the XML file example, this value is `Templates/Windows`.

- ▶ **<deploy:fullPathToDestinationGroup>** The path, within the SiteScope tree, to the target group upon which the action is performed. For example, in the XML file example, any template group objects are created as subgroups within the following group SiteScope/Windows_Monitors.
 - ▶ SiteScope/Windows_Monitors/Minor_monitors in the second instance of the deployment.

XML File Example

Here is an example of the auto template deployment XML file. This file was generated from the user interface.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--SiteScope deployment descriptor-->
<sitescope:sitescopeRoot xmlns:sitescope="./sitescope" xmlns:deploy="./deploy"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="./sitescope
../schemas/sitescope.xsd ">
  <!--To deploy use "templateDeployment", to update an existing deployment use
templateDeploymentUpdate (this element can have the attribute enableDeleteOnUpdate with values of
yes/no)-->
    <sitescope:templateDeployment>
      <!--Path to source template in SiteScope tree (not including the root node)-->
      <deploy:fullPathToTemplate>Templates/Windows</deploy:fullPathToTemplate>
      <!--Path to destination group in SiteScope tree (not including the root node). New group
will be created if need be-->
      <deploy:fullPathToDestinationGroup>
SiteScope/Windows_Monitors</deploy:fullPathToDestinationGroup>
      <!--Mandatory variables names-->
      <deploy:mandatoryFields>group frequency</deploy:mandatoryFields>
      <!--Global values for variables in current template-->
      <deploy:globalVariables>
        <deploy:variables encrypted="yes" name="password" value="(sisp)d5JLOSwaVfE="/>
        <deploy:variables encrypted="no" name="user" value="admin"/>
        <deploy:variables encrypted="no" name="frequency" value="600"/>
      </deploy:globalVariables>
      <!--Add here local variables for a deploy instance (overrides global variables with same
name)-->
      <deploy:templateInstanceDeployVariable>
        <deploy:variables encrypted="no" name="group" value="Critical_monitors"/>
        <deploy:variables encrypted="no" name="frequency" value="600"/>
      </deploy:templateInstanceDeployVariable>
      <deploy:templateInstanceDeployVariable>
        <deploy:variables encrypted="no" name="group" value="Minor_monitors"/>
        <deploy:variables encrypted="no" name="frequency" value="6000"/>
      </deploy:templateInstanceDeployVariable>
    </sitescope:templateDeployment>
  </sitescope:sitescopeRoot>
```


Variables

Once the template and destination have been specified, the next section of the XML file deals with the template variables and values. The XML file gives you the flexibility of defining variables and their values, declaring mandatory variables, and determining if their corresponding values should be applied globally across the deployment or per instance.

If you generated the XML file from the user interface and if a variable has a defined value, that value is assigned to the variable in the XML file.

Mandatory Variables

A declaration of any mandatory variables in the template appears in the `<deploy:mandatoryFields>` tag. If a variable is declared mandatory, a corresponding value for the variable must be defined in the in the file.

If you generated the XML from the user interface and if the **Mandatory** option was selected when creating or editing a variable, that variable appears in the `<deploy:mandatoryFields>` tag. You can also manually add a variable name to this list to declare it mandatory.

In the file example above, `group` and `frequency` have been defined as mandatory variables. Values for these variables must appear within the `<deploy:variables>` tags for either the `<deploy:globalVariables>` or the `<deploy:templateInstanceDeployVariables>`.

Global versus Instance Variables

The optional `<deploy:globalVariables>` tag includes the default global template variables for the deployment. Defining global template variables is optional. When you define a global template variable, you can overwrite the variable's value by identifying a different variable value in the deployment instance area of the file (`<templateInstanceDeployVariables>` tag). Global variable values can be overwritten with a different value in each deployment instance.

Multiple instances of a template that are deployed into the same location onto the same SiteScope, as seen in the XML file example, must include a variable for the group name. Group name must be made a mandatory variable and given a different value in each deployment instance. The group template object must have the same variable defined as its value. The template could include other groups whose name value is not a variable and those groups would be deployed once.

In the XML file example above, there are two instances of the deployment, so a variable called `group` has been defined as mandatory and a different value has been given to it in each instance deployment (`Critical_monitors` and `Minor_monitors`). This results in two groups created under the group object of the template with the same monitor objects.

The following groups would result from the XML file example being deployed:

- ▶ `SiteScope/Windows_Monitors/Critical_monitors` in the first instance of the deployment.
 - ▶ Included in this group would be any monitors and alerts defined in the template. Any of the template monitor objects whose frequency value was defined as the variable `frequency` would have a value of 600 or every 10 minutes.
- ▶ `SiteScope/Windows_Monitors/Minor_monitors` in the second instance of the deployment.
 - ▶ Included in this group would be any monitors and alerts defined in the template. Any of the template monitor objects whose frequency value was defined as the variable `frequency` would have a value of 6000 or every hour.

Note: If you have any system variables defined in a template (those defined by `$$` and not `%%`), they are treated as normal variables in the auto template deployment XML file. The same limitations that apply to using system variables in templates apply to using them in the XML file.

XML Validator

The XML validator is a utility that validates the XML file against the schemas used by the auto template deployment. It does not validate the SiteScope deployment itself. The path to the validator file is:

- ▶ **<SiteScope root directory>/tools/AutoDeployment/validate_template_xml.bat** for Windows
- ▶ **<SiteScope root directory>/tools/AutoDeployment/validate_template_xml.sh** for UNIX

This utility checks the structure of the XML against the XSD files to ensure that the contents of the file are valid XML and correspond to the XSD. It also validates that there have been values defined for all mandatory variables. The values can be defined either as global variables or deployment instance variables. If the validation fails, the reason for the failure is printed to screen.

Publishing Template Changes Using the XML

You can also use the auto template deployment XML to publish template changes to update the values or structure of a deployed group. If the group's **Source Template** field is identified as the same template that the XML is referencing, you can update the values and objects of the group using the auto template deployment XML.

The XML uses the same functionality as the Publish Template Changes Wizard but without having to access the user interface. In the XML file, you can identify values for variables to use for publishing the changes in the template. For details on the wizard and the template update feature, see “Updating Template Deployments” on page 1206.

You can use auto template deployment to publish the changes made to a template onto the template's deployed groups in the same way you use the XML to create a group deployment. Once the template has been modified, you create the XML and copy/paste the edited XML into the persistency folder of the target SiteScope machines.

This section includes the following topics:

- “Update Deployment XML Tag Details” on page 1260
- “Template Update Report” on page 1261

Update Deployment XML Tag Details

The XML file for updating the values or objects of a deployed group must use the `<sitescope:templateDeploymentUpdate>` tag (and not the `<sitescope:templateDeployment>` tag used for deploying the template). For details on the elements and attributes to use in the XML file, see “XML Tag Reference” on page 1269.

Within the `<sitescope:templateDeploymentUpdate>` tag, you can select to give the `enableDeleteOnUpdate` attribute a value of **yes** to ensure that any objects within the deployed groups that do not appear in the template referenced by the auto template deployment XML are deleted when updating the deployment with the XML file. Enter a value of **no** to ensure that all objects within the group are retained, even if they do not appear in the template referenced by the XML file, after the updating the deployment. For details on this option in the Publish Template Changes Wizard, see “Enable Delete on Update” on page 1241.

To successfully perform the update, you must define the target SiteScope group name of the deployed group as the value of the `deploy:fullPathToDestinationGroup` tag. The `fullPathToDestination` must end with the root group of the deployment, the equivalent of the template's root group. Each deployment section updates one group so if you have multiple groups, you must define separate deployment update sections for each and define the group name for each.

Template Update Report

After performing the auto template deployment update, a report is available in XML format. The report file is named with the name of the XML file along with a time stamp and the string **_reports**. These reports are available in the following location: **<SiteScope root directory>\persistence\autodeployment\reports**.

The report is in XML format and includes the following tags at the beginning:

- **totalNumberOfDeployments**
- **totalNumberOfFailedDeployments**
- **totalNumberOfSuccessDeployments**

The **<publishChangesSummaryPage>** section of the XML appears for each deployment instance listing the details of what has been updated. Unsuccessfully changed deployments are specified first in the file.

This file is an XML version of the .pdf file created by the Publish Template Changes Wizard if using the SiteScope user interface to update deployed groups. For details on the report, see “Publish Template Changes Summary Report” on page 1248.

Deployment Results

When you copy the XML file, for both deploying and updating, into the persistency folder of the target SiteScope, the file is copied into one of two directories as follows:

- ▶ **<SiteScope root directory>\persistency\autodeployment\successHistory** directory includes those XML files that deployed or updated successfully all instances of the deployed group.
- ▶ **<SiteScope root directory>\persistency\autodeployment\failHistory** directory includes those XML files that failed to deploy or update any instance of the deployed group. If even one instance failed and all the others succeeded, the XML is published to this folder.

The XML file name is changed to include an underscore and a timestamp added to the original name of the XML file. For example the XML file named CPUgroups.XML that succeeded in deploying all its groups and instances is saved to the **<SiteScope root directory>\persistency\autodeployment\successHistory** directory and is now named CPUgroups_1203951216931.xml.

Deploy a Monitoring Structure Using an XML File

This task describes how to perform an auto template deployment. You can follow the same steps for deploying a Solution Template.

This task includes the following steps:

- ▶ “Prerequisites” on page 1263
- ▶ “Create the XML File” on page 1263
- ▶ “Edit XML File” on page 1264
- ▶ “Encrypt Fields Such as Passwords (Optional Step)” on page 1264
- ▶ “Validate the XML File” on page 1264
- ▶ “Copy the Validated XML to the SiteScope Server Machines” on page 1265
- ▶ “Check If Deployment Was Successful” on page 1265

1 Prerequisites

Each SiteScope into which you want to automatically deploy a template must include the template within a template container. The template must have a group object at the top level. All other objects must be created within that group. The template can contain subgroups, monitors, alerts, one remote server, and variables.

If you are working with multiple SiteScopes:

- ▶ You can create the template in one SiteScope and export it to other SiteScopes using the Export/Import options in the Template containers context menu. For details on how to do this, see “Export Template Page” on page 1238 and “Import Template Page” on page 1239.
- ▶ If you are working in HP Business Availability Center, you can copy templates from one SiteScope to another using the Sync SiteScope Wizard in System Availability Management Admin. For details on the wizard interface, see “Sync SiteScopes Wizard - Select Source and Targets Page” on page 71.

2 Create the XML File

You can create the XML file using one of these options:

- ▶ Right-click the template container and select **Generate XML File** in the context menu. When deploying solution templates, this option appears at the template level. For details on this user interface option, see “Generate Auto Deployment XML” on page 1250.
- ▶ Create the XML file using a dedicated XML application. The file must be a valid XML file and based on the XSD files located in the following directories:
 - ▶ `<SiteScope root directory>/conf/xsds/deploy.xsd`
 - ▶ `<SiteScope root directory>/conf/xsds/sitescope.xsd`

3 Edit XML File

You must edit the XML file to enter the values necessary for deployment. For details on editing the file and a sample of the file, see “XML File Example and Variables” on page 1255.

For details on the XML file’s tags, see “XML Tag Reference” on page 1269.

Note: If the XML is generated from the user interface, mandatory variable fields are generated based on the templates mandatory variables. If you create the XML file, and there are fields that are mandatory for successful deployment, you must ensure that these fields have been assigned values before deploying the XML.

4 Encrypt Fields Such as Passwords (Optional Step)

For deploying templates that include fields that you do not want to appear in viewable text, use the encryption tool and follow the steps in the procedure for encrypting text. For details on this task, see “Encrypt Text” on page 1266.

5 Validate the XML File

It is recommended that you validate the XML file before it is deployed.

Use the validation tools located in the following directories:

- For Windows: <SiteScope root directory>/tools/AutoDeployment/validate_template_xml.bat
- For UNIX: <SiteScope root directory>/tools/AutoDeployment/validate_template_xml.sh

For details on this topic, see “XML Validator” on page 1259.

6 Copy the Validated XML to the SiteScope Server Machines

Copy the XML file into the `\persistence\autodeployment` directory on each SiteScope machine where you want to deploy the templates in the XML.

The templates are automatically deployed every two minutes by default. You can change the frequency in Infrastructure Setting Preferences in the following field: **Auto Deployment Check Frequency** (Property name: `_autoDeploymentCheckFrequency`).

Note: If the XML file does not pass validation when attempting to deploy, the deployment fails. It is recommended to validate the XML file before copying onto the persistence directories of the SiteScope server machines.

7 Check If Deployment Was Successful

You can check if the deployment was successful by searching in the target SiteScope's `<SiteScope root directory>\persistence\autodeployment` directory to see if the XML was copied into the `successHistory` subdirectory or the `failHistory` subdirectory.

For details on this topic, see “Deployment Results” on page 1262.

You can also check the SiteScope's Error Log.

Encrypt Text

This task describes how to encrypt text for a field that should not appear in viewable text, for example a password. This tool encrypts the field only in the XML; the templates themselves control the encryption of variables in the persistency directory.

To encrypt text for use in the deployment XML:

- 1 Run the following batch file:
 - For Windows: `<SiteScope root directory>/tools/AutoDeployment/encrypt_password.bat`
 - For UNIX: `<SiteScope root directory>/tools/AutoDeployment/encrypt_password.sh`
- 2 Open a command prompt window.
 - In Windows, drag and drop the file into your command prompt window.
 - In UNIX, you must run the .sh file from its directory.
- 3 Enter space and the password value (for example Mypassword). Click ENTER.
- 4 Use the returned string as a value for the encrypted variable in the XML file. You must change the value of the attribute **encrypted** to **yes** and the **value** of the variable attribute to the returned string.

For example, the following value was generated by the encryption tool:

```
<deploy:variables encrypted="yes" name="password" value="(sisp)d5JLOSwaVfE="/>
```

Update a Deployment

This task describes how to use the auto template deployment XML to update an existing, deployed group. You can update the structure of the deployment if the template was changed or update object properties by giving new values to the variables that are declared in the template for those properties.

The task follows the same steps as the task to deploy a template with the exceptions and additional information listed in the steps here. For details on the deployment task, see “Deploy a Monitoring Structure Using an XML File” on page 1262.

This task includes the following steps:

- “Prerequisites” on page 1267
- “Create and Edit the XML File to Update Objects and Values” on page 1267
- “Copy the Publish Template Update XML to the Target SiteScopes” on page 1268
- “Encrypt Text Such as a Password (Optional Step)” on page 1268
- “Validate the Publish Template Update XML” on page 1268
- “Results Report” on page 1268

1 Prerequisites

The **Source Template** field of the deployed groups that you want to update must be identical to the template in the XML deployment update file. This is in addition to the updated template existing in the target SiteScope.

2 Create and Edit the XML File to Update Objects and Values

When working with the XML file, you must do the following:

- Use the `<templateDeploymentUpdate>` tag instead of the `<templateDeployment>` tag.
- Enter a **yes** or **no** value for the **enableDeleteOnUpdate** attribute of the `<templateDeploymentUpdate>` tag.

- ▶ Define the **deploy:fullPathToDestinationGroup** tag with the group name to be updated as the value for this tag.

For details on these tags and the update XML file, see “Update Deployment XML Tag Details” on page 1260.

3 Copy the Publish Template Update XML to the Target SiteScopes

Copy the publish template update XML to the target SiteScope’s **persistence** directory as you would when deploying the auto template deployment XML file.

4 Encrypt Text Such as a Password (Optional Step)

For details on performing this task, see “Encrypt Text” on page 1266.

5 Validate the Publish Template Update XML

Use the validator tool to validate the edited XML file as you would when deploying the auto template deployment XML file.

6 Results Report

After deploying the update auto template deployment XML, a results report file is created in XML format. These reports are available in the following location: **<SiteScope root directory>\persistence\autodeployment\reports**.

For details on the report, see “Template Update Report” on page 1261.

XML Tag Reference

Following are tables listing all the elements and attributes that are used in the auto template deployment XML files.

Elements Table

Elements	Description
sitescope:sitescopeRoot	This must be the first tag in the XML file giving the instruction to create the deployment, the version of XML used, and the location of the XSD file. Note: This is the first element in all XML files related to SiteScope.
sitescope:template Deployment	This tag enables the deployment of the template or solution template, creating new group structures in the target SiteScope. This is the default tag used in the XML file when generated from the user interface.
sitescope:template DeploymentUpdate	This tag enables publishing the changes of a template that has been updated. These changes can be applied to the monitoring structure of a group whose Source Template field matches the template identified in the XML. The XML file also enables you to update the values of the variables used in the template. For example, if you want to add alerts or an additional monitor to an existing group that was created by a template, you can modify the template and deploy it using this tag.
deploy:fullPathToTemplate	This tag gives the full path, within the SiteScope tree, of the template or solution template to be deployed. Syntax: <template container name>/<template name>

Elements	Description
deploy:fullPathToDestinationGroup	This tag gives the full path location within the SiteScope tree of the group name where the deployed monitoring structure is to be created. If this tag has no value, the deployment is created at the SiteScope node level.
deploy:mandatoryFields	The values within this tag are those variables that were selected as mandatory fields when the template was created. If there are any values appearing within this tag, they must be given a value in the <deploy:globalVariables> tag for global variables or the <deploy:variables> tag for other variables. If there are no corresponding values for these mandatory fields, the XML fails validation.
deploy:globalVariables	This tag marks the section of the file that includes the variables that are deployed across the entire selected template. Includes attributes. For details, see “Attributes Table” on page 1271.
deploy:templateInstanceDeployVariable	This tag marks the section of the file that includes the variables that are deployed per instance of the selected template. If the same variable appears in the <deploy:globalVariables> , the instance variable value overrides the global variable value only for the instance in which it appears. All other instances have the value entered in the <deploy:globalVariables> section. Includes attributes. For details, see “Attributes Table” on page 1271.
deploy:variables	This tag defines the variables and their values. Includes attributes. For details, see “Attributes Table” on page 1271.

Attributes Table

Parent Element	Attribute	Description
templateDeploymentUpdate	enableDeleteOnUpdate	<p>Indicates whether any instances of objects appearing in a deployment of a template should be deleted when not appearing in the XML file used for updating the structure of a deployment.</p> <p>Possible values: yes, no</p> <p>For details on this option, see “Enable Delete on Update” on page 1241.</p>
deploy:globalVariables	encrypted	<p>Indicates whether the value of the variable’s field is encrypted or not.</p> <p>Possible values: yes, no</p> <p>To encrypt a value, use the encryption tool to provide the value for the variable. For details, see “Encrypt Text” on page 1266.</p>
	name	The name of the variable.
	value	The value of the variable.
deploy:variables	encrypted	<p>Indicates whether the value of the variable’s field is encrypted or not.</p> <p>Possible values: yes, no</p> <p>To encrypt a value, use the encryption tool to provide the value for the variable. For details, see “Encrypt Text” on page 1266.</p>
	name	The name of the variable.
	value	The value of the variable.

Troubleshooting and Limitations

All notes, limitations, and troubleshooting issues that apply to SiteScope templates, solution templates, and the Publish Template Changes Wizard also apply to the functionality of the auto template deployment.

I18N Users

- ▶ Do not edit the XML file using Notepad. The file cannot be parsed because Notepad adds an extra character to the beginning of the file. This character is not visible but prevents the file from being parsed when not in English. Use Wordpad or an XML editor instead.
- ▶ If the path to the SiteScope root directory includes non-English characters, the validation tool cannot be used to validate the XML before it is copied to the SiteScope's persistency directory. This means that there is no validation that the XML follows the XSD or that mandatory fields have values.

Solution Templates

You cannot perform auto template deployment for the following Solution Templates:

- ▶ JBoss Application Server 4.x
- ▶ WebLogic Application Server
- ▶ WebSphere 5.x Application Server
- ▶ WebSphere 6.x Application Server

This is because the variables in these solution templates are dynamically created and cannot be given a value in the XML file.

34

SiteScope Solution Templates

This chapter includes the main concepts, tasks, and reference information for SiteScope solution templates.

This chapter includes:

Concepts

- ▶ Solution Templates Overview on page 1273

Tasks

- ▶ Deploy a SiteScope Solution Template – Workflow on page 1276
- ▶ Troubleshooting and Limitations on page 1278

Solution Templates Overview

SiteScope solution templates are preconfigured monitor set templates designed to monitor popular enterprise applications and network systems. Using solution templates, you can rapidly deploy a combination of standard SiteScope monitor types and solution-specific monitors with settings that are optimized for monitoring the availability, performance, and health of the target application or system. For example, the solutions for Microsoft Exchange monitoring include performance counter, event log, and Exchange application specific monitor types.

Deploying the solution creates a new monitor group container in which the individual solution monitors are added. You must deploy one solution template for each server in your environment.

The following table lists solution templates available for SiteScope. For more information about each solution and the solution specific monitor types, see the chapter for the specific solution template.

Solution Name	Description
Active Directory Solution Template	Monitors the performance and efficiency of Microsoft domain controllers.
AIX Host Solution Templates	Monitors performance, availability, and health for AIX host machines.
JBoss Application Server Solution Template	Monitors performance, availability, and health for JBoss environments.
Linux Host Solution Templates	Monitors performance, availability, and health for Linux host machines.
Microsoft Exchange Solution Templates	Includes individual solution options for monitoring application health, message flow, and usage statistics for Microsoft Exchange 5.5, 2000, 2003, and 2007 servers.
Microsoft IIS Solution Template	Monitors performance, availability, and health for IIS 6.0 environments.
Microsoft SQL Server Solution Template	Monitors performance, availability, and usage statistics for Microsoft SQL Server 2005.
Microsoft Windows Host Solution Template	Monitors performance, availability, and health for Microsoft Windows 2000, Windows XP, and Windows Server 2003 host machines.
.NET Solution Templates	Monitors performance, availability, and health of .NET applications and environments on Windows 2000, Windows XP, and Windows Server 2003.
Oracle Database Solution Template	Monitors performance, availability, and usage statistics for Oracle 9i and 10g databases.
SAP Solution Templates	Monitors performance, availability, and usage statistics for SAP system components.
Siebel Solution Templates	Monitors performance, availability, and usage statistics for Siebel Application Server installed on Windows and UNIX operating systems.

Solution Name	Description
Solaris Host Solution Templates	Monitors performance, availability, and health for Solaris host machines.
WebLogic Solution Template	Monitors performance, availability, and usage statistics for BEA WebLogic application servers.
WebSphere Solution Template	Monitors performance, availability, and usage statistics for IBM WebSphere Server 5.x application servers.

Note:

- ▶ Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
 - ▶ Once some solution templates are deployed, the relevant monitors may be defined with a BAC reporting level of **Do not report to BAC**. Therefore after deploying a solution template, it is recommended that you check the monitors' reporting level. If you want to change the reporting level for the deployed monitors, you can use the Global Search and Replace wizard to update the reporting level option.
 - ▶ Solution templates do not configure any automated alerts or reports for the monitors created. You may create and associate one or more alert definitions or reports to the monitors or monitor groups created by solution templates.
-

Deploy a SiteScope Solution Template – Workflow

This task describes the steps involved in deploying a solution template. Deploy a solution template for each server in your environment.

This task includes the following steps:

- “Prerequisites” on page 1276
- “Enter the Solution Template License” on page 1276
- “Create/Select a Monitor Group” on page 1276
- “Copy and Paste a Solution Template and Input Variable Values” on page 1277
- “Configure Alerts and Reports” on page 1277
- “Results” on page 1277

1 Prerequisites

You must have the applicable SiteScope option license to use the Solution Template. Contact your HP sales representative for more information about Solution licensing.

2 Enter the Solution Template License

Enter the license into the General Preferences page. For details on the user interface, see “SiteScope General Preferences User Interface” on page 248.

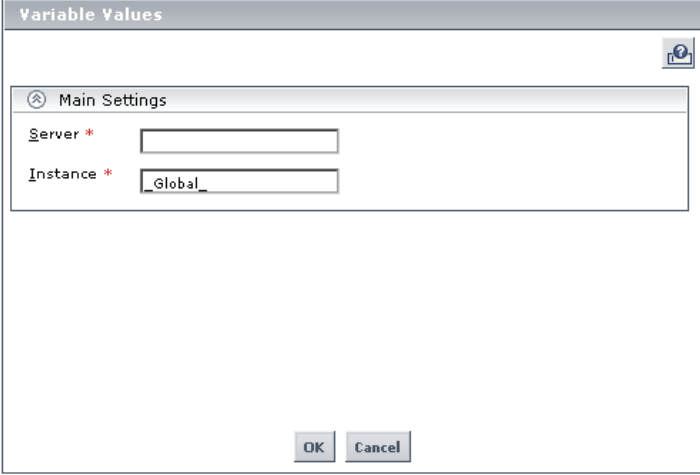
3 Create/Select a Monitor Group

Create or select a monitor group into which you want to deploy the solution monitors. For details on creating a monitor group, see “Manage a Group – Workflow” on page 460.

4 Copy and Paste a Solution Template and Input Variable Values

Expand the Solution Templates container and copy a solution template into the SiteScope or a monitor group container. Complete the items on the Variable Values page for the selected solution template. For details on the user interface, see the Variable Values page for the specific solution template.

Example - .NET CLR Data Variable Values Page



The screenshot shows a dialog box titled "Variable Values". Inside, there is a section titled "Main Settings" with a collapse icon. Below this section are two input fields: "Server *" and "Instance *". The "Instance *" field contains the text "_Global_". At the bottom of the dialog are "OK" and "Cancel" buttons.

5 Configure Alerts and Reports

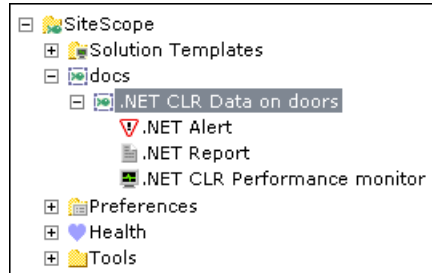
Configure alerts and reports for the newly created solution monitors. For details on configuring alerts, see “Configure an Alert” on page 1409. For details on configuring reports, see “Create a Report” on page 1444.

6 Results

Deploying the solution creates a new monitor group container in which the individual solution monitors are added. The monitor group container is assigned a name in the format <Solution Template name> on <server_name> where **server_name** is the server selected from the **Server** box. If some of the monitors failed to deploy, a message is shown listing the names of the monitors along with messages describing the error.

You can view, edit, and delete these monitors in the same way as any other monitors in SiteScope.

Example



Troubleshooting and Limitations

There are times when, if SiteScope is not running properly, it is advisable to delete the contents of SiteScope's persistency directory located in **<SiteScope root directory>\persistency**. The installed solution sets are located in this directory and if its contents are deleted, the solution sets no longer appear in the monitor tree and cannot be used. To reactivate the solution sets, you must copy the install files back into the persistency directory.

To reactivate the solution template files:

- 1** Locate the solution template files in the following directory:
<SiteScope root directory>\export.
- 2** Copy the contents of **<SiteScope root directory>\export** into **<SiteScope root directory>\persistency\import**.
- 3** Check that the solution templates have been reinstalled by locating them in the monitor tree.

35

Active Directory Solution Template

This chapter includes the main concepts, tasks, and reference information for the Active Directory Solution Template.

This chapter includes:

Concepts

- ▶ Active Directory Solution Overview on page 1279

Tasks

- ▶ Deploy the Active Directory Solution Template on page 1281

Reference

- ▶ Active Directory Solution Template User Interface on page 1282

Active Directory Solution Overview

You can use the Active Directory Solution Template to provide monitoring of domain controller performance—services on which Active Directory depends—and distributed Active Directory performance.

The Active Directory Solution Template deploys a set of monitors against a particular Domain Controller. These monitors encompass best practices monitoring for Active Directory. This template includes NT Event Log, Service, LDAP, performance counter and Active Directory Replication monitors.

The Active Directory Solution Templates provide comprehensive monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the Active Directory solution templates. Contact your HP sales representative for more information about Solution licensing.
 - ▶ An in-depth description of the Active Directory Solution is available in the SiteScope Active Directory Best Practices document. This document is part of the SiteScope installation, and can be found at <**SiteScope root directory**>\sisdocs\pdfs\SiteScope_Active_Directory_Best_Practices.pdf. This is a password protected document. The password is provided along with the Active Directory Solution license key from HP.
-

Solution Template Monitors

The Active Directory Solution Template deploys monitors that target the following aspects of Active Directory performance:

- ▶ **Domain controller performance.** This category refers to the low level health of each domain controller in the environment. The Active Directory Solution Template automatically configures monitors for domain controller health.
- ▶ **Dependent services.** Active Directory depends on several key services. Without these services, Active Directory can become unresponsive or fail altogether. The Active Directory Solution Template automatically configures monitors for a list of important services on which Active Directory performance is dependent.

- **Distributed Active Directory performance.** Perhaps the most important aspect and key indicator of Active Directory performance is how fast Active Directory is replicating changes out to all domain controllers. The Active Directory Solution Template automatically configures monitors for monitoring and testing replication of changes and updates.

Note: Some of the monitor types deployed by the solution templates can only be added to SiteScope by using the Active Directory Solution sets. For more information, see the section for the particular monitor types.

Deploy the Active Directory Solution Template

This task describes the steps involved in entering variables for the Active Directory Solution Template.

This task includes the following steps:

- “Deploy the Solution Template” on page 1281
- “Type Variable Values for the Active Directory Solution Template” on page 1281

1 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

2 Type Variable Values for the Active Directory Solution Template

Complete the items on the Variable Values page for the Active Directory Solution Template. For details on configuring the variable values, see “Active Directory Solution Template User Interface” on page 1282.

Active Directory Solution Template User Interface

Description	<p>Enables you to deploy the SiteScope Active Directory solution template.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click an Active Directory solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Included in Tasks	"Deploy a SiteScope Solution Template – Workflow" on page 1276
Useful Links	"Active Directory Solution Template" on page 1279

The following elements are found in the Active Directory Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Logical_Drive	Type in the logical drive that this Domain Controller is using for its database and log files.
Password	Type the password for the user selected above.
Host_Name	Type in the host part of the domain controller's hostname (do not include the fully qualified domain name).
Replicating_Domain_Controllers	Type in a comma separated list of domain controllers that replicate data from the domain controller selected above.

GUI Element	Description
LDAP_Security_Principal	Type the LDAP Security Principal of a Domain Admin account. For Active Directory this is in the format of cn=Domain Admin User,cn=users,dc=yoursite,dc=com.
Global Catalog (AD with Global Catalog ONLY)	If the Domain Controller is a Global Catalog server then check this box.
SERVER_LIST	Choose the Domain Controller that you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server.

36

AIX Host Solution Templates

This chapter includes the main concepts, tasks, and reference information for the AIX Host Solution Template.

This chapter includes:

Concepts

- AIX Host Solution Overview on page 1285

Tasks

- Deploy the AIX Host Solution Template on page 1287

Reference

- AIX Host Solution Configuration Requirements on page 1288
- AIX Host Solution Template User Interface on page 1288

AIX Host Solution Overview

The AIX Host Solution Template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the AIX host. The template supports the versions of AIX that are supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can create a Server-Centric Report which displays data from three different metrics about the server being monitored. It is recommended to use Solution Templates when creating the UNIX Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric Report, see “Generating a Server-Centric Report” on page 416.

The AIX Host Solution Template provides comprehensive AIX operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the AIX Host Solution Template. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the AIX Host Solutions settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at <SiteScope root directory>\sisdocs\pdfs\SiteScope_OS_Best_Practices.pdf. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

Solution Template Monitors

The AIX Host Solution Template deploys monitors that target the following aspects of AIX performance and health:

- ▶ CPU status and utilization details
- ▶ Memory status and utilization details
- ▶ File system status and utilization details

Deploy the AIX Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the AIX Host Solution Template.

Note: The AIX Host Solution Template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Server-Centric Report support.

This task includes the following steps:

- “Configure the AIX Server Environment” on page 1287
- “Deploy the Solution Template” on page 1287
- “Type Variable Values for the AIX Host Solution Template” on page 1287

1 Configure the AIX Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “AIX Host Solution Configuration Requirements” on page 1288.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the AIX Host Solution Template

Complete the items on the Variable Values page for the AIX Solution Template. For details on configuring the variable values, see “AIX Host Solution Template User Interface” on page 1288.

AIX Host Solution Configuration Requirements

Before you can use the AIX Host Solution Template, there are a number of configuration requirements involving the server environment:

- ▶ SiteScope server must be able to connect to the target AIX host.
- ▶ The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test (**Preferences > UNIX Remote Preferences**). For details, see “UNIX Remote Preferences” on page 220.
- ▶ The SiteScope server itself can also be monitoring if it runs a supported AIX operating system.
- ▶ The template supports the AIX versions supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

AIX Host Solution Template User Interface

Description	<p>Enables you to deploy the SiteScope AIX solution template.</p> <p>Use this page to add the server monitor or edit the monitor’s properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click AIX Host, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Included in Tasks	“Deploy a SiteScope Solution Template – Workflow” on page 1276
Useful Links	“AIX Host Solution Templates” on page 1285

The following elements are found in the AIX Host Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
SERVER_LIST	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a UNIX connection profile, see “UNIX Remote Preferences” on page 220.

37

JBoss Application Server Solution Template

This chapter includes the main concepts, tasks, and reference information for the JBoss Application Server Solution Template.

This chapter includes:

Concepts

- ▶ JBoss Application Server Solution Overview on page 1292

Tasks

- ▶ Deploy the JBoss Application Server Solution Template on page 1293

Reference

- ▶ JBoss Solution Configuration Requirements on page 1294
- ▶ JBoss Solution Template User Interface on page 1295

JBoss Application Server Solution Overview

The JBoss Application Server Solution Template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of JBoss application servers. The template supports JBoss Application Server versions 4.0.x and 4.2.x.

The JBoss Application Server Solution Template provides comprehensive JBoss monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the JBoss Application Server solution template. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the JBoss solution is available in the SiteScope JBoss Application Server Best Practices document. This document can be found at <SiteScope root directory>\sisdocs\pdfs**SiteScope_JBoss_Best_Practices.pdf**. This is a password protected document. The password is provided along with the JBoss Application Server solution license key from HP.

Solution Template Monitors

The JBoss Application Server solution template creates a dynamic set of monitors that target the JBoss application server performance and health. The exact monitor set depends on the entities you select during the solution template deployment. For details on the monitors, see the SiteScope JBoss Application Server Best Practices document.

Deploy the JBoss Application Server Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the JBoss Application Server Solution Template.

This task includes the following steps:

- “Configure the JBoss Server Environment” on page 1293
- “Deploy the Solution Template” on page 1293
- “Type Variable Values for the JBoss Application Server Solution Template” on page 1293

1 Configure the JBoss Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “JBoss Solution Configuration Requirements” on page 1294.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the JBoss Application Server Solution Template

Complete the items on the Variable Values page for the JBoss Application Server Solution Template. For details on configuring the variable values, see “JBoss Solution Template User Interface” on page 1295.

JBoss Solution Configuration Requirements

Before you can use the JBoss Application Server solution, there are a number of configuration requirements involving the server environment:

- ▶ You must know the URL for gathering JMX statistics (including the hostname and port of the JMX instance), and the JMX username and password.
- ▶ SiteScope and the target server can run on the same host.
- ▶ The JBoss solution template supports JBoss application servers 4.0.x and 4.2.x only.
- ▶ You must start JBoss in a particular way, so that SiteScope is able to monitor it. For details, see “Starting JBoss” below.

Starting JBoss

To enable SiteScope to monitor JBoss, you should specify the following options for the JBoss JVM:

```
-Dcom.sun.management.jmxremote.port=12345 (any other port can be used of course;
then it must be specified during ST deployment)
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false
-Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServer
BuilderImpl
-Djboss.platform.mbeanserver
-Dcom.sun.management.jmxremote
```

You can perform this using the following batch file:

```
@echo off
set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.port=12345
set JAVA_OPTS=%JAVA_OPTS% -
Dcom.sun.management.jmxremote.authenticate=false
set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.ssl=false
set JAVA_OPTS=%JAVA_OPTS% -
Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServer
BuilderImpl
set JAVA_OPTS=%JAVA_OPTS% -Djboss.platform.mbeanserver
set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote
call run.bat -b my-jboss-host
```

Note:

- ▶ **run.bat** is the default script used to start JBoss.
 - ▶ **-b** option binds JBoss 4.2.2 to the correct network interface (it binds only to localhost by default making it inaccessible from other hosts).
 - ▶ You can build a similar script for UNIX.
-

JBoss Solution Template User Interface

<p>Description</p>	<p>Enables you to deploy the JBoss Application Server solution template.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click JBoss AS 4.x, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
---------------------------	---

Included in Tasks	“Deploy a SiteScope Solution Template – Workflow” on page 1276
Useful Links	“JBoss Application Server Solution Template” on page 1291

The following elements are found in the JBoss Application Server Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
JMX_URL	The URL to gather JMX statistics. Typically the URL is in the format: service:jmx:rmi:///jndi/rmi://{hostname}:{port}/jmxrmi. Type the hostname and port of the JMX instance you want to monitor.
USERNAME	User name for connection to the JMX application (optional).
Password	Password for connection to the JMX application (optional).

JMX Settings

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the entities you want to monitor. For each instance, a specific set of monitors and thresholds is created. For details, see the SiteScope JBoss Application Server Best Practices Guide which can be found at <code><SiteScope root directory>\sisdocs\pdfs\SiteScope_JBoss_Best_Practices.pdf</code> .

38

Linux Host Solution Templates

This chapter includes the main concepts, tasks, and reference information for the Linux Host Solution Template.

This chapter includes:

Concepts

- ▶ Linux Host Solution Overview on page 1299

Tasks

- ▶ Deploy the Linux Host Solution Template on page 1301

Reference

- ▶ Linux Host Solution Configuration Requirements on page 1302
- ▶ Linux Host Solution Template User Interface on page 1302

Linux Host Solution Overview

The Linux Host Solution Template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the target Linux host. The template supports the versions of Linux that are supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can create a Server-Centric Report which displays data from three different metrics about the server being monitored. It is recommended to use Solution Templates when creating the UNIX Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric Report, see “Generating a Server-Centric Report” on page 416.

The Linux Host Solution Template provides comprehensive Linux operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the Linux Host Solution Template. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the Linux Host Solutions settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at <SiteScope root directory>\sisdocs\pdfs\SiteScope_OS_Best_Practices.pdf. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

Solution Template Monitors

The Linux Host Solution Template deploys monitors that target the following aspects of Linux performance and health:

- ▶ CPU status and utilization details
- ▶ Memory status and utilization details
- ▶ File system status and utilization details

Deploy the Linux Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Linux Host Solution Template.

Note: The Linux Host Solution Template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Server-Centric Report support.

This task includes the following steps:

- “Configure the Linux Server Environment” on page 1301
- “Deploy the Solution Template” on page 1301
- “Type Variable Values for the Linux Host Solution Template” on page 1301

1 Configure the Linux Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “Linux Host Solution Configuration Requirements” on page 1302.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the Linux Host Solution Template

Complete the items on the Variable Values page for the Linux Host Solution Template. For details on configuring the variable values, see “Linux Host Solution Template User Interface” on page 1302.

Linux Host Solution Configuration Requirements

Before you can use the Linux Host Solution Template, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the target Linux host.
- The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test (**Preferences > UNIX Remote Preferences**). For details, see “UNIX Remote Preferences” on page 220.
- The SiteScope server itself can also be monitoring if it runs a supported Linux operating system.
- The template supports the Linux versions supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

Linux Host Solution Template User Interface

Description	<p>Enables you to deploy the Linux Host solution template. Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click Linux Host, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Included in Tasks	“Deploy a SiteScope Solution Template – Workflow” on page 1276
Useful Links	“Linux Host Solution Templates” on page 1299

The following elements are found in the Linux Host Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
SERVER_LIST	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a UNIX connection profile, see “UNIX Remote Preferences” on page 220.

39

Microsoft Exchange Solution Templates

This chapter includes the main concepts, tasks, and reference information for the Microsoft Exchange Solution Templates.

This chapter includes:

Concepts

- ▶ Microsoft Exchange Solution Overview on page 1306

Tasks

- ▶ Deploy Microsoft Exchange Solution Templates on page 1308

Reference

- ▶ Microsoft Exchange Solution Configuration Requirements on page 1309
- ▶ Microsoft Exchange Solution Template User Interface on page 1310

Microsoft Exchange Solution Overview

The Microsoft Exchange Solution Templates provide monitoring of performance, availability, and usage statistics for:

- ▶ Microsoft Exchange 5.5 Server
- ▶ Microsoft Exchange 2000 Server
- ▶ Microsoft Exchange 2003 Server
- ▶ Microsoft Exchange 2007 Server (version 8.0)

Depending on the set chosen, this set includes monitors checking NT Event log entries, MAPI operations, system performance counters, and message system usage statistics.

The Microsoft Exchange Solution Templates provide comprehensive Microsoft Exchange system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the Microsoft Exchange Solution templates. Contact your HP sales representative for more information about Solution licensing.
 - ▶ An in-depth description of the Microsoft Exchange Solution is available in the SiteScope Microsoft Exchange Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_Exchange_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Microsoft Exchange Solution license key from HP.
-

Solution Template Monitors

The Microsoft Exchange solution templates deploy monitors that target the following aspects of Microsoft Exchange performance and health:

- ▶ **Basic server/OS performance.** This category refers to the system-level health of a server. The Microsoft Exchange Solution Templates automatically configure monitors for server health.
- ▶ **Application performance.** Application performance is a measure of how well specific Exchange components are functioning. The Microsoft Exchange Solution Templates automatically configure monitors for a list of important Exchange application components.
- ▶ **Mail protocol response time.** Perhaps the most important aspect and key indicator of Microsoft Exchange performance is mail protocol response time. While Microsoft Exchange can utilize many protocols, the MAPI protocol is commonly used in Microsoft networks.
- ▶ **Usage statistics.** The last category related to Microsoft Exchange performance is usage. While usage in and of itself is not necessarily a key indicator of performance, changes in usage can affect overall Microsoft Exchange performance. In addition, Microsoft Exchange usage statistics help IT organizations spot trends and plan for the future. The Microsoft Exchange Solution Templates automatically configure monitors for a list of important Microsoft Exchange usage parameters.

Note: Some of the monitor types deployed by the solution templates can only be added to SiteScope by using the Microsoft Exchange Solution templates. See the section for the particular monitor types for more information.

Deploy Microsoft Exchange Solution Templates

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft Exchange Solution Template.

This task includes the following steps:

- “Configure the Microsoft Exchange Server Environment” on page 1308
- “Deploy the Solution Template” on page 1308
- “Type Variable Values for the Microsoft Exchange Solution Template” on page 1308

1 Configure the Microsoft Exchange Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “Microsoft Exchange Solution Configuration Requirements” on page 1309.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the Microsoft Exchange Solution Template

Complete the items on the Variable Values page for the Microsoft Exchange Solution Template. For details on configuring the variable values, see “Microsoft Exchange Solution Template User Interface” on page 1310.

Microsoft Exchange Solution Configuration Requirements

Before deploying a Microsoft Exchange Solution Template, you must perform various steps depending on the solution template you want to deploy.

- ▶ Microsoft Exchange 5.5, 2000, 2003 solutions. These solution templates make use of the SiteScope MAPI Monitor. Successful deployment of this monitor type requires specific setup configuration relating to the mailbox owners and the SiteScope service. For the MAPI Monitor system requirements, see “MAPI Monitor Overview” on page 830.
- ▶ Microsoft Exchange 2007 solution. The Microsoft Exchange 2007 solution template makes use of the Microsoft Exchange 2007 Monitor. Successful deployment of this monitor type requires specific setup configuration as described in “Microsoft Exchange 2007 Monitor Overview” on page 569.

Microsoft Exchange Solution Template User Interface

<p>Description</p>	<p>Enables you to deploy the Microsoft Exchange solution templates for monitoring:</p> <ul style="list-style-type: none"> ➤ Microsoft Exchange 5.5 Servers ➤ Microsoft Exchange 2000 Servers ➤ Microsoft Exchange 2003 Servers ➤ Microsoft Exchange 2007 Servers (version 8.0) <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click a Microsoft Exchange solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
<p>Included in Tasks</p>	<p>"Deploy a SiteScope Solution Template – Workflow" on page 1276</p>
<p>Useful Links</p>	<p>"Microsoft Exchange Solution Templates" on page 1305</p>

The following elements are found in the Microsoft Exchange Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
MailBox	Type the name (alias) of the mailbox to be used for testing e-mail round trip times using MAPI. This is often the e-mail account name but it may be a different name. It is recommended that you copy the mailbox name as it appears in the E-Mail Account properties for the e-mail account you will be using for this solution.
MailUser	Type the Windows account login name for the user for which e-mail round trip times will be tested using MAPI.
MailDomain (on Microsoft Exchange 5.5, 2000, and 2003) Domain (on Exchange 2007)	Type the domain to which both the owner of the mailbox being used and the Microsoft Exchange server belong. Note: The owner of the mailbox to be used by this solution must also have administrative account privileges on the machine where SiteScope is running. SiteScope also needs user account access to the domain where the Microsoft Exchange server is running.
MAILPASSWORD	Type the Windows account login password for the user name entered above.
SERVER_LIST	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.

GUI Element	Description
AuthenticationUser (Microsoft Exchange 2003 only)	Type the user name to use when querying the server for mailbox and public folder statistics. The statistics are gathered by using WMI (Windows Management Instrumentation), so the user name entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2. If this box is left blank, the user that SiteScope is running as will be used.
AUTHENTICATION PASSWORD (Microsoft Exchange 2003 only)	Type the password for the user entered above for gathering WMI statistics, or leave this blank if the user box is left blank.
PSConsoleFile (Microsoft Exchange 2007 only)	The path to the Microsoft Exchange Management Shell PowerShell console file.

40

Microsoft IIS Solution Template

This chapter includes the main concepts, tasks, and reference information for the Microsoft IIS Solution Template.

This chapter includes:

Concepts

- ▶ Microsoft IIS 6 Solution Overview on page 1314

Tasks

- ▶ Deploy the Microsoft IIS Solution Template on page 1315

Reference

- ▶ Microsoft IIS Solution Configuration Requirements on page 1316
- ▶ Microsoft IIS Solution Template User Interface on page 1316

Microsoft IIS 6 Solution Overview

The Microsoft IIS Solution Template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of Microsoft IIS servers. The template supports Microsoft IIS 6.0 server.

The Microsoft IIS Solution Template provides comprehensive IIS monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the Microsoft IIS solution template. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the IIS solution is available in the SiteScope Microsoft IIS Best Practices document. This document can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_IIS_Best_Practices.pdf`. This is a password protected document. The password is provided along with the IIS solution license key from HP.

Solution Template Monitors

The Microsoft IIS solution template deploys monitors that target the following services and aspects of IIS server performance and health:

- ▶ Active Server Pages (ASP errors, requests, templates, sessions, transactions)
- ▶ FTP service, Web service, SMTP server, NNTP server, HTTP/HTTPS services, MSMQ Queue service, IIS Server, Global IIS status, Indexing services
- ▶ IIS statistics as a Windows process

Deploy the Microsoft IIS Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft IIS Solution Template.

This task includes the following steps:

- “Configure the Microsoft IIS Server Environment” on page 1315
- “Deploy the Solution Template” on page 1315
- “Type Variable Values for the Microsoft IIS Solution Template” on page 1315

1 Configure the Microsoft IIS Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “Microsoft IIS Solution Configuration Requirements” on page 1316.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the Microsoft IIS Solution Template

Complete the items on the Variable Values page for the Microsoft IIS Solution Template. For details on configuring the variable values, see “Microsoft IIS Solution Template User Interface” on page 1316.

Microsoft IIS Solution Configuration Requirements

Before you can use the Microsoft IIS solution, there are a number of configuration requirements involving the server environment:

- ▶ SiteScope server must be able to connect to the target Microsoft IIS host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see “Microsoft Windows Resources Monitor Overview” on page 899.
- ▶ The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Preferences > Microsoft Windows Remote Preferences**). For details, see “Microsoft Windows Remote Preferences” on page 219. Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, See “Configure SiteScope to Monitor a Remote Windows Server” on page 236.
- ▶ SiteScope and the target Microsoft IIS server can run on the same host.

Microsoft IIS Solution Template User Interface

<p>Description</p>	<p>Enables you to deploy the Microsoft IIS 6 solution template.</p> <p>Use this page to add the server monitor or edit the monitor’s properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click Microsoft IIS 6, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
<p>Included in Tasks</p>	<p>“Deploy a SiteScope Solution Template – Workflow” on page 1276</p>
<p>Useful Links</p>	<p>“Microsoft IIS Solution Template” on page 1313</p>

The following elements are found in the Microsoft IIS Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
SERVER_LIST	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.

41

Microsoft SQL Server Solution Template

This chapter includes the main concepts, tasks, and reference information for the Microsoft SQL Server Solution Template.

This chapter includes:

Concepts

- ▶ Microsoft SQL Server Solution Overview on page 1319

Tasks

- ▶ Deploy the Microsoft SQL Server 2005 Solution Template on page 1321

Reference

- ▶ Microsoft SQL Server Solution Configuration Requirements on page 1322
- ▶ Microsoft SQL Server 2005 Solution Template User Interface on page 1323

Microsoft SQL Server Solution Overview

The Microsoft SQL Server Solution Template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of Microsoft SQL servers. The template supports Microsoft SQL Server 2005.

The Microsoft SQL Server Solution Template provides comprehensive Microsoft SQL server monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the Microsoft SQL Server solution template. Contact your HP sales representative for more information about Solution licensing.
 - ▶ An in-depth description of the Microsoft SQL Server solution is available in the SiteScope Microsoft SQL Server Best Practices document. This document can be found at <SiteScope root directory>\sisdocs\pdfs\SiteScope_MSSQL_Best_Practices.pdf. This is a password protected document. The password is provided along with the Microsoft SQL Server solution license key from HP.
-

Solution Template Monitors

The Microsoft SQL Server solution template deploys monitors that target the following aspects of Microsoft SQL server performance and health:

- ▶ CPU status and utilization details
- ▶ Memory status and utilization details
- ▶ Disk utilization information
- ▶ SQL Server objects (Buffer Manager, Databases, Locks, Transactions)
- ▶ SQL Server resources (space available, percentage of currently connected users)

The Microsoft SQL Server solution makes use of the SiteScope Database Counter monitor, Microsoft SQL Server monitor, and Microsoft Windows Resources monitor. For detailed information about these monitors, see “Database Counter Monitor Overview” on page 726, “Microsoft SQL Server Monitor Overview” on page 739, and “Microsoft Windows Resources Monitor Overview” on page 899.

Deploy the Microsoft SQL Server 2005 Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft SQL Server 2005 Solution Template.

This task includes the following steps:

- “Configure the Microsoft SQL Server Environment” on page 1321
- “Deploy the Solution Template” on page 1322
- “Type Variable Values for the Microsoft SQL Server 2005 Solution Template” on page 1322

1 Configure the Microsoft SQL Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “Microsoft SQL Server Solution Configuration Requirements” on page 1322.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the Microsoft SQL Server 2005 Solution Template

Complete the items on the Variable Values page for the Microsoft SQL Server 2005 Solution Template. For details on configuring the variable values, see “Microsoft SQL Server 2005 Solution Template User Interface” on page 1323.

Microsoft SQL Server Solution Configuration Requirements

Before you can use the Microsoft SQL Server solution, there are a number of configuration requirements involving the server environment:

- ▶ SiteScope server must be able to connect to the target Microsoft SQL host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see “Microsoft Windows Resources Monitor Overview” on page 899.
- ▶ The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Preferences > Microsoft Windows Remote Preferences**). For details, see “Microsoft Windows Remote Preferences” on page 219. Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, See “Configure SiteScope to Monitor a Remote Windows Server” on page 236.
- ▶ The SQL Server user must have **VIEW SERVER STATE** permissions on the monitored SQL Server 2005 instance to retrieve data from SQL Server System Views. For more information about granting permissions on Microsoft SQL Server 2005, see <http://msdn2.microsoft.com/en-us/library/ms186717.aspx>.
- ▶ SiteScope and the target Microsoft SQL Server can run on the same host.

Microsoft SQL Server 2005 Solution Template User Interface

Description	<p>Enables you to deploy the Microsoft SQL Server 2005 solution template for monitoring key components on Microsoft SQL Server 2005.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click Microsoft SQL Server 2005, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Included in Tasks	"Deploy a SiteScope Solution Template – Workflow" on page 1276
Useful Links	"Microsoft SQL Server Solution Template" on page 1319

The following elements are found in the Microsoft SQL Server 2005 Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Login to Microsoft SQL Server 2005	Type the login name for the user on the monitored Microsoft SQL Server 2005 instance.
Microsoft SQL Server 2005 password	Type the password for the user on the monitored Microsoft SQL Server 2005 instance.
Microsoft SQL Server 2005 URL	<p>Type the URL for the monitored Microsoft SQL Server 2005 instance.</p> <ul style="list-style-type: none"> ▶ Replace <code>#{host}</code> with the host name on which the Microsoft SQL Server 2005 is running. This must be the same as the host name defined for the Windows remote machine. For details, see “Microsoft Windows Remote Preferences” on page 219. ▶ Replace <code>#{port}</code> with the port number on which the Microsoft SQL Server 2005 accepts connections. By default, the port is 1433. <p>Example: <code>jdbc:mercury:sqlserver://doors:1433</code></p>
SERVER_LIST	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see “Configure SiteScope to Monitor a Remote Windows Server” on page 236.

42

Microsoft Windows Host Solution Template

This chapter includes the main concepts, tasks, and reference information for the Microsoft Windows Host Solution Template.

This chapter includes:

Concepts

- ▶ Microsoft Windows Host Solution Overview on page 1325

Tasks

- ▶ Deploy the Microsoft Windows Host Solution Template on page 1327

Reference

- ▶ Microsoft Windows Host Solution Configuration Requirements on page 1328
- ▶ Microsoft Windows Host Solution Template User Interface on page 1329

Microsoft Windows Host Solution Overview

The Microsoft Windows Host Solution Template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the Windows host. The template supports Microsoft Windows 2000, Windows XP, and Windows Server 2003.

For Microsoft Windows Resource Monitors, you can create a Server-Centric Report which displays data from three different metrics about the server being monitored. It is recommended to use Solution Templates when creating the Microsoft Windows Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric Report, see “Generating a Server-Centric Report” on page 416.

The Microsoft Windows Host Solution Template provides comprehensive Windows operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the Microsoft Windows Host Solution template. Contact your HP sales representative for more information about Solution licensing.
 - ▶ An in-depth description of the Microsoft Windows Host Solution settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_OS_Best_Practices.pdf`. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.
-

Solution Template Monitors

The Microsoft Windows Host solution template deploys monitors that target the following aspects of Microsoft Windows performance and health:

- ▶ High-level CPU status and utilization details
- ▶ High-level Memory status and utilization details
- ▶ Disk utilization information

Deploy the Microsoft Windows Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft Windows Host Solution Template.

Note: The Microsoft Windows Host Solution deploys a Microsoft Windows Resource Monitor for each target host. This monitor is an additional monitor that is required for Server-Centric Report support.

This task includes the following steps:

- ▶ “Configure the Microsoft Windows Server Environment” on page 1327
- ▶ “Deploy the Solution Template” on page 1327
- ▶ “Type Variable Values for the Microsoft Windows Host Solution Template” on page 1327

1 Configure the Microsoft Windows Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “Microsoft Windows Host Solution Configuration Requirements” on page 1328.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the Microsoft Windows Host Solution Template

Complete the items on the Variable Values page for the Microsoft Windows Host Solution Template. For details on configuring the variable values, see “Microsoft Windows Host Solution Template User Interface” on page 1329.

Microsoft Windows Host Solution Configuration Requirements

Before you can use the Microsoft Windows Host Solution, there are a number of configuration requirements involving the server environment:

- ▶ SiteScope server must be able to connect to the target Windows host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see “Microsoft Windows Resources Monitor Overview” on page 899.
- ▶ The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Preferences > Microsoft Windows Remote Preferences**). For details, see “Microsoft Windows Remote Preferences” on page 219. Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, See “Configure SiteScope to Monitor a Remote Windows Server” on page 236.
- ▶ You can monitor Windows operating system usage statistics on the SiteScope server provided SiteScope is installed on a supported Windows operating system. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.
- ▶ SiteScope and the target server can run on the same host if SiteScope is installed on a Windows operating system supported by the template. The template supports Microsoft Windows 2000, Windows XP, and Windows Server 2003.

Microsoft Windows Host Solution Template User Interface

Description	<p>Enables you to deploy the Microsoft Windows Host solution template for monitoring a Microsoft Windows 2000, Windows XP, and Windows Server 2003 operating system.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click Microsoft Windows Host, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Included in Tasks	"Deploy a SiteScope Solution Template – Workflow" on page 1276
Useful Links	"Microsoft Windows Host Solution Template" on page 1325

The following elements are found in the Microsoft Windows Host Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
SERVER_LIST	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see "Configure SiteScope to Monitor a Remote Windows Server" on page 236.

43

.NET Solution Templates

This chapter includes the main concepts, tasks, and reference information for the .NET Solution Templates.

This chapter includes:

Concepts

- ▶ .NET Solution Overview on page 1331

Tasks

- ▶ Deploy the .NET Solution Template on page 1333

Reference

- ▶ .NET Solution Configuration Requirements on page 1334
- ▶ .NET Solution Template User Interface on page 1334

.NET Solution Overview

The .NET Solution Templates enable you to monitor .NET applications of servers that run a Windows operating system. This solution template deploys a set of monitors that test the health, availability, and performance of a .NET application and .NET environment on the Windows host. The template supports Windows 2000, Windows XP, and Windows Server 2003.

The .NET Solution Templates provide comprehensive .NET monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the .NET Solution templates. Contact your HP sales representative for more information about Solution licensing.
 - ▶ An in-depth description of the .NET Solution is available in the SiteScope .NET Best Practices document. This document can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_NET_Best_Practices.pdf`. This is a password protected document. The password is provided along with the .NET Solution license key from HP.
-

Solution Template Monitors

The .NET solution templates deploy monitors that target the following aspects of .NET performance and health:

- ▶ **.NET CLR Data.** This category refers to the common language runtime data (environment of .NET applications). It is designed to check several resource statistics for the .NET CLR for selected application. The .NET Solution Template automatically configures monitors for server health.
- ▶ **ASP.NET.** This category is designed to check several resource statistics for the ASP.NET. It gathers common information about application restarts and whole ASP.NET system stability. The .NET Solution Template automatically configures monitors for server health.
- ▶ **ASP.NET Applications.** This category is designed to check several resource statistics for the selected ASP.NET application. It gathers common information about application cache, errors, and other critical information. The .NET Solution Template automatically configures monitors for server health.

Deploy the .NET Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the .NET Solution Template.

This task includes the following steps:

- “Configure the .NET Server Environment” on page 1333
- “Deploy the Solution Template” on page 1333
- “Type Variable Values for the .NET Solution Template” on page 1333

1 Configure the .NET Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “.NET Solution Configuration Requirements” on page 1334.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the .NET Solution Template

Complete the items on the Variable Values page for the .NET Solution Template. For details on configuring the variable values, see “.NET Solution Template User Interface” on page 1334.

.NET Solution Configuration Requirements

Before you can use the .NET Solution, there are a number of configuration requirements involving the server environment:

- ▶ SiteScope server must be able to connect to the target Windows host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see “Microsoft Windows Resources Monitor Overview” on page 899.
- ▶ The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Preferences > Microsoft Windows Remote Preferences**). For details, see “Microsoft Windows Remote Preferences” on page 219. Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, See “Configure SiteScope to Monitor a Remote Windows Server” on page 236.
- ▶ SiteScope and the target .NET application can run on the same host if SiteScope is installed on a Windows operating system supported by the template. The template supports Windows 2000, Windows XP, and Windows Server 2003.

.NET Solution Template User Interface

Description	<p>Enables you to deploy the .Net solution template for monitoring .NET application and .NET environments.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click a .NET solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Included in Tasks	“Deploy a SiteScope Solution Template – Workflow” on page 1276
Useful Links	“.NET Solution Templates” on page 1331

The following elements are found in the .NET Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Server	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. See “Configure SiteScope to Monitor a Remote Windows Server” on page 236 for the steps you use to create a Windows connection profile.
ASP.NET Application (ASP.NET Application only)	Type the name of the ASP.NET application you want to monitor. The name must be as it appears in the Task Manager
Instance (.NET CLR Data only)	Type the name of the application you want to monitor. The name must be the same as it appears in the Task Manager, or can be whole system statistics (by default).

44

Oracle Database Solution Template

This chapter includes the main concepts, tasks, and reference information for the Oracle Database Solution Templates.

This chapter includes:

Concepts

- ▶ Oracle Database Solution Overview on page 1338

Tasks

- ▶ Deploy Oracle Database Solution Templates on page 1340

Reference

- ▶ Oracle Database Solution Template Usage Guidelines on page 1341
- ▶ Oracle Database Solution Template Tools on page 1341
- ▶ Oracle Solution Template User Interface on page 1344

Oracle Database Solution Overview

You can use the Oracle Database Solution Templates to deploy a set of monitors that test the health, availability, and performance of an Oracle database. The deployed monitors check general system statistics, such as cache hit ratios and disk I/O, and include tools that provide diagnostic information about important aspects of the database. This solution can be used with Oracle 9i and 10g databases.

This solution uses the Database Counter Monitor to collect performance metrics from JDBC-accessible databases. In addition, you can use the Oracle Database Solution Template to deploy a collection of monitors configured with default metrics.

Important system metrics are computed with data retrieved from system tables in the Oracle database. A wide range of Oracle system tables such as V\$SYSSTAT, V\$LATCH, V\$ROLL_STAT, and V\$BUFFER_POOL_STATISTICS are consulted to produce these metrics. In this way, the Oracle Database Solution implements the equivalent of many of the system monitoring scripts that come bundled with the Oracle installation.

The Oracle Database Solution Templates provide comprehensive Oracle database monitoring without requiring the SiteScope user or the IT organization to be an expert on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the Oracle Database Solution Template. Contact your HP Sales representative for more information about Solution licensing.
 - ▶ An in-depth description of the Oracle Database Solution is available in the SiteScope Oracle Database Best Practices document. This document is part of the SiteScope installation, and can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_Oracle_Database_Best_Practices.pdf`. This is a password protected document. The password is provided along with the Oracle Database Solution license key from HP.
-

Solution Template Monitors

The Oracle Database Solution Template deploys monitors that target the following aspects of Oracle performance and health:

- ▶ **General System Statistics.** The most important V\$SYSSTAT statistics are monitored by default in the monitors deployed by the Oracle Database Solution. Where applicable, these metrics are combined to calculate deltas and rates on a per-second or per-transaction basis. When monitoring the important metrics from the V\$ tables in the database, the Oracle Database Solution is a replacement for manually generated SQL scripts.
- ▶ **Oracle Logs.** Important Oracle log files are monitored for ORA- errors. Users may customize these monitors to look for specific text in a log file, depending on their database configuration.
- ▶ **Diagnosing Database Problems.** In addition to the deployed monitors, Oracle Solution offers several tools that can be used to gain diagnostic information about a database. Resource-intensive SQL statements, shared server process contention, and the number of sessions waiting for specific events are all examples of the diagnostic data that these tools can provide.

Deploy Oracle Database Solution Templates

This task describes the steps involved in configuring the server environment and entering variables for the Oracle Database Solution Template.

This task includes the following steps:

- “Prerequisites” on page 1340
- “Configure the Oracle Database Server Environment” on page 1340
- “Deploy the Solution Template” on page 1340
- “Type Variable Values for the Oracle Database Solution Template” on page 1340

1 Prerequisites

You must have CREATE SESSION system privileges to successfully deploy the Oracle Database 9i and 10g Solution Template.

2 Configure the Oracle Database Server Environment

Follow the usage guidelines and perform the configuration requirements involving the server environment. For details on this topic, see “Oracle Database Solution Template Usage Guidelines” on page 1341.

3 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

4 Type Variable Values for the Oracle Database Solution Template

Complete the items on the Variable Values page for the Oracle Database Solution Template. For details on configuring the variable values, see “Oracle Solution Template User Interface” on page 1344.

Oracle Database Solution Template Usage Guidelines

Before configuring the Oracle Database Solution for deployment, consult the documentation for the Database Counter Monitor (see “Database Counter Monitor Overview” on page 726) and the Log File Monitor (see “Log File Monitor Settings” on page 802) for information about some of the prerequisites and parameters required by the solution template. For example, you find more information on installing the Oracle JDBC driver needed to communicate with the database and the format of the log file path parameter.

Oracle Database Solution Template Tools

The Oracle Solution Template deploys several tools that you can use to gather diagnostic information about an Oracle database. These tools are deployed to the same group as the monitors that are deployed by the solution template. They are displayed in much the same way as monitors but they are set as disabled. These tools are identified by the bold text **Solution Tool** in the **Status** field of the group content table. Although the Solution tools are listed in the monitor table, they are not monitor instances. They do not run automatically, do not display a status based on action results, nor do they trigger alerts. They are preconfigured actions that make use of a SiteScope Diagnostic Tool to check certain statistics from the Oracle database that may indicate a performance problem.

When the user clicks on one of these Solution Tools, SiteScope makes a custom SQL query to the database by using the Database Connection Test tool. The results of the query are found in a table at the bottom of the page. From this page, the tool may be run as many times as necessary by clicking the Connect and Execute Query button. Bear in mind that some tools may incur substantial overhead on the database, so executing them in quick succession is not recommended.

List of Oracle Database Solution Tools

The following describes tools deployed as part of the Oracle Database Solution:

Oracle Solution Tool Name	Description and Usage Guidelines
Top Ten SQL Statements in Logical IOs Per Row	<p>This tool performs a query which is designed to locate the most resource-intensive SQL statements being run in the database. The V\$SQL table is queried for the ten SQL statements which are performing the most logical IOs per row are displayed in a table.</p> <p>The statement IDs of these ten statements are displayed in a table, along with some additional resource-usage data for each statement.</p> <p>This additional data includes:</p> <ul style="list-style-type: none"> ▶ Physical IO Blocks. The number of disk reads performed on behalf of the statement. ▶ Logical IOs. The number of buffer gets performed on behalf of the statement. ▶ Rows Processed. The number of rows processed when executing the statement. ▶ Logical IOs Per Row. The number of buffer gets performed per row that was processed when executing the statement. ▶ Runs. The number of executions of the statement. ▶ Logical IOs Per Run. The number of buffer gets per statement execution. <p>Note: The action performed can have a significant affect on database resources and should not be run frequently.</p>
Number of Sessions Waiting Per Event	<p>This tool can be used in troubleshooting stuck sessions. When several sessions become unresponsive, this tool can determine whether the stuck sessions are all waiting on the same event. The tool action displays a table containing the number of sessions waiting on specific events.</p>

Oracle Solution Tool Name	Description and Usage Guidelines
Shared Server Process Contention (Common Queue Average Wait Time)	This tool calculates the average wait time of the shared server message queue (the Common Queue as recorded in V\$QUEUE). A high average wait time may indicate contention between shared server processes.

Use the following steps to run the Oracle Database Solution tools.

To run an Oracle Database Solution tool:

- 1** Click the group name for the group where the Oracle Solution monitors are deployed. The Group Detail page opens.
- 2** Find the Solution Tool for the action that you want to run. See the **Name** column for the Solution Tool for a description of the action performed by that tool.
- 3** Click the **Tools** link to the right of the tool **Name** to run the action. The Database Connection Test page opens. From this page, the tool may be run as many times as necessary by clicking the **Connect and Execute Query** button.

Note: Some Solution Tools may create significant overhead on the database depending on the query. Executing the tools in quick succession is therefore not advised.

The upper portion of the Database Connection Test page displays the database connection parameters used for the test. The results of the tool query are found in a table near the bottom of the page. Review the results based on the Description and Usage Guidelines for that tool.

 **Oracle Solution Template User Interface**

Description	<p>Enables you to deploy the Oracle solution template.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click an Oracle solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Important Information	<p>You must have CREATE SESSION system privileges to successfully deploy the Oracle Database 9i and 10g Solution Template.</p>
Included in Tasks	<p>"Deploy a SiteScope Solution Template – Workflow" on page 1276</p>
Useful Links	<p>"Oracle Database Solution Template" on page 1337</p>

The following elements are found in the Oracle Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
DatabaseConnection URL	Type the connection URL to the database you want to connect to. The syntax is jdbc:oracle:thin:@<server name or ip address>:<database server port>:<sid>. <p>Example: To connect to the ORCL database on a machine using port 1521 you would use: jdbc:oracle:thin:@206.168.191.19:1521:ORCL.</p> <p>Note: The colon and @ symbols must be included as shown.</p>
DatabaseDriver	The name of the JDBC driver to be used by this monitor. Each driver supports a specific connection URL pattern, so it must match the URL entered in Database Connection URL .
OracleAlertLogPath	Type the full path to the Oracle alert log. For Windows machines, this should be the full UNC path. Type the full path to the Oracle alert log. Consult your database administrator or the Oracle documentation for information about how to access this file.
OracleListenerLog Path	Type the full path to the Oracle listener log. For Windows machines, this should be the full UNC path. Consult your database administrator or the Oracle documentation for information about how to access this file.
DatabaseUserName	Type the user name that SiteScope should use to connect to the database.
DATABASEPASSWORD	Type the password for the user name that SiteScope should use to connect to the database.

GUI Element	Description
Log File Encoding	<p>If the file content to be monitored uses an encoding that is different than the encoding used on server where SiteScope is running, type the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the target file. This will enable SiteScope to match and display the encoded file content correctly.</p> <p>Examples: Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.</p>
SERVER_LIST	<p>Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a connection profile, see “Microsoft Windows Remote Preferences” on page 219 and “UNIX Remote Preferences” on page 220.</p>

45

SAP Solution Templates

This chapter includes the main concepts, tasks, and reference information for the SAP Solution Templates.

This chapter includes:

Concepts

- ▶ SAP Solution Overview on page 1348

Tasks

- ▶ Deploy the SAP Solution Template on page 1349

Reference

- ▶ SAP Solution Template Configuration Requirements on page 1350
- ▶ SAP Solution Template User Interface on page 1351

SAP Solution Overview

The SAP solution includes solution templates for the monitoring the following key SAP components:

- SAP CCMS
- SAP Java Web Application Server

The SAP Solution uses two solution templates which you use to deploy a collection of monitors configured with metrics to report on availability and performance. These monitoring configurations have been researched using best practice data and expertise from various sources.

The SAP Solution Templates provide comprehensive SAP monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note: You must have the applicable SiteScope option license to use the SAP R/3 and SAP J2EE solution templates. Contact your HP sales representative for more information about licensing for solution templates.

You use the SAP R/3 solution template to deploy monitoring for SAP R/3 systems. You use the SAP J2EE template to monitor the SAP Java Web Application server if this component is deployed in the IT environment.

Deploy the SAP Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the SAP Solution Template.

This task includes the following steps:

- “Configure the SAP Server Environment” on page 1349
- “Deploy the Solution Template” on page 1349
- “Type Variable Values for the SAP Solution Template” on page 1349

1 Configure the SAP Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “SAP Solution Template Configuration Requirements” on page 1350.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the SAP Solution Template

Complete the items on the Variable Values page for the SAP Solution Template. For details on configuring the variable values, see “SAP Solution Template User Interface” on page 1351.

SAP Solution Template Configuration Requirements

SAP R/3 Solution Template

The SiteScope SAP R/3 solution template provides the tools you use to monitor the availability, usage statistics, and server performance statistics for SAP R/3 systems. This solution template deploys a set of monitors that test the health, availability, and performance of SAP R/3 servers.

Before you can use the SAP R/3 solution template, there are a number of configuration requirements involving the server environment. The following lists an overview of these requirements:

- ▶ SAP Java Connector libraries should be copied to the required SiteScope folders.
- ▶ You must know the user name and password that SiteScope must use to log into the SAP R/3 server.

For more information on system and configuration requirements, see “SAP CCMS Monitor Overview” on page 579. This monitor is deployed as part of the SAP R/3 solution template.

SAP NetWeaver Solution Template

The SiteScope SAP NetWeaver Application Server solution enables you to monitor the availability and server statistics for SAP Java Web application server clusters.

This solution template deploys a monitor that tests the health, availability, and performance of SAP Java Web application servers. You can use this solution template to deploy monitors for server-wide resources and metrics.

Before you can use the SAP NetWeaver Application Server solution template, there are a number of configuration requirements involving the server environment. The following lists an overview of these requirements:

- ▶ SAP Java Web application server libraries must be copied to the required SiteScope folders.
- ▶ You must know the user name and password that SiteScope must use to log into the SAP Java Web application server.

For more information on system and configuration requirements, see “SAP Java Web Application Server Monitor Overview” on page 588. This monitor is deployed as part of the SAP J2EE solution template.

SAP Solution Template User Interface

Description	<p>Enables you to deploy the SAP solution templates for monitoring key components on SAP CCMS and SAP Java Web Application Servers.</p> <p>Use this page to add the server monitor or edit the monitor’s properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click an SAP solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Included in Tasks	“Deploy a SiteScope Solution Template – Workflow” on page 1276
Useful Links	“SAP Solution Templates” on page 1347

SAP R/3

The Main Settings include the following elements:

GUI Element	Description
CLIENT_NUMBER	Type the Client to use for connecting to SAP.
Password	Type the password required to connect to the SAP server.
USER_NAME	Type the user name required to connect to the SAP server.
SYSTEM_NUMBER	Type the System number for the SAP server.
APPLICATION_SERVER	Type the address of the SAP server you want to monitor.

SAP NetWeaver Application Server

The Main Settings include the following elements:

GUI Element	Description
TARGET_SERVER_NAME	Type the address of the SAP Java Web Application Server you want to monitor.
USER_NAME	Type the user name required to connect to the SAP Java Web Application Server.
PORT	Type the port for the SAP Java Web Application Server.
Password	Type the password required to connect to the SAP Java Web Application Server.

46

Siebel Solution Templates

This chapter includes the main concepts, tasks, and reference information for the Siebel Solution Templates.

This chapter includes:

Concepts

- ▶ Siebel Solution Overview on page 1354

Tasks

- ▶ Deploy the Siebel Solution Template on page 1356

Reference

- ▶ Siebel Solution Configuration Requirements on page 1357
- ▶ Siebel Solution Template User Interface on page 1358

Siebel Solution Overview

The SiteScope Siebel Solution Templates provide efficient and thorough monitoring of performance, availability, and usage statistics for Siebel Application, Gateway, and Web servers installed on Microsoft Windows and UNIX operating systems.

The primary solution template for Siebel is the Siebel Application Server template. This solution template is applicable to all Siebel deployments on Windows and UNIX platforms. You use this template to deploy monitoring for the core of the Siebel application. You use the Siebel Gateway Server and Siebel Web Server templates if these optional components are deployed in the IT environment.

The Siebel Solution Templates provide comprehensive Siebel monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy various performance monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the Siebel Solution templates. Contact your HP sales representative for more information about Solution licensing.
 - ▶ An in-depth description of the Siebel Solution is available in the SiteScope Siebel Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_Siebel_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Siebel Solution license key from HP.
-

Solution Template Monitors

The Siebel Solution includes solution templates for monitoring the following key Siebel components:

- ▶ **Siebel Application Server.** The SiteScope Siebel Application Server Solution allows you to monitor the availability, usage statistics, and server performance statistics for Siebel Application servers installed on Windows and UNIX platforms. This solution template deploys a set of monitors that test the health, availability, and performance of Siebel 6.x, 7.x, and 8.x application servers.
- ▶ **Siebel Gateway Server.** The SiteScope Siebel Gateway Server Solution allows you to monitor the availability and server statistics for Siebel Gateway servers installed on Windows and UNIX platforms. This solution template deploys a set of monitors that test the health, availability, and performance of Siebel Gateway Servers. You can use this solution template to deploy monitors for server-wide resources and metrics.
- ▶ **Siebel Web Server.** The SiteScope Siebel Web Server Solution allows you to monitor the availability and server statistics for Siebel Web servers installed on Windows and UNIX platforms. This solution template deploys a set of monitors that test the health, availability, and performance of Siebel Web Servers.

Deploy the Siebel Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Siebel Solution Template.

This task includes the following steps:

- “Configure the Siebel Server Environment” on page 1356
- “Deploy the Solution Template” on page 1356
- “Type Variable Values for the Siebel Solution Template” on page 1356

1 Configure the Siebel Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “Siebel Solution Configuration Requirements” on page 1357.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the Siebel Solution Template

Complete the items on the Variable Values page for the Siebel Solution Template. For details on configuring the variable values, see “Siebel Solution Template User Interface” on page 1358.

Siebel Solution Configuration Requirements

Before you can use the Siebel Application or Web Server Solution, there are a number of configuration requirements involving the server environment.

Siebel Application Server Solution Template

- ▶ The Siebel Server Manager client must be installed only on a Windows machine where SiteScope is running or that is accessible to the SiteScope machine (even if the Siebel application server is installed on UNIX). There are several options for how you can do this. See the documentation for the Siebel Server Manager Monitor for more information.
- ▶ You must know the install path for the Server Manager client to be able to setup Siebel Server Manager monitors in SiteScope. If the client is installed on the machine where SiteScope is running, this is the path on that machine. If the client is installed on a remote machine, you must know the fully qualified path to the client executable relative to that machine.
- ▶ You must know the name of the Siebel applications that are available in your network. For example, call center, sales, and so on.
- ▶ You must know the Siebel database machine name, user name, password, connection URL, and Database Driver.
- ▶ You must know the user and password that SiteScope uses for logging into the Siebel server. This user must be granted Siebel Administrator responsibility on the Siebel server.
- ▶ You must make sure that the following Siebel server component groups are enabled:
 - ▶ Siebel Call Center (CallCenter)
 - ▶ Siebel Remote (Remote)
 - ▶ System Management (System)
 - ▶ Auxiliary System Management (SystemAux) - Siebel 8.x only

- ▶ You need to know a significant list of Siebel system component names and their corresponding aliases. For a listing of component names and aliases, see “Siebel Solution Template User Interface” on page 1358.

For more information on system and configuration requirements, see the sections on the “Siebel Web Server Monitor Overview” on page 602 and “Database Query Monitor Overview” on page 729. These monitor types that are deployed as part of the Siebel Application Server Solution Template.

Siebel Web Server Solution Template

- ▶ SiteScope server must be able to connect to the machine where the Siebel Web Server is running.
- ▶ Siebel Web Server Solution is designed for use with Siebel running on Microsoft Windows platforms.
- ▶ Template assumes that the Siebel Web Server is running on Microsoft Internet Information Server (IIS).

Siebel Solution Template User Interface

<p>Description</p>	<p>Enables you to deploy the Siebel solution templates for monitoring the Siebel 6.x, 7.x, and 8.x Application Server, Siebel Gateway Server, and Siebel Web Server on Windows and UNIX platforms.</p> <p>Use this page to add the server monitor or edit the monitor’s properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click a Siebel solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
<p>Included in Tasks</p>	<p>“Deploy a SiteScope Solution Template – Workflow” on page 1276</p>
<p>Useful Links</p>	<p>“Siebel Solution Templates” on page 1353</p>

Siebel Application Server

The Main Settings include the following elements for monitoring Siebel Application Server 6.x, 7.x, and 8.x on Windows and UNIX environments:

GUI Element (A-Z)	Description
Application	Type the Siebel Application Server machine name.
CG_Auxiliary_System_Management_Alias (Siebel 8.x only)	Type the Siebel Auxiliary System Management component group alias.
CG_Auxiliary_System_Management_Name (Siebel 8.x only)	Type the Siebel Auxiliary System Management component group name.
CG_Callcenter_Alias	Type the Siebel CallCenter component group alias.
CG_Callcenter_Name	Type the Siebel CallCenter component group name.
CG_System_Management_Alias	Type the Siebel System Management component group alias.
CG_System_Management_Name	Type the Siebel System Management component group name.
CP_Callcenter_Alias	Type the Siebel CallCenter component alias.
CP_Callcenter_Name	Type the Siebel CallCenter component name.
CP_Client_Administration_Alias (Siebel 6.x-7.x only)	Type the Siebel Client Administration component alias.
CP_Client_Administration_Name (Siebel 6.x-7.x only)	Type the Siebel Client Administration component name.
CP_eService_Alias	Type the Siebel eService component alias.
CP_eService_Name	Type the Siebel eService component name.
CP_File_System_Manager_Alias	Type the Siebel File System Manager component alias.

GUI Element (A-Z)	Description
CP_File_System_Manager_Name	Type the Siebel File System Manager component name.
CP_Server_Manager_Alias	Type the Siebel Server Manager component alias.
CP_Server_Manager_Name	Type the Siebel Server Manager component name.
CP_Server_Request_Broker_Alias	Type the Siebel Server Request Broker component alias.
CP_Server_Request_Broker_Name	Type the Siebel Server Request Broker component name.
CP_Server_Request_Processor_Alias	Type the Siebel Server Request Broker component alias.
CP_Server_Request_Processor_Name	Type the Siebel Server Request Processor component name.
Database_Connection_URL	<p>Type the URL to the database connection.</p> <p>Example: If the ODBC connection is called <code>test</code>, the URL would be <code>jdbc:odbc:test</code>.</p> <p>Type the connection URL to the database you want to connect to. The syntax is <code>jdbc:oracle:thin:@<server name or ip address>:<database server port>:<sid></code>.</p> <p>Example: To connect to the ORCL database on a machine using port 1521 you would use: <code>jdbc:oracle:thin:@206.168.191.19:1521:ORCL</code>.</p> <p>Note: The colon and <code>@</code> symbols must be included as shown.</p>
Database_Driver	Type the driver used to connect to the database.
Database_PASSWORD	Type the password for the user name used to access the Siebel database.
Database_Username	Type the user name SiteScope should use to access the Siebel database.
Enterprise	Type the Siebel Enterprise server name.

GUI Element (A-Z)	Description
Gateway	Type the name of the Siebel Gateway server machine.
PASSWORD	Type the password for the Siebel Client.
SERVER_LIST	Select the server where the Siebel Application Server is running.
Server_Logical_Instance_Name	Type the Siebel server logical name.
Server_Manager_Path	Type the local path to the Siebel server manager client. Example: D:\sea703\client\bin.
Siebel_Database_Machine_Name	Type the Siebel database machine name.
Siebel_Disk	Type the disk drive name where Siebel is installed.
Siebel_Root_Dir	Type the path of the shared Siebel root directory. Example: The shared root directory for a Siebel 7.5.2 server would be: sea752.
Username	Type the Siebel Client user name.

Siebel Gateway Server

The Main Settings include the following elements:

GUI Element	Description
Siebel_Root_Dir	Type the path to the Siebel root directory. This directory should contain at least an Admin Console installation.
Siebel_Disk	Type the disk drive where the Siebel gateway server is running.
Siebel_Logical_Instance_Name	Type the Siebel server logical name value (for UNIX only).
SERVER_LIST	Type the name of the server where the Siebel Gateway Server is running. Do not type backslashes (\\) that indicate a UNC path as part of the name of the server.

Siebel Web Server

The Main Settings include the following elements:

GUI Element	Description
Application	Type the Siebel application to monitor. For example: callcenter_enu. Consult with your Siebel administrator for information about names of the installed Siebel applications.
Siebel_Disk	Type the disk drive name or drive letter where the Siebel Web server is installed.
Siebel_Root_Dir	Type the name of the shared Siebel root directory. Example: Siebel root directory on Windows: sea752.
Siebel_Logical_Instance_Name	Type the Siebel server logical name value (for UNIX only).
Username	Type the Siebel Client user name needed to log into the Siebel Web server.
Password	Type the Siebel Client password needed to log into the Siebel Web server.
SERVER_LIST	Select the Siebel Web server machine name. Use the choose server to view the server selection page. Use the Server drop-down menu to select the server where the Siebel Web server is running.

47

Solaris Host Solution Templates

This chapter includes the main concepts, tasks, and reference information for the Solaris Host Solution Template.

This chapter includes:

Concepts

- ▶ Solaris Host Solution Overview on page 1363

Tasks

- ▶ Deploy the Solaris Host Solution Template on page 1365

Reference

- ▶ Solaris Host Solution Configuration Requirements on page 1366
- ▶ Solaris Host Solution Template User Interface on page 1366

Solaris Host Solution Overview

The Solaris Host Solution Template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the Solaris host. The template supports the versions of Solaris that are supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can create a Server-Centric Report which displays data from three different metrics about the server being monitored. It is recommended to use Solution Templates when creating the UNIX Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric Report, see “Generating a Server-Centric Report” on page 416.

The Solaris Host Solution Template provides comprehensive Solaris operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the Solaris Host Solution Template. Contact your HP sales representative for more information about Solution licensing.
 - ▶ An in-depth description of the Solaris Host Solution settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at <**SiteScope root directory**>\sisdocs\pdfs**SiteScope_OS_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.
-

Solution Template Monitors

The Solaris Host solution Template deploys monitors that target the following aspects of Solaris performance and health:

- ▶ CPU status and utilization details
- ▶ Memory status and utilization details
- ▶ File system status and utilization details

Deploy the Solaris Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Solaris Host Solution Template.

Note: The Solaris Host Solution Template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Server-Centric Report support.

This task includes the following steps:

- “Configure the Solaris Server Environment” on page 1365
- “Deploy the Solution Template” on page 1365
- “Type Variable Values for the Solaris Host Solution Template” on page 1365

1 Configure the Solaris Server Environment

Perform the configuration requirements involving the server environment. For details on this topic, see “Solaris Host Solution Configuration Requirements” on page 1366.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the Solaris Host Solution Template

Complete the items on the Variable Values page for the Solaris Host Solution Template. For details on configuring the variable values, see “Solaris Host Solution Template User Interface” on page 1366.

Solaris Host Solution Configuration Requirements

Before you can use the Solaris Host Solution Template, there are a number of configuration requirements involving the server environment:

- ▶ SiteScope server must be able to connect to the target Solaris host.
- ▶ The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test (**Preferences > UNIX Remote Preferences**). For details, see “UNIX Remote Preferences” on page 220.
- ▶ The SiteScope server itself can also be monitoring if it runs a supported Solaris operating system.
- ▶ The template supports the Solaris versions supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

Solaris Host Solution Template User Interface

Description	<p>Enables you to deploy the Solaris solution template. Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click Solaris Host, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Included in Tasks	“Deploy a SiteScope Solution Template – Workflow” on page 1276
Useful Links	Solaris Host Solution Templates

The following elements are found in the Solaris Host Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
SERVER_LIST	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a UNIX connection profile, see “UNIX Remote Preferences” on page 220.

48

WebLogic Solution Template

This chapter includes the main concepts, tasks, and reference information for the WebLogic Solution Templates.

This chapter includes:

Concepts

- ▶ WebLogic Solution Overview on page 1369

Tasks

- ▶ Deploy the WebLogic Solution Template on page 1371

Reference

- ▶ WebLogic Solution Usage Guidelines on page 1372
- ▶ Selecting WebLogic Modules for Monitoring on page 1372
- ▶ WebLogic Solution Template User Interface on page 1374

WebLogic Solution Overview

The WebLogic Solution Template is a template that you can use to deploy a collection of WebLogic Monitors configured with default metrics. The monitors test the health, availability, and performance of a WebLogic Application Server and its deployed applications and components. The deployed monitors check server-wide statistics such as memory usage, as well as metrics specific to individual J2EE components, such as the number of activates and passivates of a particular EJB.

Use the WebLogic Solution to monitor statistics from WebLogic 6.x, 7.x, 8.x, 9.x, and 10.x servers. This solution automatically creates several groups by default which monitor important application server metrics, but it also provides a user interface that allows you to select all or some of the individual components that are available for monitoring.

The WebLogic Solution monitor deployment process is highly customizable in that it allows the user to select the specific J2EE components on an application server which SiteScope should actively monitor.

The WebLogic Solution Templates provide comprehensive WebLogic monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the WebLogic Solution Template. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the WebLogic Solution is available in the SiteScope WebLogic Best Practices document. This document is part of the SiteScope installation, and can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_WebLogic_Best_Practices.pdf`. This is a password protected document. The password is provided along with the WebLogic Solution license key from HP.

Solution Template Monitors

The WebLogic Solution Template deploys monitors that target the following aspects of WebLogic performance and health:

- ▶ **Server Performance Statistics.** This category refers to a collection of server-wide resources that are exposed through the management interface of a WebLogic Application Server.

- ▶ **Application Performance Statistics.** Metrics for all of your deployed applications, EJBs, web applications, and servlets are available for monitoring through the WebLogic Solution. The user is responsible for selecting which of these J2EE components he would like to have monitors automatically deployed for. A set of metrics based on WebLogic best practices are monitored for each selected J2EE component.
- ▶ **WebLogic Solution Metrics.** For the list of components that can be monitored, see the SiteScope WebLogic Best Practices document.

Deploy the WebLogic Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the WebLogic Solution Template.

This task includes the following steps:

- ▶ “Configure the WebLogic Server Environment” on page 1371
- ▶ “Deploy the Solution Template” on page 1371
- ▶ “Type Variable Values for the WebLogic Solution Template” on page 1371

1 Configure the WebLogic Server Environment

Follow the usage guidelines and perform the configuration requirements involving the server environment. For details on this topic, see “WebLogic Solution Usage Guidelines” on page 1372.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the WebLogic Solution Template

Complete the items on the Variable Values page for the WebLogic Solution Template. For details on configuring the variable values, see “WebLogic Solution Template User Interface” on page 1374.

WebLogic Solution Usage Guidelines

The WebLogic Solution Template deploys a WebLogic Application Server Monitor for each module that is selected from the user interface. This monitor uses the Java JMX interface to access Runtime MBeans on the WebLogic server. An MBean is a container that holds the performance metrics. You may need to set certain permissions on the WebLogic server for SiteScope to be able to monitor MBeans. For an overview on configuring access to WebLogic servers for SiteScope monitors, see “WebLogic Application Server Monitor Overview” on page 610.

Selecting WebLogic Modules for Monitoring

The WebLogic Solution presents a hierarchical list from which the user can select the modules to deploy WebLogic Monitors against. This list is broken down into two main sections:

- ▶ per-server resources
- ▶ J2EE components organized by application

Some of the modules in these categories are automatically selected by default because they represent critical components in the system (for example, the JVM statistics for the application server). The remainder of the modules are not automatically selected. This allows the user to customize the deployment of this solution to focus on one application, a particular type of EJB, a set of servlets and web applications, or some other aspect of the application server.

For the most part, the organization of this list of modules is intuitive. The hierarchy of applications, EJBs, web applications, and servlets is very similar to the organization of these entities in the WebLogic Administration Console. In almost every case, selecting a module causes a monitor with all relevant metrics to be deployed against that part of the WebLogic server. However, when selecting EJBs to monitor, you notice that they are broken down according to three types of metrics: Pool, Transaction, and Cache. The reason for this is twofold: (1) it is more useful to be able to monitor one aspect of a particular EJB instead per WebLogic Monitor for purposes of alerting and organization, and (2) not all three of these types of metrics are available for all EJBs.

Below is a brief description of the metrics that are monitored for each type of EJB monitoring:

- ▶ **Per-EJB Transaction Statistics.** This category of EJB monitor contains metrics related to transactions made for the EJB. These metrics include the number of transactions rolled back, the number of transactions that timed out, and the number of transactions that were successfully committed.
- ▶ **Per-EJB Pool Statistics.** This category of EJB monitor contains metrics related to the pool for the EJB. When the user selects an EJB under this heading, many useful metrics are monitored, including the number of times an attempt to get a bean instance from the pool failed, the number of current available instances in the pool, the number of threads currently waiting for an instance, and the number of times a bean instance was destroyed due to a non-application exception.
- ▶ **Per-EJB Cache Statistics.** The cache statistics include any metrics relating to the caching of the particular EJB. Metrics like the number of cache hits and misses, and the number of activates and passivates of the EJB are monitored when an EJB under this heading is selected for monitoring.

When you have finished making your module selections in the popup window, scroll to the bottom of the Module Selection window and click the **Select Modules** button. This updates the main browser window with a list of the modules you selected. You can then review your selections and remove any modules that you don't want a monitor to be created for.

When you are satisfied with the list of selected modules in the main browser window, click the **Submit** button.

WebLogic Solution Template User Interface

Description	<p>Enables you to deploy the WebLogic solution template for monitoring BEA WebLogic 6.x, 7.x, 8.x, 9.x, and 10.x application servers.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click a WebLogic solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Included in Tasks	"Deploy a SiteScope Solution Template – Workflow" on page 1276
Useful Links	"WebLogic Solution Template" on page 1369

WebLogic 9.x-10.x

The Main Settings include the following elements:

GUI Element	Description
WEBLOGIC_URL	<p>Type the URL for the WebLogic 9.x or 10.x application server. The default is:</p> <pre>service:jmx:rmi:///jndi/iiop://<local host>:7001/weblogic.management.mbeanservers.runtime</pre> <p>where <local host> is the name of the machine running WebLogic Application Server 9.x or 10.x.</p>

The JMX Settings include the following elements:

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

WebLogic 6.x, 7.x, 8.x

The Main Settings include the following elements:

GUI Element	Description
WEBLOGIC_PORT	Type the port number that the WebLogic server is responding on. Default value: 7001
WEBLOGIC_PASSWORD	Type the password required to log into the WebLogic server.
WEBLOGIC_USERNAME	Type the user name required to log into the WebLogic server.
WEBLOGIC_SERVER	Type the name or address of the server where WebLogic is running.
WEBLOGIC_TIMEOUT	Type the number of seconds to wait for a data request to arrive at the WebLogic server. Default value: 180
WEBLOGIC_JAR_FILE	Type the absolute path to the weblogic.jar file on the SiteScope machine. This file must be installed on the SiteScope server and can be downloaded from the WebLogic server. Example: c:\bea\weblogic7\ebcc\lib\ext\weblogic.jar.

49

WebSphere Solution Template

This chapter includes the main concepts, tasks, and reference information for the WebSphere Solution Templates.

This chapter includes:

Concepts

- ▶ WebSphere Solution Overview on page 1377

Tasks

- ▶ Deploy the WebSphere Solution Template on page 1379

Reference

- ▶ WebSphere Solution Template User Interface on page 1380

WebSphere Solution Overview

The WebSphere Solution Template is a template that you can use to deploy a collection of WebSphere Monitors configured with default metrics. The monitors test the availability, server statistics, and deployed J2EE components for IBM WebSphere Application Server 5.x and 6.x. You can use this solution template to deploy monitors for server-wide resources and metrics (for example, thread pool and JVM metrics). You can also create monitors for the deployed EJBs, Web Applications, and Servlets using this solution template.

The WebSphere Solution monitor deployment process is highly customizable in that it allows the user to select the specific J2EE components on an application server which SiteScope should actively monitor.

The WebSphere Solution Templates provide comprehensive WebSphere monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- ▶ You must have the applicable SiteScope option license to use the WebSphere Solution templates. Contact your HP Sales representative for more information about Solution licensing.
 - ▶ An in-depth description of the WebSphere Solution is available in the SiteScope WebSphere Best Practices document. This document is part of the SiteScope installation, and can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_WebSphere_Best_Practices.pdf`. This is a password protected document. The password is provided along with the WebSphere Solution license key from HP.
-

Solution Template Monitors

The WebSphere Solution Template deploys monitors that target the following aspects of WebSphere performance and health:

- ▶ **Server Performance Statistics.** This category refers to a collection of server-wide resources that are exposed through the management interface of a WebSphere Application Server.
- ▶ **Application Performance Statistics.** Metrics for all of your deployed applications, EJBs, web applications, and servlets are available for monitoring through the WebSphere Solution. The user is responsible for selecting which of these J2EE components he would like to have monitors automatically deployed for. A set of metrics based on WebSphere best practices are monitored for each selected J2EE component.
- ▶ **WebSphere Application Server Solution Metrics.** For the list of components that can be monitored, see the SiteScope WebSphere Best Practices document.

Deploy the WebSphere Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the WebSphere Solution Template.

This task includes the following steps:

- “Configure the WebSphere Server Environment” on page 1379
- “Deploy the Solution Template” on page 1379
- “Type Variable Values for the WebSphere Solution Template” on page 1379

1 Configure the WebSphere Server Environment

Perform the configuration requirements involving the server environment. For an overview of these requirements, see “WebSphere Application Server Monitor Overview” on page 613.

2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1276.

3 Type Variable Values for the WebSphere Solution Template

Complete the items on the Variable Values page for the WebSphere Solution Template. For details on configuring the variable values, see “WebSphere Solution Template User Interface” on page 1380.

 **WebSphere Solution Template User Interface**

Description	<p>Enables you to deploy the WebSphere solution template for monitoring IBM WebSphere Application Servers 5.x and 6.x.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p>To access:</p> <p>In the monitor tree, expand Solution Templates, right-click a WebSphere solution template, and click Copy. Right-click the SiteScope or monitor group container into which you want to deploy the solution, and click Paste.</p>
Included in Tasks	"Deploy a SiteScope Solution Template – Workflow" on page 1276
Useful Links	"WebSphere Solution Template" on page 1377

The following elements are found in the WebSphere Solution Template Variable Values page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
WEBSPHERE_USER_NAME	<p>Type the user name that SiteScope should use to login to WebSphere Application server.</p> <p>In WebSphere 6.x, Global Security is not supported in the solution template. This means that you can type in any text however, the text box cannot be left empty. If you need to work with Global Security, complete this template. Edit the WebSphere monitor and, in the Advanced Settings pane, update the Global Security boxes (Trust Store, Trust Store Password, Key Store, Key Store Password).</p>
WEBSPHERE_CLIENT_PROPERTIES_FILE	<p>Type the client properties file.</p> <p>Default value: /properties/soap.client.props</p>
WEBSPHERE_DIRECTORY	<p>Type the path to the WebSphere directory that contains the /java and /lib subdirectories from the WebSphere Application Server.</p> <p>In WebSphere 6.x, this directory must also contain /profiles subdirectory. This subdirectory has all Key Store and Trust Store files needed for Global Security. The server profile in /profiles subdirectory must be called default. If the server profile has a different name, rename it to default.</p>
WEBSPHERE_SERVER	<p>Type the name of the server where the WebSphere Application is running. Do not type backslashes (\\) that indicate a UNC path as part of the name of the server.</p>

GUI Element	Description
WEBSHERE_ PORT	<p>Type the port number of the WebSphere server. This should be the SOAP port for WebSphere 5.x.</p> <p>Default value: 8880</p>
WEBSHERE_ PASSWORD	<p>Type the password that SiteScope should use to login to WebSphere server.</p> <p>In WebSphere 6.x, Global Security is not supported in the solution template. This means that you can type in any text however, the text box cannot be left empty. If you need to work with Global Security, complete this template. Edit the WebSphere monitor and, in the Advanced Settings pane, update the Global Security boxes (Trust Store, Trust Store Password, Key Store, Key Store Password).</p>

Part VIII

Alerts and Reports

50

SiteScope Alerts

This chapter includes the main concepts, tasks, and reference information for SiteScope Alerts.

This chapter includes:

Concepts

- ▶ SiteScope Alerts Overview on page 1386
- ▶ Creating Alert Actions on page 1389
- ▶ Understanding When SiteScope Alerts Are Sent on page 1390
- ▶ Customizing Alert Templates on page 1394
- ▶ Working with Database Alerts on page 1396
- ▶ Working with Disable or Enable Monitor Alerts on page 1397
- ▶ Working with E-Mail Alerts on page 1398
- ▶ Working with Log Event Alerts on page 1399
- ▶ Working with Pager Alerts on page 1400
- ▶ Working with Post Alerts on page 1401
- ▶ Working with Script Alerts on page 1402
- ▶ Working with SMS Alerts on page 1406
- ▶ Working with SNMP Trap Alerts on page 1407
- ▶ Working with Sound Alerts on page 1408

Tasks

- ▶ Configure an Alert on page 1409
- ▶ Customize an Alert's Message Content on page 1411

- ▶ Customize Alert Template Tag Styles on page 1413

Reference

- ▶ SiteScope Alert Templates Directory on page 1414
- ▶ SiteScope Alerts User Interface on page 1414

SiteScope Alerts Overview

SiteScope alerts are notification actions that are triggered when the conditions for the alert definition are detected. Normally, you use an alert to send some notification of an event or change of status in some element or system in your infrastructure. For example, an alert can be triggered when a SiteScope monitor detects a change from Good to Error indicating that the monitored system has stopped responding.


An alert definition contains settings that tell SiteScope what monitors can trigger the alert, what condition to watch for, and what information to send. The type of action is set by the alert type. For example, you can create an alert that includes instructions for SiteScope to send the specific server address and error code to your pager or e-mail when an error condition is detected on a particular system. You can also have SiteScope respond to problems by automatically initiating recovery or action scripts with Script Alert. For example, you can configure a Script Alert to run a script to restart a server if a monitor detects that a system is no longer responding and CPU utilization has reached 100%. For details on the alert types, see “Types of Alert Actions” on page 1438.

SiteScope alerts can be configured in several ways. Alerts can be associated explicitly with one or more individual monitors, with one or more groups of monitors, a combination of monitors and groups, or globally for all monitors on a particular installation of SiteScope. Global and group-wise alerting is generally the most efficient but may not provide the needed control. You can use the **Filter Settings** function on each alert definition page to create filter criteria to control global and group alerts to more

specific criteria. Filter criteria can be used to restrict the alert to only monitors of a certain type, that contain a certain text string or other filter criteria. For example, creating a global alert with a filter criteria for CPU Monitor creates an alert that is only triggered for CPU monitor types. For details on how to configure alerts, see “SiteScope Alerts - Add/Edit Alert” on page 1415.

Alert Associations and Considerations

The table below shows an overview of the different alert associations and considerations.

Alert Class	Description
Global Alerts	<p>Alerts that are triggered when any monitor on a given SiteScope reports the category status defined for the alert.</p> <p>New groups and monitors added after the alert definition is created are automatically associated with the alert.</p> <p>The following display is an example of a global alert associated with the SiteScope node. All monitors can trigger this alert.</p>  <p>The screenshot shows a tree view of the SiteScope node. The root node is 'SiteScope' (represented by a globe icon). Underneath it are several sub-nodes: 'Templates' (folder icon), 'Databases' (database icon), 'internal_email' (document icon), 'Network' (network icon), 'Web_Sales_Process' (document icon), 'WebServers' (server icon), 'Preferences' (gear icon), 'Health' (heart icon), 'Global Alert on All' (warning icon), and 'Tools' (toolbox icon). Each sub-node has a small square icon to its left, with a plus sign indicating it is expanded.</p> <p>Note: It is not recommended to create a global alert because the alert can potentially be triggered by every group and monitor within SiteScope.</p>

Alert Class	Description
<p>Group Alerts</p>	<p>Alerts that are triggered when any monitor within the associated group or groups reports the category status defined for the alert.</p> <p>The following is an example of a group alert. Any monitor or subgroup within the group WebServers can trigger this alert.</p> <pre data-bbox="654 460 906 555"> └─ WebServers └─ External └─ Internal └─ Webservers Alert </pre> <p>New subgroups and monitors added within the associated group or groups after the alert definition is created are automatically associated with the alert.</p>
<p>Individual Monitor Alerts</p>	<p>Alerts that are triggered when any associated monitor reports the category status defined for the alert.</p> <p>The following is an example of an individual monitor alert. Only the associated monitor can trigger this alert.</p> <pre data-bbox="654 954 978 1058"> └─ Network └─ SiteScope Network Interface └─ SiteScope interface traffic └─ Ping DHCP server </pre> <p>New monitors added after the alert definition is created are not automatically associated with the alert but can be added by editing the alert definition.</p>

You can create as many SiteScope alert definitions as you want. It is recommended however, that you plan and consolidate alerts to keep the number of alert definitions to a minimum. This facilitates alert administration and helps reduce redundant alert messages or actions.

Creating Alert Actions

When you create an alert scheme in SiteScope, you create alert actions to be triggered when the alert conditions are met. You create alert actions using the Alert Action Wizard. While in the wizard, you determine the following:

- ▶ The type of alert action. For a detailed list of available alert actions, see “Types of Alert Actions” on page 1438.
- ▶ The settings for the type of alert being sent. For example, you can define the recipients and their addresses for an e-mail alert action.
- ▶ The status condition that triggers the alert. For example, you can instruct SiteScope to trigger an alert action when a monitor’s status changes to error or unavailable.
- ▶ The trigger settings that determine when the alert is triggered and when it is sent. For details, see “Understanding When SiteScope Alerts Are Sent” on page 1390.

You can create multiple alert actions for an alert scheme. For example, you can create an alert action to send a sound alert and another alert action to send an e-mail alert. Both are sent when the alert is triggered. You can also set different schedules for the different actions within the same alert definition. For example, you can schedule an e-mail alert action to be sent during regular working hours and an SMS alert action for evening and night hours. Both are triggered by the same change in condition but are sent at different times, depending on when the alert is triggered.

You can also make one alert action dependent on another alert action. This enables you to instruct SiteScope to send one type of alert when the trigger condition is first met and send another type of alert only when the first type of alert has been sent a number of times.

Creating alert actions for an alert enables you to copy those alert actions into other monitors or groups for use by other alerts. To use alert actions for other alerts, you must copy the alert and paste it into another monitor or group. All the alert actions for the alert are copied into the new alert. You can then edit the alert to be triggered for the new target monitor or group.










For details on working with the Alert Action Wizard, see “Alert Actions Wizard - Action Type Page” on page 1421.

Understanding When SiteScope Alerts Are Sent

SiteScope triggers the alert as soon as any monitor it is associated with matches the alert trigger condition. The Trigger Settings options of the Alert Action Wizard enable you to control when alerts are actually sent in relation to when a given condition is detected. For example, you can choose to have SiteScope send an alert only after an error condition persists for a specific interval corresponding to a given number of monitor runs. This is useful for monitors that run frequently that monitor dynamic, frequently changing environment parameters. In some cases, a single error condition may not warrant any intervention. For details about configuring trigger settings, see “Trigger Settings Page” on page 1435.

The following examples illustrate how different alert configurations send alerts after the error condition has persisted for more than one monitor run. It is important to note that the sample interval corresponds to how often the monitor is run. If a monitor runs every fifteen seconds and the alert is set to be sent after the third error reading, the alert is sent 30 seconds after the error was detected. If the monitor run interval is once every hour with the same alert setup, the alert is not sent until 2 hours later.

Example 1a. An alert is sent for each time monitor is in error after condition persists for at least three monitor runs. Compare this with Example 1b below.

Alert setup	Always, after the condition has occurred at least 3 times								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=3 alert!	c=4 alert!	c=5 alert!	c=0	c=1	c=2










Example 1b. An alert is sent for each time monitor is in error after condition persists for at least three monitor runs. Shows how the count is reset when the monitor returns one non-error reading between consecutive error readings. Compare this with Example 1a above.

Alert setup	Always, after the condition has occurred at least 3 times								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=0	c=1	c=2	c=3 alert!	c=0	c=0










Example 2. An alert is sent only once if monitor is in error for at least three monitor runs, regardless of how long the error is returned thereafter.

Alert setup	Once, after the condition has occurred exactly 3 times								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=3 alert!	c=4	c=5	c=6	c=7	c=8

Example 3a. An alert is sent on the fifth time monitor is in error and for every third consecutive error reading thereafter. Compare this with Example 3b below.

Alert setup	Initially, after 5 times, and repeat every 3 times								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=3	c=4	c=5 alert!	c=6	c=7	c=8 alert!










Example 3b. An alert is sent on the third time monitor is in error and for every fifth consecutive error reading thereafter. Compare this with Example 3a above.

Alert setup	Initially, after 3 times, and repeat every 5 times								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=3 alert!	c=4	c=5	c=6	c=7	c=8 alert!

Because you can create multiple alerts and associate more than one alert to a monitor, you can tell SiteScope to take more than one action for a given situation. For example, you can create one alert that tells SiteScope to page you whenever any monitor returns an error status. You can then create another alert that tells SiteScope to run a script file to delete files in the /tmp directory on your server if your Disk Space Monitor returns an error. If your disk becomes too full, SiteScope would page you because of the first alert definition and would run the script to delete files in the /tmp directory because of the second alert definition.

SiteScope alerts are generated when there is a change in state for a monitor reading. Thus you can set an alert for OK or warning conditions as well as error conditions. One way to take advantage of this is to add two alerts, one alert on error, and one alert on OK. Set alerts to be sent after the condition is detected 3 time. For the OK alert, check the box marked **Only alert if monitor was previously in error at least 3 times**. This prevents unmatched OK alerts, such as when a monitor was disabled for any reason (manually, by schedule, or by **depends on**) and then starts up again. This can also be used so that an OK alert is only sent after a corresponding error alert was sent. With these two alerts, you get a page when a link or service goes down (monitor detects change from OK to error), and another when it comes back up (monitor detecting change from error to OK). The following diagram is an example of using two alerts with a monitor.

Example 4. An Alert on error sent once for error after condition persists for at least three monitor runs. Alert on OK sent once for good status after at least one error or warning interval.

Alert on Error Setup	On Error	Once, after the condition has occurred exactly 3 times							
Alert on OK Setup	On OK	Once, after the condition has occurred exactly 1 times and Only alert if monitor was previously in error at least 3 times							
Sample Interval	0	1	2	3	4	5	6	7	8
Status									
Count	c=0	c=1	c=2	c=3 alert!	c=4	c=5	c=6	c=7	c=1 alert!

Once the monitor's status changes, the relevant status count is reset to zero.

Customizing Alert Templates

SiteScope uses templates when generating alert messages and reports. In most cases, you select the template you want to use in the Alert page when you create an alert. You can customize the existing templates or create your own by making a copy of an existing template. You customize the alert templates by adding or removing text, by adding property variables as listed in the Template Properties section, or changing the order of text or property variables that are included in the template.

Note: It is recommended that you create custom alert templates using new filenames. If you modify one of the default templates provided with SiteScope and save the changes to the same file, the changes that you make may be lost if you reinstall SiteScope or upgrade the SiteScope installation.

To make a custom alert template available to SiteScope, you must save any customized alert templates into the directory containing the templates for the applicable alert type. For the list of directory names containing SiteScope alert templates you can copy and customize, see “SiteScope Alert Templates Directory” on page 1414.

The templates in these groups are text files that include property variable markers. You use a text editor to create or modify these templates. The new templates saved into the directories shown become available to the applicable alert on the Alert page.

For details on customizing alert template settings, see “Customize an Alert’s Message Content” on page 1411 and “Customize Alert Template Tag Styles” on page 1413.

Example - Default Template Used for the E-mail Alert

The following is an example of the default template used for the E-mail Alert. The names that appear within <brackets> are property variable markers. When the alert is generated, SiteScope replaces these markers with the corresponding values of the variable for the monitor or monitor group that has triggered the alert.

```
This alert is from SiteScope at <SiteScopeURL>
Monitor: <groupID>:<name>
Group: <group>
Status: <state>
Sample #: <sample>
Time: <time>
-----Detail -----
<mainParameters>
<mainStateProperties>
```

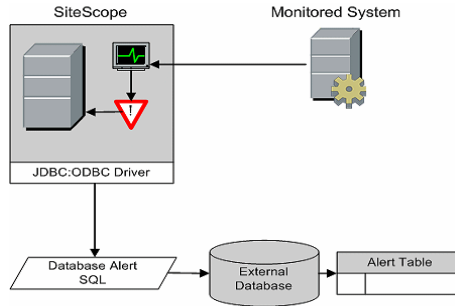
You add or edit the text portions of the template. For example, you could change the first line of the template above to read:

```
A Web monitoring alert was generated by the SiteScope installation found at
<SiteScopeURL>
```

Working with Database Alerts

Database alerts can forward system fault data and other status information to any SQL-compliant database.

The following diagram illustrates the Database alert.



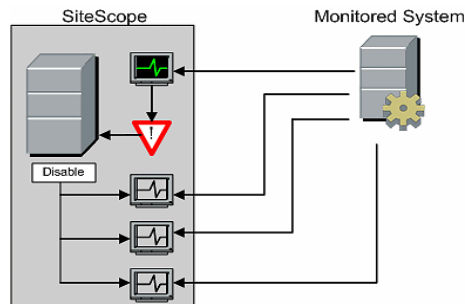
You need the following to be able to use the Database alert type:

- ▶ Access to a SQL compliant database.
- ▶ The applicable database connection URL which the SiteScope server uses to connect to the database.
- ▶ Installation of the applicable database middleware driver that the SiteScope application uses to communicate with the database on the SiteScope server.
- ▶ Database tables that have been created and structured to match the corresponding SQL statement that SiteScope uses to enter the alert into the database.

Working with Disable or Enable Monitor Alerts

Disable or Enable Monitor alerts can turn off and turn on the triggering of alerts for monitors. This is useful for times when server maintenance or other activities are being performed that would logically result in errors for some monitors and cause unnecessary alerts to be generated.

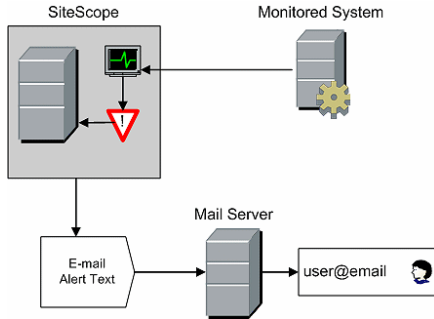
The following diagram illustrates an example of this alert type used to disable several monitors based on the condition reported to one monitor.



This alert type provides a functionality similar to the **Depends On** function for building group dependencies between monitors and monitor groups. One important difference is that monitors disabled by this type of alert are not automatically re-enabled when the status of the subject monitor or group changes back to the original state. You can create one alert with an **Alert Category** of **Error** that disables monitors. You can then create a second alert with an **Alert Category** of **Good** that enables the same monitors.

Working with E-Mail Alerts

E-mail alerts send event notifications from SiteScope to a designated e-mail address as seen in the following diagram.



You need the following to be able to use the E-mail alert type:

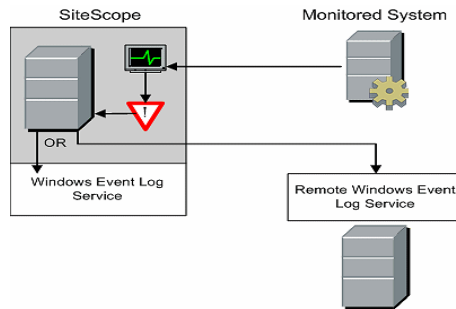
- ▶ Access to an active e-mail server
- ▶ One or more e-mail accounts that can receive the e-mail alerts
- ▶ SiteScope E-mail Preferences set to work with the external e-mail server

For more information on configuring SiteScope e-mail recipients, see “E-mail Preferences” on page 222.

Working with Log Event Alerts

Log Event alerts can be used to extend the types of events that are logged to a Windows Application Event Log. This provides a way to forward event data to log query systems that may not normally be logged by the Windows operating system.

The following diagram illustrates the Log Event alert.



You need the following to be able to use the Log Event alert type:

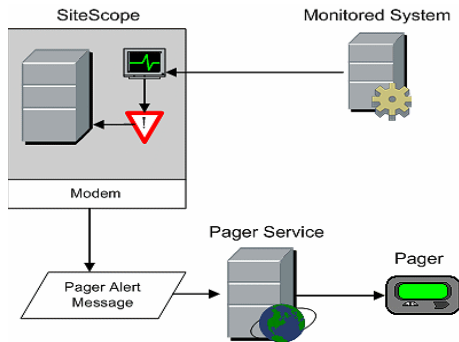
- Access to the Windows Event Log service. By default, this is the Event Log on the machine where SiteScope is running. The alert definition can be configured to send log events to another server.
- SiteScope running on a Microsoft Windows platform.

Important: If you are using SiteScope's Microsoft Windows Event Log Monitor, you must use care when using the Log Event alert type because it is possible to create an endless loop condition that can fill your Event log file. This can happen when a Microsoft Windows Event Log Monitor detects an event that triggers a Log Event alert, which in turn puts a new event into the event log, which the Event Log Monitor then detects, and then triggers the Log Event alert, and so forth. To avoid this, Log Event alert types should not be associated with Microsoft Windows Event Log Monitors.

Working with Pager Alerts

Pager alerts can be used to send event notification to electronic pagers. This is particularly useful when access to e-mail may not be available. Depending on the type of pager you use and the capabilities of the pager service, you can configure the Pager Alert to send a pager message with an abbreviated description of the problem or detected condition.

The following diagram illustrates the Pager alert.



You need the following to be able to use the Pager alert type:

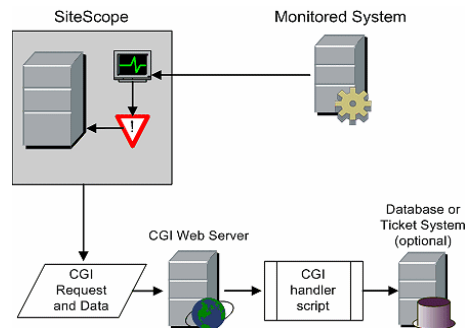
- ▶ Access to an active pager service
- ▶ A modem which the SiteScope server can use to connect to the pager service
- ▶ One or more pagers that can receive the pager alerts
- ▶ SiteScope Pager Preferences set to work with the modem and pager service

For more information on configuring SiteScope to use pager alerts, see “Pager Preferences” on page 222.

Working with Post Alerts

Post alert use the Common Gateway Interface protocol to forward POST data to a CGI enabled program. This can be used to forward event data to CGI script on another server that is a front-end for a trouble ticket system or reporting database. This alert type also provides a way of sending alert information through a firewall using HTTP or HTTPS without having to make other security changes.

The following diagram illustrates the Post alert.



You need the following to be able to use the Post alert type:

- HTTP access between the SiteScope server and the server running the CGI script or server
- Format and syntax of the CGI POST request to the applicable CGI script or server

Working with Script Alerts

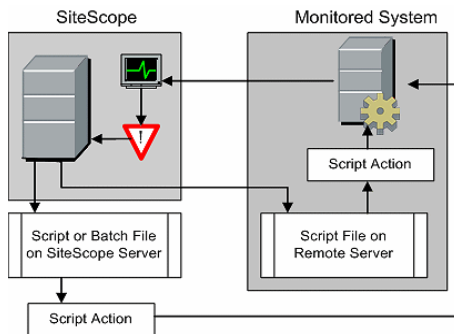
Script alerts can automatically initiate recovery scripts. You can configure a Script alert to run a command to restart a server or a service.

The most important components of Script Alerts are:

- ▶ The script definition itself.
- ▶ The monitor or monitors that are assigned to trigger the alert.
- ▶ The script to be run by the alert.

The alert message template and resulting alert message file may also need to be considered depending what the script needs to do. You can use a script template, together with the **Parameters** setting to pass data to your script.

The following diagram illustrates the general concept of the script alert for both a local script and a script on a remote host.



The script alert definition or instance and the monitor or monitors that trigger the alert are handled as with other alerts or monitors in SiteScope. For example, you may create a monitor to watch a Web server running on a remote UNIX server. You can create a Script Alert associated with that monitor that runs a script to kill and restart the Web server process if the monitor reports an error.

Managing Script Files

Creating the script file to be called or run by the Script Alert definition is another key step in using this automation capability in SiteScope. The specific commands and actions taken by the script are up to you. The script file should be written as a plain text file compatible with the operating system where the script is to be run. This may be the same server where SiteScope is running or it may be on a remote machine to which SiteScope has access.

To run a script on the machine where SiteScope is running, the script file must be saved in the **<SiteScope root_directory>\scripts** directory on the SiteScope machine where the Script Alert is defined.

To run a script on a remote machine, you must save the script in a directory called **\scripts** in the home directory tree for the user account that SiteScope has execute permissions for on the remote machine.

The current execution directory when a script is run is **<SiteScope root directory>\classes** and not the **<SiteScope root directory>\scripts** directory. For commands run by the script itself, the relative execution directory is **<SiteScope root directory>\classes**. Use full paths for any other file system commands or programs called by your script so that you do not need to worry about the current directory. Also, the server system environment variables may not have been set up for the script execution. This is another reason to use full paths for executables called by the script. If a script works when you run it from the command line but not from SiteScope, then you must determine what the error is.

Passing Data to a Script

SiteScope passes a number of parameters to the script as command line arguments. You can use this option to pass data to a script that can be used to modify a script's action. This adds versatility to the Script Alert. By default, a SiteScope Script Alert passes seven command line arguments to a script. These are:

- The path of the scripts directory.
- The name of the monitor that caused the alert.
- The current status of the monitor.
- The path to the Alert Message File.
- The ID code of the monitor.
- The group the monitor is in.
- Any additional parameters specified on the **Parameters** text box in the alert form.

Two of these default arguments allows the script to access even more data. One is the Alert Message File and the other is the **Parameters** text box. The Alert Message File is a temporary text file created by SiteScope based on the alert template chosen for the Script Alert instance. Depending on the template you create or use, the Alert Message File may contain custom information as well as data specific to the monitor that triggered the alert. By passing the path to the Alert Message File to the script, you can have the script access this data.

You use the Parameters text box to specify individual monitor parameter data to be passed to the script. You can include multiple parameters by separating the parameters with spaces. This effectively allows you to increase the total number of parameters passed to the script.

The path of the scripts directory can be useful in setting a execution path to another program as well as setting a directory path for any output written by the script.

For more information and examples of passing parameters and data to scripts, see “Writing Scripts for Script Alerts” on page 1523.

Running Different Types of Scripts

In previous versions of SiteScope, it was not possible to run non-batch scripts, for example VBScript or Perl scripts, without wrapping them into a batch file. In SiteScope 9.50, you can do the following:

- ▶ You can see scripts with any extensions that you specify in the `_scriptExtensions` property of the **master.config** file. For example, to see **.pl**, **.py**, or **.php** scripts, use the following format:
`_scriptMonitorExtensions=.pl;.py;.php`
- ▶ You can run script interpreters with script extensions by specifying the `_scriptInterpreters` property of the **master.config** file as follows:
`_scriptInterpreters=pl=c:/perl/perl.exe;py=c:/python/python.exe;php=c:/php/php.exe`

Troubleshooting Scripts

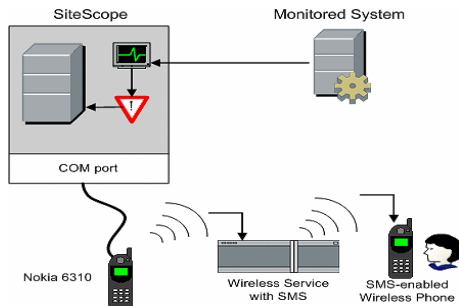
- ▶ The scripts are run with the permissions of the account used by the SiteScope service. Some scripts may need extra permissions and you must use the Services control panel to change the login account for SiteScope and then stop and start SiteScope. For example, scripts that restart services or reboot remote machines or scripts that copy protected files.
- ▶ Because the script is run by the SiteScope service, anything done as part of your login may not have occurred in the script. For example, you can not rely on mapped drives, environment variables, or other login script items. In addition, it cannot receive any interactive input from a keyboard or other input device. Any script action or command that requires a user confirmation or input would cause the script to hang. Do not include any interactive commands requiring a user action as part of the script. Also, opening a WIN32 application (for example, Notepad) also causes the script to hang because it is waiting for the user to exit or close the application before continuing with the script execution.
- ▶ If there are quotation marks in the Script Alerts status summary, SiteScope doubles the quotation marks in the Script Alert results. You should take this into account when defining a content match filter.

Working with SMS Alerts

SMS alerts are designed to transmit the name of the SiteScope monitor that has reported an event condition and the status of that monitor as the content of the message. It is an alternative to the Pager alert for communicating event notifications to mobile users without using e-mail.

Note: At present, the SMS alert can only be sent from SiteScope by using the hardware specified in this section. For alternative ways of sending SMS messages using SiteScope, see the HP Software Self-solve knowledge base (<http://h20230.www2.hp.com/selfsolve/documents>). To enter the knowledge base, you must log in with your HP Passport ID.

The following diagram illustrates the SMS Alert.



You need the following to be able to use the SMS alert type:

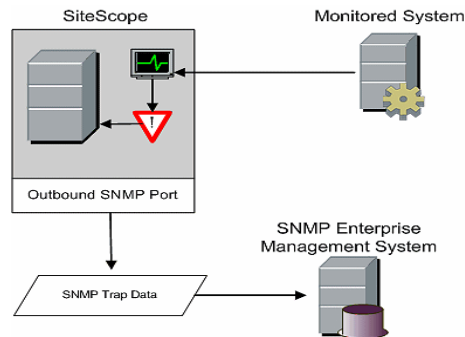
- ▶ An available serial communications port on the SiteScope machine that is sending the SMS alerts.
- ▶ A serial-to-wireless device interface cable, RS-232 Adapter Cable Nokia DLR-3P to connect the wireless transmitting device to the machine where SiteScope is running.
- ▶ An SMS-enabled wireless device connected to the SiteScope machine that is sending the alerts (that is, the Nokia 6310 phone using the interface cable).
- ▶ The necessary software to enable the SMS Alert (normally included with SiteScope 7.6c1 and later).

Note: Make sure that you do not have Nokia Data Suite, Palm Hot Sync, or any PDA software running on the server where SiteScope is running. These programs can bind the COM ports and prevent the dialer from working correctly.

Working with SNMP Trap Alerts

SNMP Trap alerts forward event data from any type of SiteScope monitor to an SNMP enabled host or management system. This means that SiteScope can be used to monitor and report events for applications and systems that do not have their own SNMP agent. For example, this can be used to send measurement data from a SiteScope Microsoft Windows Performance Counter based monitor type or a URL monitor in the form of an SNMP trap.

The following diagram illustrates the SNMP Trap Alert.



You need the following to be able to use the SNMP trap alert type:

- ▶ Access to the applicable SNMP network ports
- ▶ SiteScope SNMP Preferences set to work with the applicable SNMP management console

For more information on configuring SiteScope to use SNMP alerts, see “SNMP Trap Preferences” on page 223.

Working with Sound Alerts

Sound alerts play a sound or audio file on the machine on which SiteScope is running when an alert is generated. The alert is effective only if the SiteScope server is in an area regularly occupied by support staff and the server is equipped with a sound card capable of processing the associated sound file.

Alternatively, SiteScope can be configured to embed an alert audio file into the Web pages served by SiteScope. This audio file is included with any SiteScope page that includes an error status for any monitor, such as the main panel or group detail pages. While this allows audio notification to all SiteScope clients through the user interface, it is not a true SiteScope alert and thus does not enable the same configuration options as the Sound Alert. For information about how to configure SiteScope to embed audio files for error notification, refer to the HP Software Self-solve knowledge base (h20230.www2.hp.com/selfsolve/documents). To enter the knowledge base, you must log in using your HP Passport ID.

Configure an Alert

This task describes the steps involved in configuring an alert definition.

This task includes the following steps:

- “Create an Alert” on page 1409
- “Test the Alert” on page 1410
- “Customize an Alert’s Message Content” on page 1410
- “Customize Alert Template Tag Styles” on page 1413
- “Results” on page 1410

1 Create an Alert

You can create a new alert or copy an existing alert into any group or monitor container in the SiteScope tree.

- **Create a new Alert.** Right-click the container to which you want to associate the alert, and click **New Alert**. Type a name for the alert, and click **Add Action** to start the Alert Action wizard. For details on the user interface, see “SiteScope Alerts - Add/Edit Alert” on page 1415.
- **Copy an Alert Definition.** Select the alert you want to copy, and paste it into the desired group or monitor container. The alert target automatically changes to the group or monitor into which the alert is copied.

Important: If you copy an alert definition from one group container to another, the **Alert Targets** for the pasted alert are automatically reset to include all of the children of the container into which the alert is pasted. After pasting an alert, edit the alert definition properties to be sure that the assigned **Alert Targets** are appropriate to the new alert context and your overall alerting plan.

2 Test the Alert

Select the alert in the monitor tree and click **Test**. Select the monitor instance you want to test and click **Test**. The Test Preferences dialog box opens with information about the alert test.

Note: The monitor you select does not have to be reporting the same status category that is selected to trigger the alert to test the alert. For example, the monitor does not have to currently be reporting an error to test an alert that is triggered by error conditions.


3 Customize an Alert's Message Content

Customize SiteScope alert templates to alter the content and format of alert messages. For details on how to perform this task, see “Customize an Alert's Message Content” on page 1411.

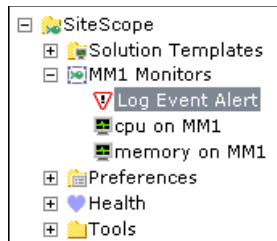
4 Customize Alert Template Tag Styles

Customize SiteScope alert templates tag styles if you have a parser that needs a specific delimiter or to change the bracket delimiters used to identify variables. For details on how to perform this task, see “Customize Alert Template Tag Styles” on page 1413.

5 Results

An alert is added to the specified container in the monitor tree (indicated by the  icon). The alerts icon is also displayed in SiteScope Dashboard next to each group or monitor that has one or more configured alerts.

Example



Customize an Alert's Message Content

This task describes how to customize SiteScope alert templates to alter the content and format of alert messages.

Note: Only alerts that have a template or that have message parameters can be customized.

To customize an alert's message content:

- 1 Open a text editor that has access to the alert template directories on the SiteScope machine.
- 2 Open one of the existing template files in the template directory of the alert type you want to customize.
- 3 Make changes to the template. Depending on the alert type, you can add or remove text, change the order of text or property variables, or add other property variables. To add specific properties, add the applicable property variable name between < > bracket pairs to the template.
- 4 Save the changes to a unique filename within the directory for the applicable alert type.

Example

For example, you can change the SNMP Alert message from displaying the SNMP monitor's status to displaying a list of counters that are in Error state along with their values. This causes the message to only contain counters that breached the Error threshold and to omit all other counters.

In the <SiteScope root dir>\templates.SNMP directory, open the **Default** template file. The file contains the line:

```
SiteScope\<group>\<name>\<sample>\<state>\
```

Replace the string <state> with the string <errorOnly>. The angle brackets (<,>) must remain around the text.

Note: If you want to display a list of counters that are in Warning state, replace the string `<state>` with the string `<warningOnly>`.

Edit `<SiteScope root dir>\groups\master.config` file and add the line `_errorOnlyDelimiter=,`

with other similar error definitions.

In this example, the delimiter is a comma (,), but you can also use a space (" ") or a tab (\t). The added line in `master.config` looks something like:

```
_errorInsertHTML=  
_errorOnlyDelimiter=  
_errorOnlyNewlineFormat=true
```

Note:

- If you used the string `<warningOnly>`, you must use the string `_warningOnlyDelimiter=<delimiter>` in `master.config`.
 - If no `_errorOnlyDelimiter` is defined in `master.config`, the default delimiter is a space (" ").
-

Customize Alert Template Tag Styles

This task describes how to change the delimiter between items in the list if, for example, you have a parser that processes alert messages and needs a specific delimiter. You can also change the bracket delimiters that are used to identify variables. This is useful if you want the message read by XML and a variable replaced by an XML string.

To change the bracket delimiter:

1 Edit the template file for which you want to change the bracket delimiter. For example: <SiteScope root directory>\templates.mail\.

2 Use a text editor to add the following lines to the top of the relevant file:

```
[Tag-Style:{}]
```

Type the characters after the colon (in this example {}) that should be used as the delimiter instead of the html brackets (<>).

3 Edit the relevant variables to be bracketed by the new characters defined in the Tag-Style string. For example: {state}.

SiteScope Alert Templates Directory

The following is a list of the directory names containing SiteScope alert templates you can copy and customize.

Template Group	Description	Location
Event Log	Format and content of data written into event logs	<SiteScope root directory>\ templates.eventlog
History	Format and content of e-mail messages that notify recipients that a report has been generated	<SiteScope root directory>\ templates.history
E-Mail	Format and content of alert messages sent by e-mail	<SiteScope root directory>\ templates.mail
Template	Group Description Location Pager Format and content of pager alerts	<SiteScope root directory>\ templates.page
Post	Format and content of messages submitted to a CGI script by a Post alert	<SiteScope root directory>\ templates.post
Script	Format and content of messages sent to a script when a script alert is triggered	<SiteScope root directory>\ templates.script
SNMP	Format and content of messages sent by SNMP when a SNMP trap is triggered	<SiteScope root directory>\ templates.snmp

SiteScope Alerts User Interface

This section describes:

- ▶ SiteScope Alerts - Add/Edit Alert on page 1415
- ▶ Alert Actions Wizard - Action Type Page on page 1421
- ▶ Types of Alert Actions on page 1438





SiteScope Alerts - Add/Edit Alert

Description	Enables you to define alerts for a SiteScope, a group, or a monitor. To access: Right-click the SiteScope, group, or monitor for the alert. Select New Alert .
Important Information	Any box with a red asterisk (*) must be filled or the wizard does not proceed to the next step.
Included in Tasks	“Configure an Alert” on page 1409
Useful Links	“SiteScope Alerts Overview” on page 1386

The following areas are found throughout the New Alert page:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Deploys the Alert Action wizard to define an action to be done when an alert is triggered.
	Edits the alert action. This appears only after an alert action has been defined.
	Duplicates the alert action. This appears only after an alert action has been defined.
	Deletes the alert action. It does not disable the associated monitors. This appears only after an alert action has been defined.

GUI Element (A-Z)	Description
<p>Alert Actions</p>	<p>The columns in this table are defined in the Alert Action wizard:</p> <ul style="list-style-type: none"> ▶ Name. The name given to the alert action in the Alert Actions Wizard - Action Type Page. ▶ Category. The category selected in the Trigger Page that triggers the alert action. ▶ When. The schedule selected in the Trigger Settings Page for when the alerts are sent. ▶ Schedule. The daily/weekly schedule selected in the Action Type Settings Page. <p>For a complete description of each action type, see “Types of Alert Actions” on page 1438.</p>
<p>Alert Name</p>	<p>Enter a text description for this alert definition. This name is used to identify this alert definition in the product display.</p>
<p>Alert Targets</p>	<p>Use the context menu tree to the right of this item to select the groups and/or monitors to trigger this alert. The context menu includes the currently selected object and all of the child objects. Check the box beside the current object to associate this alert with all objects within this object. Check one or more individual object to associate this alert definition to the selected objects.</p> <p>Alternatively, you may select the SiteScope root and then define an alert filter rule in the Filters Settings to limit alerting to those objects that match the conditions set in the filter.</p>

Enable/Disable Alert

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Disable Description	<p>(Optional) Description of the purpose of the disable operation. You can include HTML tags such as the
, <HR>, and tags to control display format and style.</p> <p>Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> ▶ Tags: script, object, param, frame, iframe. ▶ Any tag that contains an attribute starting with on is declined. For example, onhover. ▶ Any attribute with javascript as its value.

GUI Element (A-Z)	Description
Disable This Alert	<p>Use to manually control the generation of alerts. This can be useful when the systems being monitored are off-line for maintenance or if the recipient of the alerts is unavailable for a period of time.</p> <ul style="list-style-type: none"> ➤ Enable Alert. Overrides any disable action on the alert and enables the alert for execution based on the conditions defined. ➤ Disable Alert Indefinitely. Prevents SiteScope from executing the alert action even if the alert condition is met until this radio button is cleared and the alert definition is updated. <ul style="list-style-type: none"> Note: Use of this option may result in loss of expected alert capability if the alert is disabled to accommodate a temporary condition. It is important to review this status later to manually enable the alert definition, as needed. ➤ Disable Alerts for the Next Time Period. Prevents the execution of the alert action for the time period you type, even if the alert condition is met. The alerts are disabled immediately and re-enabled when the time period expires. <ul style="list-style-type: none"> Default value: 10 minutes ➤ Disable on a One-Time Schedule from Time1 to Time2. Prevents SiteScope from executing the alert action for the time period indicated, even if the conditions are met. The alerts are disabled at the beginning of the time period and re-enabled after the time period expires.

Filter Settings

Description	<p>Creates filter conditions to limit the alert action to only those monitors that match the criteria you entered.</p> <p>You can define alerts for a large number of monitors and then apply a filter so that only certain monitors within the selected list actually trigger the alert. This can simplify the creation of alert definitions and alert management.</p> <p>To access:</p> <p>Right-click the SiteScope, group, or monitor for the alert. Select New Alert.</p>
Important Information	<p>To disable alert filtering, clear the applicable fields and update the alert definition.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Monitor Type Match	<p>Limits the alert action to a monitor type from the set of monitors associated with this alert. You choose multiple types.</p>
Name Match	<p>Suppresses the alert for all associated groups or monitors except those with a specific text appearing as part of their name.</p> <ul style="list-style-type: none"> ▶ Type a regular expression in this text box to match a name string pattern. For details, see “Regular Expressions Overview” on page 1494. ▶ Type all or part of the monitor name string you want to use as a filter criteria. For example, entering the string URL: limits this alert to monitors whose name contains the string URL:. <p>Note: The match is case sensitive.</p>

GUI Element (A-Z)	Description
Status Match	<p>Suppresses the alert for all associated monitors except those returning a specific status text.</p> <ul style="list-style-type: none"> ▶ Type a string that you expect to appear in the status text for the monitor you want to trigger this alert. For example, if you type the text <code>timeout</code> in this box, an alert is only triggered by a monitor associated with this alert that also has a status of <code>timeout</code>. ▶ Type a regular expression in this text box to match a status string pattern. For details, see “Regular Expressions Overview” on page 1494. <p>Note: The match is case sensitive.</p>

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Description	<p>You can type free text to give a description to this alert. This description does not appear in any other context. It appears only when editing the alert. You can include HTML tags such as the <code>
</code>, <code><HR></code>, and <code></code> tags to control display format and style.</p> <p>Note: HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> ▶ Tags: script, object, param, frame, iframe. ▶ Any tag that contains an attribute starting with on is declined. For example, <code>onhover</code>. ▶ Any attribute with javascript as its value.

Category Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Assigned Categories	For details, see “Working with Categories” on page 197.

Alert Actions Wizard - Action Type Page

Description	<p>The first page in the Alert Action wizard. Use the Alert Action wizard to configure actions to be taken when an alert is triggered.</p> <p>To access:</p> <p>In the Main Settings section of the Add Alert page, click Add Action.</p> <p>Use the Action Type Page to define the SiteScope Alert name and type.</p>
Important Information	<p>You can select only one type of alert at a time.</p> <p>If you are editing an alert, you cannot change the action type, the action to be done when an alert is triggered. For example, if an alert’s action type was E-mail, you cannot change it to SMS. You must delete the alert and create an alert whose action type is SMS.</p>
Included in Tasks	“Configure an Alert” on page 1409
Wizard Map	The Alert wizard includes: Alert Actions Wizard - Action Type Page > Action Type Settings Page > Trigger Page > Trigger Settings Page.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Action Name	<p>The name given to the action to be done when the alert is triggered. It is not the name of the alert.</p> <p>For example, if you want to configure an alert to check the CPU of all Solaris machines and send an SMS message when some alert is triggered, you could define the alert name in Main Settings to be Solaris_CPU and the action name to be send_sms.</p>
Database	<p>Sends an alert message with a description of the problem as a record to a SQL database.</p> <p>You can then use database tools to provide more advanced recording, sorting, and reporting on your monitoring data.</p>
Disable or Enable Monitors	<p>Automatically enables or disables monitors or monitor groups based on a change of state in another monitor.</p> <p>Note: This action is not available when creating a template alert.</p>
E-Mail	<p>Sends an e-mail message to one or more e-mail addresses with a description of condition that triggered the alert.</p>
Log Event	<p>Logs events to the Microsoft Windows Event Log.</p> <p>Entries in the event log can then be viewed with the Event Viewer and/or used by other software utilities that perform centralized alerting from the event log.</p>
Pager	<p>Sends a message to a pager to signal that SiteScope has detected a particular condition.</p>
Post	<p>Submits a CGI POST message to a CGI script, servlet, or other CGI-enabled program. The message contains a description of a monitor condition.</p>

GUI Element (A-Z)	Description
Script	<p>SiteScope can run scripts or batch files when the alert condition is met. The script or batch file can run a system command or a program in any language that can be called from a command line entry.</p> <p>You can use this alert to run recovery scripts that automatically respond to critical conditions or failures (for example, to reboot a server or to copy files).</p>
SMS	Sends a short text message using the Short Message Service (SMS) to an SMS-enabled mobile phone or wireless device.
SNMP Trap	Sends an SNMP trap to an SNMP management console or host. This enables SNMP reporting of system parameters not normally supported by SNMP agents.
Sound	Plays a sound or audio file on the machine on which SiteScope is running when an event has been detected

Action Type Settings Page

Description	Use the Action Type Settings page to define the settings that are specific to the alert type.
Important Information	The settings vary according to the type of alert action you selected in the Alert Actions Wizard - Action Type Page.
Wizard Map	The Alert Action wizard includes: Alert Actions Wizard - Action Type Page > Action Type Settings Page > Trigger Page > Trigger Settings Page.

Database Alert Properties

The following properties must be entered for the **database** alert:

GUI Element (A-Z)	Description
Backup Database Connection URL	<p>If a backup database for SiteScope alert logging is required, this is the URL to the backup database connection to use if the main database connection fails.</p> <p>Example: If the ODBC connection for the backup database connection is called <code>testdb2</code>, the URL would be <code>jdbc:odbc:testdb2</code>.</p>
Database Connection URL	<p>The URL to a database connection.</p> <p>Example: In Windows NT, use the ODBC Data Sources manager in the Settings control panel to create a connection called <code>test</code> and then type <code>jdbc:odbc:test</code> as the database connection URL.</p> <p>Note for using Windows Authentication: If you want to access the database using Windows authentication, type <code>jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>;AuthenticationMethod=type2</code> as the connection URL, and <code>com.mercury.jdbc.sqlserver.SQLServerDriver</code> as your database driver. Leave the Database User name and Database Password boxes empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.</p>
Database Driver	<p>The Java class name of the JDBC database driver.</p> <p>SiteScope uses the same database driver for both primary and backup database connections. If a custom driver is used, the driver must also be installed in the <code>SiteScope/java</code> directory. See “Database Query Monitor Overview” on page 729 for more information about setting up database drivers for SiteScope.</p> <p>Default value: <code>sun.jdbc.odbc.JdbcOdbcDriver</code></p>
Database Password	The password to connect to the database.
Database User Name	The user name to connect to the database.

GUI Element (A-Z)	Description
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. Default value: every day, all day
SQL Statement	The SQL statement used to add the alert to the database. Items enclosed in angle brackets (< and >) are replaced with fields from the monitor that triggered the alert. Default value: INSERT INTO SiteScopeAlert VALUES('<time>', '<group>', '<name>', '<state>')

Disable/Enable Monitors Alert Properties

The following properties must be entered for the **disable/enable monitors** alert:

GUI Element (A-Z)	Description
Group/Monitors Action	You can choose whether this alert action disables a monitor or enables a monitor when the alert is triggered. Default value: Disable
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. Default value: every day, all day
Targets	The groups and monitors that should be affected by the action of this alert. The list includes all groups and monitors configured for the SiteScope. You can select any group or any monitor running in any group for this alert action. Press CTRL RIGHT to select multiple items. Example: This alert action is being configured for a Disk Space monitor. An alert triggered for this monitor can disable all CPU monitors monitoring the same server.

E-Mail Alert Properties

The following properties must be entered for the **e-mail** alert:

GUI Element (A-Z)	Description
Addresses	Separate multiple e-mail addresses with a comma (,). The addresses are checked for valid syntax but not for other errors (for example, that the e-mail user exists).
Mark this action to close alert	When the status changes and the alert trigger condition is no longer true, this action closes the alert and sends a close notification by adding the word Close to the message sent. Default value: Cleared
Recipients	Type e-mail recipients who have been configured in Mail Preferences. For details, see “E-mail Preferences” on page 222.
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. You cannot edit this value. It is determined by the schedule defined for the mail recipients in preferences.
Template	A drop-down list of all templates for the e-mail alert action. In an E-mail alert action, select the ShortMail template for a shorter e-mail message. Other options enable you to choose the level of detail to include in E-mail alerts. Default value: Typical. This template includes the following values: Monitor: <groupID>:<name>; Group: <group>; Status: <state>; Sample #: <sample>; Time: <time> Note: You can add additional templates into the <SiteScope root directory>\templates.mail directory. For details on the available templates, you can open the files in this directory in a text editor to see what values are sent with each option.

Log Event Alert Properties

The following properties must be entered for the **log event** alert:

GUI Element (A-Z)	Description
Category ID	Used as the <category ID> for the event created by this alert. Default value: 0
Event ID	A number used to set the <ID> field of the event that is logged. Syntax: must be numeric. Default value: 1000
Event Source	A string used to set the <Source> field of the logged event. Syntax: must be text. Default value: SiteScope
Event Type	Default Value: the monitor status. In other words, the Event Type is Error for an Error status, Warning for Warning, and Informational for monitors reporting a status of Good.
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. Default value: every day, all day
Send To	The name of the Windows machine where the event is to be appended to the event log. Default value: localhost (the machine where SiteScope is running).
Template	A drop-down list of all templates for the log event type alert action. Default value: Default template Note: You can view the contents of the existing templates or add additional templates in <SiteScope root_directory>\templates.eventlog.

Pager Alert Properties

The following properties must be entered for the **pager** alert:

GUI Element (A-Z)	Description
Mark this action to close alert	When the status changes and the alert trigger condition is no longer true, this action closes the alert and sends a close notification by adding the word Close to the message sent. Default value: Cleared
Message	The content is determined by the type of alert you are defining: For Pager Alerts, the maximum length is 32 characters.
Pager Recipients	Type pager recipients that have been configured in Pager Preferences. For details, see “Pager Preferences” on page 222.
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. You cannot edit this value. There is a predefined schedule for pager recipients defined in preferences.
Template	A drop-down list of all templates for the pager alert action type. Default value: Default template Note: You can view the contents of the existing templates or add additional templates in the <code><SiteScope root directory>\templates.page</code> directory.

Post Alert Properties

The following properties must be entered for the **post** alert:

GUI Element (A-Z)	Description
Authorization Password	<p>This is the password for the Authorization User Name in a Post Alert.</p> <p>Alternatively, leave this entry blank and type the password in the Default Authentication Credentials section on the General Preferences page. Use this method to define common authentication credentials for use with multiple monitors.</p>
Authorization User Name	<p>This user name permits access to the URL of the CGI script in a Post Alert. Not all CGI scripts require a user name.</p> <p>Alternatively, leave this entry blank and type the user name in the Default Authentication Credentials section in the General Preferences page. Use this method to define common authentication credentials for use with multiple monitors.</p>
HTTP Proxy	<p>The domain name and port of an HTTP Proxy Server used to access the URL of the CGI script.</p>
Post to URL Form	<p>The URL of the CGI script that SiteScope should submit to the alert. For example, http://admindb.server.net/cgi-bin/error.pl.</p> <p>Syntax: You must include the string http://. There is syntax checking for a valid URL address.</p>
Proxy Server Password	<p>The user name and password to access the URL of the CGI script, if required by the proxy server.</p>
Proxy Server User Name	<p>Your proxy server must support Proxy-Authenticate.</p>

GUI Element (A-Z)	Description
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. Default value: every day, all day
Template	A drop-down list of all templates for the post alert action type. Default value: Default template Note: You can view the contents of the existing templates or add additional templates in the <SiteScope root directory>\templates.post directory.

Script Alert Properties

The following properties must be entered for the **script** alert:

GUI Element (A-Z)	Description
<p>Parameters</p>	<p>Additional monitor parameters that you can pass to your script, such as:</p> <ul style="list-style-type: none"> ▶ path of the scripts directory ▶ name of the monitor that caused the alert ▶ current status of the monitor ▶ path to the alert message file ▶ ID of the monitor ▶ monitor group <p>These parameters are sent as the seventh, eighth, ninth, and so forth, command line arguments respectively.</p> <p>The parameters available to be passed to the script are dependent on the type of monitor that triggers the alert.</p> <p>Syntax: Surround the property name variable in the properties list with angle brackets (< >). For example, to pass the server name to the script, type <_machine> in the text box. To pass more than one extra parameter, separate the parameters with a single space. This is the same way the arguments would be added on the command line.</p> <p>Default value: The Script Alert always passes the above parameters to a script as command line arguments. They do not need to be listed here.</p>
<p>Schedule</p>	<p>The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered.</p> <p>Default value: every day, all day</p>
<p>Script</p>	<p>The script to run in response to the selected condition.</p> <p>You can create as many custom scripts as you need. Place them in <SiteScope root directory>\scripts directory or the applicable scripts directory on a remote machine. SiteScope lists all files found in this directory on the selected server in the drop-down list.</p>

GUI Element (A-Z)	Description
Server	The server on which the script should be run. The scripts directory must be in the directory tree of the remote login account that allows remote scripts to be run by SiteScope.
Template	A drop-down list of all templates for the script alert action type. Default value: Default template Note: You can view the contents of the existing templates or add additional templates in the <code><SiteScope root directory>\templates.script</code> directory.

SMS Alert Properties

The following properties must be entered for the **SMS** alert:

GUI Element (A-Z)	Description
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. Default value: every day, all day
SMS Number	The telephone number required by the SMS service that identifies the destination for the message. Syntax: Numeric only. Maximum of 9 digits.

SNMP Trap Alert Properties

The following properties must be entered for the **SNMP trap** alert:

GUI Element (A-Z)	Description
Mark this action to close alert	When the status changes and the alert trigger condition is no longer true, this action closes the alert and sends a close notification by adding the word Close to the message sent. Default value: Cleared

GUI Element (A-Z)	Description
Message	The prefix to be added to the SNMP trap sent by this alert.
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. Default value: every day, all day
SNMP Trap	The SNMP Trap to trigger an alert. Default value: Default
Template	<p>A drop-down list of all templates for the SNMP trap alert action type.</p> <p>Each line in the template is sent as a separate SNMP variable. The template file can also be modified using:</p> <ul style="list-style-type: none"> ➤ [Agent Host: <hostname-or-ip-address>] as the first line of the template, to send the trap with that hostname or IP address as the source of the trap. By default, the IP address of the machine that SiteScope is running on is used as the source of the trap. ➤ [Command: <command name>] to override the default command. ➤ [Type: <var-type>] to override the default type of the object. <p>[OID: <object id>] to change the default object id. For example, use this to change a var-binding variable object id.</p> <p>Default value: Default template</p> <p>Note: You can view the contents of the existing templates or add additional templates in the <SiteScope root directory>\templates.snmp directory.</p>

Sound Alert Properties

The following properties must be entered for the **sound** alert:

GUI Element (A-Z)	Description
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. Default value: every day, all day
Sound File	Additional sounds can be added to the <SiteScope root directory>\templates.sound directory in AU format (8 bit, 8000 Hz, one-channel) with an .au suffix.

Trigger Page

Description	Use the Trigger page to select the status of the object type that triggers an alert action.
Wizard Map	The Alert wizard includes: Alert Actions Wizard - Action Type Page > Action Type Settings Page > Trigger Page > Trigger Settings Page.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
Alert Category	<p>Alerts are triggered when the status changes from one state to another. Select the category that triggers the alert action. The categories are:</p> <ul style="list-style-type: none"> ▶ Error. Alerts are triggered if the monitor was previously reporting a status of Good. ▶ Good. Alerts are triggered if the monitor was previously reporting a status of Error. ▶ Unavailable. Alerts are triggered if the monitored machine was previously available and is no longer. ▶ Warning. Alerts are triggered if the monitor was previously reporting a status of Good. <p>Default value: Error</p>

Trigger Settings Page











Description	Use the Trigger Settings page to select the trigger frequency.
Important Information	<p>The available options vary according to what you chose in the Trigger Page.</p> <p>For more detailed information on the options here, see “Understanding When SiteScope Alerts Are Sent” on page 1390.</p> <p>Warning: When editing an alert within the Alert Action Wizard, the trigger settings may reset to their default selections if you click Back and then Next to return to the Trigger Settings page.</p>
Wizard Map	The Alert wizard includes: Alert Actions Wizard - Action Type Page > Action Type Settings Page > Trigger Page > Trigger Settings Page.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
<p>Escalate, after action <> occurred exactly N times.</p>	<p>Select this option if the alert action you are creating is dependent on another alert action. You must select the name of the alert action on which this alert action is dependent and the number of times the first alert action is triggered before this alert action is triggered.</p> <p>Example: You created an alert action to send a sound alert when a certain condition is met. You want an E-mail alert to be sent when the sound alert action has been triggered 3 times. Select the name of the sound alert action and 3.</p> <p>Note: This option appear only if another alert action has been defined for the alert.</p>
<p>Always, after the condition has occurred at least N times.</p>	<p>After the alert conditions have occurred at least N times, the alert is triggered every time the alert conditions are met again after the initial trigger.</p> <p>Type the minimum number of times the alert condition must be met before the alert is triggered the first time.</p> <p>Default value: Once, after condition has occurred exactly 1 time</p> <p>Syntax: numeric only</p> <p>Range: 1-99</p>
<p>Once, after the condition has occurred exactly N times.</p>	<p>The alert is triggered only once after the alert condition is met for the Nth time.</p> <p>Type the number of times the alert conditions must be met before the alert is triggered.</p> <p>Syntax: numeric only</p> <p>Range: 1-99</p>

GUI Element (A-Z)	Description
Initially after X times, and repeat every Y times afterwards.	<p>The alert is triggered after the alert condition occurs X consecutive times, and then the alert is triggered every consecutive Y occurrences that the alert conditions are met. For example, if X is set to 3, and Y is set to 4, then the alert action would be done on the 3rd, 7th, 11th, and so forth, occurrences of the alert condition.</p> <p>Syntax: numeric only</p> <p>Range: 1-99</p>
Once, after N group errors.	<p>This is displayed if you chose Error in the Trigger Page. The alert is triggered only after any monitor in the group has reported the alert condition exactly N consecutive times.</p> <p>Note: This option is only available for SiteScope groups.</p>
Once, after all monitors in this group are in error.	<p>This is displayed if you chose Error in the Trigger Page. The alert is triggered the first time all monitors in the group are in error.</p> <p>Note: This option is only available for SiteScope groups.</p>
Only alert if monitor was previously in error/warning	<p>This is displayed if you chose Good or Warning in the Trigger Page.</p> <p>This option suppresses the triggering of the alert until the subject monitor or group has reported a status of either of the following:</p> <ul style="list-style-type: none"> ➤ Error or Warning for alert category Good ➤ Good or Error for alert category Warning, for at least the number of times that you entered

Types of Alert Actions

GUI Element	Alert Action Name	Description
	Database	Sends an alert message with a description of the problem as a record to a SQL database.
	E-mail	Sends an e-mail message to one or more e-mail addresses with a description of the error or warning.
	Enable/Disable	Manually controls the generation of alerts.
	Log	Logs events to the Microsoft Windows Event Log.
	Pager	Sends a message to a pager to signal that SiteScope has detected a particular condition.
	Post	Submits a CGI POST containing a description of a monitor condition to a CGI script, servlet, or other CGI-enabled program.
	Script	SiteScope can run scripts or batch files when the alert trigger condition is detected. The script or batch file that is called can run a system command or a program in any language that can be called from a command line entry.
	SMS	Sends a short text message using the Short Message Service (SMS) to an SMS-enabled mobile phone or wireless device.
	SNMP Trap	Sends an SNMP trap to an SNMP host or management console.
	Sound	Plays a sound or audio file on the machine on which SiteScope is running when an event has been detected

51

SiteScope Reports

This chapter includes the main concepts, tasks, and reference information for SiteScope reports.

This chapter includes:

Concepts

- SiteScope Reports Overview on page 1439
- SiteScope Report Types on page 1441
- Working with SiteScope Management Reports on page 1443

Tasks

- Create a Report on page 1444

Reference

- SiteScope Reports User Interface on page 1446

SiteScope Reports Overview

SiteScope reports display information about how the servers and applications you are monitoring have performed over time. SiteScope reports are important tools in monitoring and troubleshooting operational performance and availability and reviewing the monitored environment.

You can create a report for a single monitor, several monitors, or even several monitor groups. Report definitions include several report content options including tables of specific monitor measurements, summaries of results, and graphs.

SiteScope reports can be valuable to many people in your organization, including management personnel in Sales, Marketing, Customer Support, and Operations. SiteScope User accounts can be created to enable these users restricted access to the SiteScope service to view reports. For more information, see “User Preferences” on page 226.

Note: To view certain report elements on SiteScope for UNIX/Linux, it is necessary that an X Window system be running on the server where SiteScope is running.

SiteScope Monitor Data Log Files

SiteScope monitor data available for generating reports is limited to the amount of log data stored on the SiteScope server. By default, SiteScope retains monitor data log files for 40 days. The log files are rotated and files older than the log retention period are automatically deleted.

Note: Keeping monitor data logs for longer periods can cause a data storage problem for the SiteScope server depending on the total number of monitors configured and how often the monitors run per day. You should monitor the size of log files in the **SiteScope\logs** directory to estimate the data accumulation rate.

You can change the length of time that SiteScope retains monitor data using the log preferences. You can configure SiteScope to export monitor data to an external SQL-compliant database to maintain monitor data for longer periods or to make the data available to other reporting applications. For details, see “Log Preferences” on page 221.

SiteScope Report Types

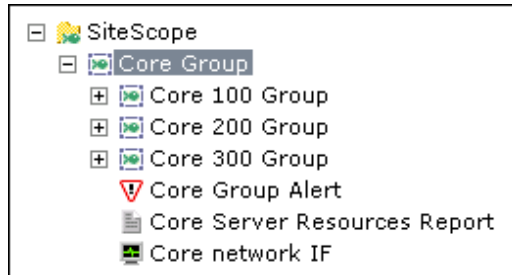
SiteScope includes four kinds of management reports. The following describes the report types and their usage.

Report Type	Description
Alert Reports	<p>Alert reports provide information about SiteScope alerts generated during a specified period of time. You create an Alert report on an ad hoc basis. In addition, the settings for an Alert report are not saved to the SiteScope configuration data for later use.</p> <p>For details on configuring the Alert report, see “New Alert Report Page” on page 1447.</p>
Management Reports	<p>Management reports provide a summary of infrastructure availability and performance data for a given period of time. Management reports are generated automatically based on their preset schedule from data collected by SiteScope monitors. According to the preset schedule, SiteScope reads the applicable log files and generates the report based on the monitor metrics for the time interval specified. You can save the report data in a file suitable for exporting to third-party applications.</p> <p>For details on configuring the Management report, see “New Management Report Page” on page 1448.</p>

Report Type	Description
<p>Monitor Summary Reports</p>	<p>Monitor reports enable you to review configuration properties and settings for existing monitors. You can export a monitor report in one of three text data formats. Unlike a Management report which is based on a schedule that you specify, you create a Monitor report on an ad hoc basis. In addition, the settings for a Monitor Summary report are not saved to the SiteScope configuration data for later use.</p> <p>For details on configuring the Monitor Summary report, see “New Monitor Report Page” on page 1459.</p>
<p>Quick Reports</p>	<p>Quick reports enable you to view monitor data for specific monitors or groups of monitors during specific time periods.</p> <p>Unlike a Management report that is generated based on a schedule that you specify, you create a Quick report on an ad hoc basis. In addition, the settings for a Monitor Summary report are not saved to the SiteScope configuration data for later use.</p> <p>For details on configuring the Quick report, see “New Quick Report Page” on page 1462.</p>

Working with SiteScope Management Reports

Reports are added as elements to the SiteScope menu tree. They can be added as a child to the SiteScope node, to a monitor group, or to an individual monitor. The following figure is an example of how reports are displayed in the left menu tree.



Reports have a scope based on the container to which they are added. You add a report to the container or element that contains all of the monitors whose data you want to include in the report. You then use the **Monitors and Groups to report on** setting in the Report Properties tab to narrow the selection of monitors to be included in the report.

You can create as many SiteScope report definitions as you want. It is recommended however that you plan and consolidate reports to keep number of report definitions to a minimum. This can facilitate report administration and help reduce redundant report messages or actions. When creating a report for a large number of monitors, you should consider making separate reports based on the type of monitor or measurement. For example, when reporting on system resources for 20 different remote servers, consider making one report with monitors that measure numeric values such as CPU or disk space and another report for monitors that report basic availability such as services or processes.

By default, SiteScope keeps the 10 most recently generated reports. This means that hourly reports are available for the last 10 hours, daily reports are available for 10 days, weekly reports are available for 10 weeks, and so forth. You can change this report storage period by changing the value of the `_maximumReports` setting in the SiteScope `master.config` file.

Deleting a Management report definition discontinues the generation of applicable report. Previously generated reports continue to be available until the underlying data is removed.

You can copy and paste a report definition. The report definition settings are pasted to the new location with the exception of the **report Targets** setting, which are automatically reset to include all of the children of the container into which the report is pasted. After pasting a report, you should edit the report definition properties to be sure that the assigned **report targets** are appropriate to the new report context and your overall reporting plan.

Create a Report

This task describes the steps involved in creating a SiteScope report.

This task includes the following steps:

- “Select a Report Type” on page 1444
- “Configure the Report Settings” on page 1445
- “Results” on page 1445

1 Select a Report Type


Right-click the group or monitor container in which you want to create a report, and click **New Report**. Select the report type you want to add from the New SiteScope Report page. For details of report types, see “SiteScope Report Types” on page 1441.

2 Configure the Report Settings

Select the monitors to include in the report and configure the report settings. For details on the report settings user interface, see “SiteScope Reports User Interface” on page 1446.

Note: By default, a report includes data from all monitors within the selected container. For Alert Reports, you cannot remove any of the monitors in the selected container from the report.

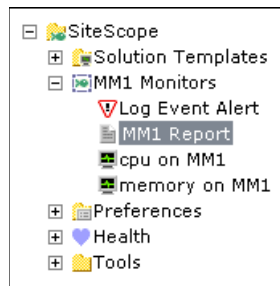
3 Results

Management reports are added to the selected container in the monitor tree (indicated by the  icon). For details on viewing the Management report, see “Management Report” on page 1473.

All other reports are generated and displayed in your Web browser.

- For details on viewing the Alert report, see “Alert Report” on page 1471.
- For details on viewing the Monitor Summary report, see “Monitor Summary Report” on page 1477.
- For details on viewing the Quick report, see “Quick Report” on page 1480.

Example - Management Report in Monitor Tree



SiteScope Reports User Interface

This section describes:

- New SiteScope Report Page on page 1446
- New Alert Report Page on page 1447
- New Management Report Page on page 1448
- New Monitor Report Page on page 1459
- New Quick Report Page on page 1462
- Alert Report on page 1471
- Management Report on page 1473
- Monitor Summary Report on page 1477
- Quick Report on page 1480
- Annotation Tool on page 1484

New SiteScope Report Page

Description	Enables you to define a new report for all monitors in the selected SiteScope, monitor group, or monitor container. To access: Right-click the SiteScope node, a group, or a monitor container, and select New Report .
Included in Tasks	“Create a Report” on page 1444
Useful Links	“SiteScope Reports Overview” on page 1439 “SiteScope Report Types” on page 1441

New Alert Report Page

Description	Enables you to create a report used to display SiteScope alerts sent over a given time period. To access: Right-click the SiteScope node, a monitor group, or a monitor container, and select New Report . In the New SiteScope Report page, click Alert .
Included in Tasks	“Create a Report” on page 1444
Useful Links	“SiteScope Reports Overview” on page 1439

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Alert types	Choose the alert types that you want to include in the report. Use the CTRL and SHIFT keys to select more than one alert type. Default value: All Types

GUI Element	Description
Alert time period	<p>Specify the period of time that you want the report to cover. Type the time and date you want report coverage to start in the From boxes and the time and date you want coverage to end in the To boxes.</p> <p>Default value: The alert time period is from one hour before the time that the Alert Report is generated until the current time. Click Apply to validate the time period.</p> <p>Note: Times should be entered in 24-hour format.</p>
Detail level	<p>Select the level of detail to include in the report. The options are:</p> <ul style="list-style-type: none"> ▶ Basic. Displays the time and summary information for each alert sent. This is the default setting. ▶ Show Detail for Failed Alerts. Displays the time and summary information for each alert, and a full diagnostics breakdown for each failed alert. ▶ Show Detail for All Alerts. Displays detailed alert information for each alert in the report.

New Management Report Page

Description	<p>Enables you to create a report that provides a summary of system availability data for a given time period.</p> <p>To access: Right-click the SiteScope node, a monitor group, or a monitor container, and select New Report. In the New SiteScope Report page, click Management.</p>
Important Information	<p>HTML code entered in report text boxes is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected.</p>
Included in Tasks	<p>“Create a Report” on page 1444</p>
Useful Links	<p>“SiteScope Reports Overview” on page 1439</p>

The New Management Report page includes the following areas:

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	Type a text description for this Management Report definition. This name is used to identify this Management Report definition in the product display.
Monitor and Groups to report on	Select the groups and/or monitors to be include in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers. Default value: The current container and all child elements are selected.
Thresholds	Creates a table of monitor error, warning, and good threshold settings for all of the monitors included in the report. If selected, this table is displayed as the first report section.
Uptime and Readings	Creates two report tables: Uptime Summary and Measurement Summary . For details of the data included in these tables, see “Uptime Summary and Measurement Summary Data” on page 1457.
Uptime: Count warning good	Includes any monitor readings that are reported as warnings in the overall Uptime calculation.
Uptime: Remove warning	Suppresses monitor readings reported as warnings from the overall Uptime and Readings Summary section. Note: This option only suppresses the display of the Warning % column in the table; it does not change the calculation of the Uptime %.

GUI Element	Description
Uptime: Failure as good	<p>Suppresses monitor readings reported as errors from the overall Uptime and Readings Summary section.</p> <p>Note: This option only suppresses the display of the Error % column in the table; it does not change the calculation of the Uptime %.</p>
Time in Error	<p>Creates a table summary listing each monitor selected for the report with a summary of how many minutes the monitor status was calculated as being in error for the period of the report.</p>
Monitor Readings	<p>Creates a table of individual readings recorded by the monitors during the report period, including all readings (error, good, and warning). This report table may also include blank "buckets" depending on the period of the report and how often the monitors ran during the period.</p>
Errors	<p>Creates a table of individual error readings recorded by the monitors during the report period.</p>
Warnings	<p>Creates a table of individual warning readings recorded by the monitors during the report period.</p>
Goods	<p>Creates a table of individual good readings recorded by the monitors during the report period.</p>
Graph of Measurements	<p>For graph reports, use the drop-down list to choose a graphical measurement to be included in the report. For details of the options, see “Graph Measurement Options” on page 1458.</p>

GUI Element	Description
Time Period for Report	<p>Select the time period for which you want to view monitoring data. You can choose to report on data for a set number of hours, for the last day, the last several days, the past week, past month, or month-to-date for the current calendar month.</p> <p>Note: Daily and month-to-date reports are generated every day at the scheduled time. Weekly reports are generated on Sundays at the scheduled time, and monthly reports are generated on the first day of the month following the current month so that they contain an entire month's worth of data.</p>
Alert Table	<p>Select an option to include a table of alerts sent for the monitors in the report. The options for the Alert Table level are:</p> <ul style="list-style-type: none"> ▶ No Alert Table. No table of alerts is included in the report (default) ▶ Basic Alert Table. Displays the time and summary information for each alert sent. ▶ Show Detailed Alert Table for Failed Alerts. Displays the time and summary information for each alert, and a full diagnostics breakdown for each failed alert. ▶ Show Detailed Alert Table for All Alerts. Displays detailed alert information for each alert in the report.
File Format	<p>This option enables some customization of the report appearance. The options are:</p> <ul style="list-style-type: none"> ▶ Color Background (default) ▶ Color Background, no table borders ▶ White Background
Send Report by E-Mail	<p>To have the report forwarded by e-mail when it is generated, type the e-mail address(es) to which this report should be sent each time its generated. To send the reports to multiple e-mail addresses, separate the e-mail addresses with commas.</p>

GUI Element	Description
HTML Format	Select if you want the reports sent in HTML format. Use this option to include the SiteScope report graphics. If you do not select this option only a text summary of the report is sent.
Format Template	<p>Select a template for SiteScope to use to create the e-mail message. You can choose from the following templates or make a copy of one of these and customize it to meet your own needs.</p> <ul style="list-style-type: none"> ➤ HistoryLongMail - Choose this option to send a detailed history report. It contains both user and administration links. ➤ HistoryLongXMLMail - Choose this option to send a detailed history report. It contains both user and administration links for reports & XML files. ➤ HistoryMail - This is the default option. ➤ HistoryMailAlertDetail - Choose this option to have all alerts included in the report that is e-mailed. ➤ HistoryMailNoLinks - Choose this option to send the report without any links in it.

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Detailed monitor information	<p>Displays all of the information gathered for each monitor on the report. Otherwise, only the primary data is displayed for each monitor.</p> <p>Example: If this box is checked on a URL Sequence Monitor, the timing information for each step in the sequence is displayed in the report.</p>
Show Which Monitors	<p>Select a subset of those monitors to be shown in the report—those that have had the specified status sometime during the report's time frame. You can select only monitors in Error or Warning, monitors in Error, monitors in Warning, monitors that were OK, or all monitors.</p> <p>Default value: Show All Monitors</p> <p>Example: Choosing Show Only Monitors in Error displays report data only if that monitor had spent time in error sometime during the time interval of the report.</p>
Schedule Filter	<p>Select a schedule filter option for showing only a subset of the data in the report—those monitors that have samples during the time period of the schedule.</p> <p>Default value: The report shows data for the full period of the report (every day, all day).</p> <p>Example: Choosing weekdays, 09:00-18:00 displays report data for the selected monitors with samples from the 9am to 6pm time period, Monday through Friday. Only this data is used for all the calculations.</p>
Best Case Calculation	<p>Select this option to calculate the monitor uptime percentage, warning percentage, and error percentage using a best case scenario. In this scenario, monitor time in error is calculated from the first monitor run that explicitly reported an Error instead of from the time of the last known Good monitor run.</p>

GUI Element	Description
Time Between Samples	<p>Use this time scale option to choose the time interval between monitor readings. You can choose intervals that range from once every minute to once a day, or you can use the automatic scaling. When automatic scaling is used, SiteScope determines how many readings were taken over the chosen time period for the given monitors and then selects an appropriate interval for the management report.</p> <p>Default value: Automatic Time Scale</p>
Max Value on Graph	<p>Select a vertical scale option to choose the maximum value displayed on a graph. Choosing a specific scale value makes it easier to compare graphs from different monitors and times.</p> <p>Default value: Automatic Vertical Scale</p>
Description	<p>(Optional) Use this text box to describe other information about this report definition. For example, include information about the purpose, target, setup date, or audience for this report.</p>
Disable	<p>Select this box to temporarily disable the generation of this report. To enable the report again, clear the box.</p>
End of Report Period	<p>By default SiteScope generates reports starting at the indicated time and ending at the time the report was generated. You may choose an alternate end time by selecting a time from the drop-down list. For example, you may want to have your reports run from midnight to midnight.</p>

GUI Element	Description
<p>Comma-delimited file</p>	<p>Select this box to save a generated management report to a comma-delimited text file which you can then import into a spreadsheet application.</p> <p>SiteScope automatically saves these files in the <SiteScope root directory>\htdocs directory. To find the exact location of the saved file on your machine, click the View Report tab for the report, and move the pointer over the text link for the report in the Information For column. The full path to the file is listed in the status bar of your Web browser. To open the saved file on your machine, click the text link to go to the Report page. If you type an e-mail address in the E-mail text box, SiteScope sends a copy of the comma-delimited file to that address.</p> <p>Note: The comma-delimited file creates two columns for each monitor reading; one containing the value with units, and the other containing just the value. This is to make it easier to import the comma-delimited data into a third party application which may not automatically separate data values from the text describing the units.</p>
<p>Send Comma-delimited file by E-mail</p>	<p>If you type an e-mail address in the text box, SiteScope sends a copy of the file to that address.</p>

GUI Element	Description
XML file	<p>Select this box to save a generated management report to an XML text file. SiteScope automatically saves these files in the <SiteScope root directory>\htdocs directory. To find the exact location of the saved file on your machine, click the View Report tab for the report, and move the pointer over the xml link for the report in the Information For column. The full path to the file is listed in the status bar of your Web browser. To open the saved file on your machine, click the xml link to go to the Report page. If you type an e-mail address in the E-mail text box, SiteScope sends a copy of the comma-delimited file to that address.</p> <p>Note: The XML file creates two columns for each monitor reading; one containing the value with units, and the other containing just the value. This is to make it easier to import the XML data into a third party application which may not automatically separate data values from the text describing the units.</p>
Send XML file by E-mail	<p>If you type an e-mail address in the text box, SiteScope sends a copy of the XML file to that address.</p>
Generate report at	<p>Indicate the time that you want SiteScope to create this management report. The report contains information for the last day, week, or month, ending at the time the report is run. For example, if a daily report is generated at 18:00 (6:00 p.m.), it contains data generated between 18:00 the previous day and 18:00 of the current day. The default value is 00:00 which represents midnight.</p> <p>Note: SiteScope Management report generation may temporarily affect overall SiteScope performance and responsiveness depending on the number of monitors and time period of the report. Generally, you should schedule reports to be generated during off-peak hours relative to overall monitoring tasks and load. If you are generating many reports each day, you should consider staggering the Generate report at value for different reports.</p>

Category Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see “Create and Define a New Category” on page 198.

Uptime Summary and Measurement Summary Data

These tables include the following data:

Table	Data
Uptime Summary Table	<ul style="list-style-type: none"> ▶ Name. The name of monitors included in the report ▶ Uptime %. The percentage of monitor readings reported as good ▶ Warning %. The percentage of monitor readings reported as warning ▶ Error %. The percentage of monitor readings reported as error ▶ Last. The last reading of the monitor for the report period
Measurement Summary Table	<ul style="list-style-type: none"> ▶ Name. The name of monitors included in the report ▶ Measurement. The parameter being monitored (for error condition) ▶ Max. The maximum value recorded for the Measurement parameter during the report period ▶ Avg. The average value of the readings recorded for the report period ▶ Last. The last reading of the monitor for the report period

Graph Measurement Options

This table includes a description of the graph measurement options that can be included in the report:

Graph	Description
None - no graph	No graphs are included in the report. The report only includes the tabular data contents you have selected.
Bar graph - one graph per measurement	This bar graph option displays a single type of measurement per graph and per monitor during the specified time frame. For reports on multiple monitors, this results in the most number of graphs with one bar graph generated for each type of measurement for each monitor.
Line Graph - one graph per measurement	This line graph option displays a separate line graph for each type of measurement for a single monitor. Like the bar graph option, this results in the most number of line graphs with one line graph generated for each type of measurement for each monitor selected for the report regardless of any compatibility of measurement type.
Line Graph - group per monitor instance	This line graph option attempts to group all measurements from a single monitor instance into a single graph per monitor. The number of line graphs actually generated depends on whether the monitor records multiple measurements per monitor run (for example, the Microsoft Windows Resources or UNIX Resources monitor types) and whether the measurement types are compatibility with one another. Separate graphs are generated if the measurability types are not compatible.

Graph	Description
Line Graph - group same measurement types	Select this option to plot the same measurement types gathered by several different monitor instances into single graphs. A line graph is generated for each set of compatible measurement types regardless of the number of monitors selected for the report.
Line Graph - group compatible measurements	Select this option to display all compatible measurements from the selected monitors on a single graph. The option is intended to minimize the total number of line graphs generated. The number of graphs generated is still dependent on the compatibility of the selected monitor types and the measurement types collected by those monitors. If all of the monitors selected for the report are of the same type, for example URL monitors, then a single graph is generated with a colored line for each of the monitors.

Note: A bar graph is generated using standard HTML, so it can be printed from all browser types. Line graphs are generated using a java applet and may not print directly from all browsers.

New Monitor Report Page

Description	Enables you to create a report that provides detailed information about the monitors defined in one or more monitor groups. To access: Right-click the SiteScope node, a monitor group, or a monitor container, and select New Report . In the New SiteScope Report page, click Monitor .
Included in Tasks	“Create a Report” on page 1444
Useful Links	“SiteScope Reports Overview” on page 1439 “Monitor Summary Report” on page 1477

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Monitor and Groups to report on	<p>Select the groups and/or monitors to be include in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers.</p> <p>Default value: The current container and all child elements are selected.</p>
Display Columns	<p>Select the monitor information to display in the report columns. Data is shown in the report for the selected parameters only if the particular option has been selected, such as Disabled and Frequency, or if a value has been supplied, such as Monitor Descriptions. If the option or value has not been defined in the particular monitor setup, the column is blank for that parameter for that monitor.</p> <p>Note: Hold down the SHIFT key to select a set of adjacent groups. Use CTRL-click to select non-adjacent items.</p>
Sort By	<p>Select the monitor parameter to use as a sort key for the report. Select the applicable radio button below the list box to have the report sorted in Ascending or Descending order using the selected sort key.</p> <p>Example: To sort the report alphabetically by monitor type, select Monitor Type, and select Ascending sort order.</p>
Show Parameters	<p>Select this box if you want the report to contain the parameters defined for each monitor. This option includes a list of the active options defined for each selected monitor in a single table cell rather than individual columns as with the option above.</p>

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Export to File	Select this box to have SiteScope export the Monitor Summary report data to a text file.
File Name	When the Export to File option is enabled, SiteScope writes the data to the file name specified in this box using the selected text format. The file is written into the <SiteScope root directory>\htdocs directory. Default value: monSummary.csv
File Format	Select the format for the exported file. The options are comma-delimited text, tab delimited text, or HTML. Default value: comma-delimited text

 **New Quick Report Page**

Description	<p>Enables you to create a one-time SiteScope management report for any monitor or group of monitors over a given time period.</p> <p>To access: Right-click the SiteScope node, a monitor group, or a monitor container, and select New Report. In the New SiteScope Report page, click Quick.</p>
Important Information	<ul style="list-style-type: none"> ▶ The time interval for a Quick report is not incremented automatically. This means that a Quick report always contain the data for the absolute Report Period interval defined in the report definition. To view more recent data using a Quick report, edit the Report Period setting. ▶ When working in Business Availability Center, Quick Report definitions in System Availability Management Administration are stored only with the Business Availability Center context. Quick Report definitions are not stored in and do not persist on the SiteScope server.
Included in Tasks	"Create a Report" on page 1444
Useful Links	"SiteScope Reports Overview" on page 1439

Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Monitor and Groups to report on	Select the groups and/or monitors to be include in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers. Default value: The current container and all child elements are selected.
Thresholds	Creates a table of monitor error, warning, and good threshold settings for all of the monitors included in the report. If selected, this table is displayed as the first report section.
Uptime and Readings	Creates two report tables: Uptime Summary and Measurement Summary . For details of the data included in these tables, see “Uptime Summary and Measurement Summary Data” on page 1468.
Uptime: Count warning good	Includes any monitor readings that are reported as warnings in the overall Uptime calculation.
Uptime: Remove warning	Suppresses monitor readings reported as warnings from the overall Uptime and Readings Summary section. Note: This option only suppresses the display of the Warning % column in the table; it does not change the calculation of the Uptime %.
Uptime: Failure as good	Suppresses monitor readings reported as errors from the overall Uptime and Readings Summary section. Note: This option only suppresses the display of the Error % column in the table; it does not change the calculation of the Uptime %.
Time in Error	Creates a table summary listing each monitor selected for the report with a summary of how many minutes the monitor status was calculated as being in error for the period of the report.

GUI Element	Description
Monitor Readings	Creates a table of individual readings recorded by the monitors during the report period, including all readings (error, good, and warning). This report table may also include blank "buckets" depending on the period of the report and how often the monitors ran during the period.
Errors	Creates a table of individual error readings recorded by the monitors during the report period.
Warnings	Creates a table of individual warning readings recorded by the monitors during the report period.
Goods	Creates a table of individual good readings recorded by the monitors during the report period.
Graph of Measurements	For graph reports, use the drop-down list to choose a graphical measurement to be included in the report. For details of the options, see “Graph Measurement Options” on page 1469.
Report Period	<p>Specify the time period for which you want to view monitoring data. Type the time from which you want the report coverage to start in the From boxes and the time to which you want to cover in the To boxes.</p> <p>Default value: The time period is from one hour before the time that the Quick Report is generated until the current time.</p> <p>Note: Times should be entered in 24-hour format.</p>
Report In	Select the format to be used in displaying the report: HTML format, Text format or XML format.

GUI Element	Description
Alert Table	<p>Select an option to include a table of alerts sent for the monitors in the report. The options for the Alert Table level are:</p> <ul style="list-style-type: none"> ▶ No Alert Table. No table of alerts is included in the report (default) ▶ Basic Alert Table. Displays the time and summary information for each alert sent. ▶ Show Detailed Alert Table for Failed Alerts. Displays the time and summary information for each alert, and a full diagnostics breakdown for each failed alert. ▶ Show Detailed Alert Table for All Alerts. Displays detailed alert information for each alert in the report.
File Format	<p>This option enables some customization of the report appearance. The options are:</p> <ul style="list-style-type: none"> ▶ Color Background (default) ▶ Color Background, no table borders ▶ White Background
Send Report by E-Mail	<p>To have the report forwarded by e-mail when it is generated, type the e-mail address(es) to which this report should be sent each time its generated. To send the reports to multiple e-mail addresses, separate the e-mail addresses with commas.</p>

Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Detailed monitor information	<p>Displays all of the information gathered for each monitor on the report. Otherwise, only the primary data is displayed for each monitor.</p> <p>Example: If this box is checked on a URL Sequence Monitor, the timing information for each step in the sequence is displayed in the report.</p>
Show Which Monitors	<p>Select a subset of those monitors to be shown in the report—those that have had the specified status sometime during the report's time frame. You can select only monitors in Error or Warning, monitors in Error, monitors in Warning, monitors that were OK, or all monitors.</p> <p>Default value: Show All Monitors</p> <p>Example: Choosing Show Only Monitors in Error displays report data only if that monitor had spent time in error sometime during the time interval of the report.</p>
Schedule Filter	<p>Select a schedule filter option for showing only a subset of the data in the report—those monitors that have samples during the time period of the schedule.</p> <p>Default value: The report shows data for the full period of the report (every day, all day).</p> <p>Example: Choosing weekdays, 09:00-18:00 displays report data for the selected monitors with samples from the 9am to 6pm time period, Monday through Friday. Only this data is used for all the calculations.</p>
Best Case Calculation	<p>Select this option to calculate the monitor uptime percentage, warning percentage, and error percentage using a best case scenario. In this scenario, monitor time in error is calculated from the first monitor run that explicitly reported an Error instead of from the time of the last known Good monitor run.</p>

GUI Element	Description
Time Between Samples	<p>Use this time scale option to choose the time interval between monitor readings. You can choose intervals that range from once every minute to once a day, or you can use the automatic scaling. When automatic scaling is used, SiteScope determines how many readings were taken over the chosen time period for the given monitors and then selects an appropriate interval for the management report.</p> <p>Default value: Automatic Time Scale</p>
Max Value on Graph	<p>Select a vertical scale option to choose the maximum value displayed on a graph. Choosing a specific scale value makes it easier to compare graphs from different monitors and times.</p> <p>Default value: Automatic Vertical Scale</p>

Uptime Summary and Measurement Summary Data

These tables include the following data:

Table	Data
Uptime Summary Table	<ul style="list-style-type: none"> ➤ Name. The name of monitors included in the report ➤ Uptime %. The percentage of monitor readings reported as good ➤ Warning %. The percentage of monitor readings reported as warning ➤ Error %. The percentage of monitor readings reported as error ➤ Last. The last reading of the monitor for the report period
Measurement Summary Table	<ul style="list-style-type: none"> ➤ Name. The name of monitors included in the report ➤ Measurement. The parameter being monitored (for error condition) ➤ Max. The maximum value recorded for the Measurement parameter during the report period ➤ Avg. The average value of the readings recorded for the report period ➤ Last. The last reading of the monitor for the report period

Graph Measurement Options

This table includes a description of the graph measurement options that can be included in the report:

Graph	Description
None - no graph	No graphs are included in the report. The report only includes the tabular data contents you have selected.
Bar graph - one graph per measurement	This bar graph option displays a single type of measurement per graph and per monitor during the specified time frame. For reports on multiple monitors, this results in the most number of graphs with one bar graph generated for each type of measurement for each monitor.
Line Graph - one graph per measurement	This line graph option displays a separate line graph for each type of measurement for a single monitor. Like the bar graph option, this results in the most number of line graphs with one line graph generated for each type of measurement for each monitor selected for the report regardless of any compatibility of measurement type.
Line Graph - group per monitor instance	This line graph option attempts to group all measurements from a single monitor instance into a single graph per monitor. The number of line graphs actually generated depends on whether the monitor records multiple measurements per monitor run (for example, the Microsoft Windows Resources or UNIX Resources monitor types) and whether the measurement types are compatibility with one another. Separate graphs are generated if the measurement types are not compatible.

Graph	Description
Line Graph - group same measurement types	Select this option to plot the same measurement types gathered by several different monitor instances into single graphs. A line graph is generated for each set of compatible measurement types regardless of the number of monitors selected for the report.
Line Graph - group compatible measurements	Select this option to display all compatible measurements from the selected monitors on a single graph. The option is intended to minimize the total number of line graphs generated. The number of graphs generated is still dependent on the compatibility of the selected monitor types and the measurement types collected by those monitors. If all of the monitors selected for the report are of the same type, for example URL monitors, then a single graph is generated with a colored line for each of the monitors.

Note: A bar graph is generated using standard HTML, so it can be printed from all browser types. Line graphs are generated using a java applet and may not print directly from all browsers.

Alert Report

The following is an example of the Alert report.

Alerts (SiteScope) from 4:20 PM 7/30/07 to 4:26 PM 7/30/07

Time	Type	Message	Monitor	Group
4:20 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:21 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:22 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:23 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:24 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:25 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:26 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36

Description	<p>Displays information about SiteScope alerts generated during a specified period of time for the monitors in the selected container.</p> <p>To access: Right-click the SiteScope node, a monitor group, or a monitor container, and select New Report. In the New SiteScope Report page, click Alert. Configure the report properties, and click Apply.</p>
Included in Tasks	“Create a Report” on page 1444
Useful Links	“New Alert Report Page” on page 1447

Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Report title>	The report title contains the name of the monitor group container or individual monitor for which the report was created, and the time period that the report covers.
Time	The time at which the alert was triggered.
Type	The type of alert action.
Message	The type of message in the alert (for example, Default, alarm).
Monitor	The name of the monitor on which the alert was triggered.
Group	The name of the group on which the alert was triggered.

Management Report

The following is an example of the Management report.

Management SiteScope Report "Cor...ort"
Properties **View Report**

[Table Format](#)
[Error List](#)
[Warning List](#)
[Good List](#)

[Index of Reports](#)

Core Weekly Report

(information from 9:34 AM 12/3/07 to 9:34 AM 12/4/07)

Uptime Summary

Name	Uptime %	Error %	Warning %	Last
CPU Utilization on SiteScope Server	100	0	0	good
Memory on SiteScope Server	100	0	0	good
FTP on localhost	100	0	0	good
URL List	0	0	0	good
Disk Space: C on SiteScope Server	100	0	0	good
Directory: c:\ on SiteScope Server	100	0	0	good
Service: HTTP on SiteScope Server	100	0	0	good

Measurement Summary

Name	Measurement	Max	Avg	Last
CPU Utilization on SiteScope Server	utilization	74%	28.08%	24%
Memory on SiteScope Server	percent used	22%	22%	22%
FTP on localhost	round trip time	0.02 sec	0.01 sec	0.016 sec
URL List	errors	0 URLs	0 URLs	0 URLs
Disk Space: C on SiteScope Server	percent full	32%	32%	32%
Directory: c:\ on SiteScope Server	total of file sizes	10998795264 bytes	10997342208 bytes	10998795264 bytes

Description	<p>Displays a summary and specific details of infrastructure availability and performance data for monitors and monitor groups over a given period of time. Use Management reports to detect emerging trends and correct potential problems before they become a crisis.</p> <p>To access: Right-click the SiteScope node, a monitor group, or a monitor container, and click Edit. Click the View Report tab. Click the date-coded link for the report period you want to view. If no reports have been generated, or if you want to create an updated report, click the Generate button.</p>
Included in Tasks	“Create a Report” on page 1444
Useful Links	<p>“Working with SiteScope Management Reports” on page 1443</p> <p>“New Management Report Page” on page 1448</p>

Report Content - Index Page

The following elements are included in the Management report index page:

GUI Element	Description
Most Recent Report	Click to display the most recent Management report available for the currently selected monitor or group.
Information For <report time and data>	Click to display the Management report for the time period specified in the link for the currently selected monitor or group. For details on the Management Report page, see “Report Content - Management Report Page” below.
Generate	Click to create a new report for the currently selected monitor or group, regardless of when the report was normally scheduled to be generated.

Report Content - Management Report Page

The following elements are included in the Management report page:

GUI Element	Description
<License details>	License details are displayed at the top of the page. It includes the SiteScope license category, the number of monitor points available, and the number of days remaining on the license.
Table Format	Click the Table Format link to go to the measurements data in table format in the currently selected report.
Error List	Click the Error List link to go to the list of monitors with error status in the currently selected report.
Warning List	Click the Warning List link to go to the list of monitors with warning status in the currently selected report.
Good List	Click the Good List link to go to the list of monitors with good status in the currently selected report.
Index of Reports	Click the Index of Reports link to go to the index of Management reports. For details on the Management Report index page, see "Report Content - Index Page" on page 1474.
Uptime Summary	A summary, in percentage terms, of the time that each monitor was operational, in error status, and in warning status for the report period. It also shows the latest status of the monitor before the report was generated.
Measurement Summary	A summary, in percentage terms, of the average and maximum measurements or values recorded for the report period. It also shows the latest percentage for each measurement before the report was generated.
<Measurement Graphs>	Measurement data in graph format for each monitored instance for the report period.

GUI Element	Description
<Measurement Tables>	Measurement data in table format, shown at 30 minute increments, for each monitored instance for the report period. Entries highlighted in red or yellow indicate that the measurement exceeded the error or warning status threshold for the monitor. Blue indicates that the monitor was disabled.
<Error List Table>	Lists the monitor instances that exceeded the error status threshold for the monitor. Entries are highlighted in red.
<Warning List Table>	Lists the monitor instances that exceeded the warning status threshold for the monitor. Entries are highlighted in yellow.
<Good List Table>	Lists the monitor instances that were in the good status threshold for the monitor. Entries are highlighted in green.

 **Monitor Summary Report**

The following is an example of the Monitor Summary report.

SiteScope Monitor Summary Report					
Group	name	class	frequency	disabled	schedule
AutoSanity: Basic	URL List	URL List	1 hour		
AutoSanity: Basic	Service: HTTP on SiteScope Server	Service	10 minutes		
AutoSanity: Basic	FTP on localhost	Port	1 minute		
Health	Monitor Load Checker	Monitor Load Monitor	100 seconds		
AutoSanity: Basic	Memory on SiteScope Server	Memory	1 minute		
Health	Log Event Checker	Log Event Health Monitor	10 minutes		
AutoSanity: Basic	Link Check: http://www.google.com	Link Check	1 hour		
Health	Health of SiteScope Server	Health of SiteScope Server	5 minutes		
EMS	EMS Log File on SiteScope Server	EMS Log File	10 minutes		
AutoSanity: Basic	Disk Space: C on SiteScope Server	Disk Space	1 minute		
AutoSanity: Basic	Directory: c:\ on SiteScope Server	Directory	1 minute		
AutoSanity: Basic: DisabledGroup	disabledMonitor	CPU Utilization	10 minutes	disabled	
AutoSanity: Basic	CPU Utilization on SiteScope Server	CPU Utilization	1 minute		
Health	BAC Integration Statistics	BAC Integration Statistics	100 seconds		

[Close Window](#)

Description	<p>Displays information about the configuration and current settings of monitors in the groups you have selected to include in the report.</p> <p>Use this report to view setup information on monitors as well as the organization and makeup of groups of monitors. For example, you can check and compare monitor run frequencies (the Frequency setting) if you are having problems with monitor skips. You can also use the report to check for monitor dependencies that can impact alerting.</p> <p>To access: Right-click the SiteScope node, a monitor group, or a monitor container, and select New Report. In the New SiteScope Report page, click Monitor. Configure the report properties, and click Apply.</p>
Included in Tasks	“Create a Report” on page 1444
Useful Links	“New Monitor Report Page” on page 1459

Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Group	The group name to which the monitor belongs.
Name	The display name or text description for each monitor.
Class	The monitor type.
Frequency	The frequency at which the monitor is set to run.
Disabled	Whether or not the monitor is disabled.
Depends on	Lists any dependent monitors, if the running of this monitor is dependent on the status of other monitors.

GUI Element	Description
Points	The number of license points used by the monitor instance.
OID	The Object ID for this monitor.
Schedule	The monitor schedule, if a schedule other than the default schedule is selected.
Error Frequency	If the Error Frequency option is selected, the monitoring interval, in seconds, for monitors that have reported an error condition.
Timeout	The timeout setting for the monitor.
Verify Error	Displays On if the Verify Error option is selected. This option automatically runs the monitor again if it detects an error.
Monitor Description	The text description for the monitor in the Monitor Description box.
Thresholds	The threshold conditions for the monitor instance.

Quick Report

The following is an example of the Quick report.

Evaluation license for 1,000 points, 9 days remaining

[Table Format](#) [Close Window](#)
[Error List](#)
[Warning List](#)
[Good List](#)

Summary for Multiple Monitors

(information from 7:53 AM 11/1/07 to 8:53 AM 11/1/07)

Uptime Summary

Name	Uptime %	Error %	Warning %	Last
Log Event Checker	100	0	0	good
Monitor Load Checker	100	0	0	good
BAC Integration Statistics	100	0	0	good
Health of SiteScope Server	100	0	0	good
cpu on core	0	0	0	DISABLED
memory on core	0	0	0	DISABLED
ping	0	100	0	ERROR

Measurement Summary

Name	Measurement	Max	Avg	Last
Log Event Checker	Currently logging to Business Availability Center	0	0	0
Log Event Checker	Current Monitors Running	0	0	0
Log Event Checker	Current Monitors Waiting	0	0	0

Description	<p>Displays a summary and specific details of infrastructure availability and performance data for monitors and monitor groups over a given period of time. Quick reports are generated on an ad hoc basis and are not saved to the SiteScope configuration data.</p> <p>To access: Right-click the SiteScope node, a monitor group, or a monitor container, and select New Report. In the New SiteScope Report page, click Quick. Configure the report properties, and click Apply.</p>
Important Information	<ul style="list-style-type: none"> ▶ The time interval for a Quick report is not incremented automatically. This means that the report always contains the data for the absolute Report Period interval defined in the report definition. To view more recent data using a Quick report, edit the Report Period setting. ▶ When working in Business Availability Center, Quick Report definitions in System Availability Management Administration are stored only with the Business Availability Center context. Quick Report definitions are not stored in and do not persist on the SiteScope server.
Included in Tasks	“Create a Report” on page 1444
Useful Links	“New Quick Report Page” on page 1462



Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<License details>	License details are displayed at the top of the page. It includes the SiteScope license category, the number of monitor points available, and the number of days remaining on the license.
Table Format	Click to go to the measurements data in table format in the currently selected report.
Error List	Click to go to the list of monitors with error status in the currently selected report.
Warning List	Click to go to the list of monitors with warning status in the currently selected report.
Good List	Click to go to the list of monitors with good status in the currently selected report.
Uptime Summary	Summarizes the time, in percentage terms, terms that each monitor was operational, in error status, and in warning status recorded for the period of the report. It also shows the latest status of the monitor before the report was generated.
Measurement Summary	A summary, in percentage terms, of the average and maximum measurements or values recorded for the period of the report. It also shows the latest percentage for each measurement before the report was generated.
<Measurement Graphs>	Measurement data in graph format for each monitored instance for the period of the report.



GUI Element	Description
<Measurement Tables>	Measurement data in table format, shown at 30 minute increments, for each monitored instance for the period of the report. Entries highlighted in red or yellow indicate that the measurement exceeded the error or warning status threshold for the monitor. Blue indicates that the monitor was disabled.
<Error List Table>	Lists the monitor instances that exceeded the error status threshold for the monitor. Entries are highlighted in red.
<Warning List Table>	Lists the monitor instances that exceeded the warning status threshold for the monitor. Entries are highlighted in yellow.
<Good List Table>	Lists the monitor instances that were in the good status threshold for the monitor. Entries are highlighted in green.








Annotation Tool



Description	<p>Enables you to annotate a snapshot of the report you are viewing, to highlight important areas. The Annotation Tool is available when viewing Baseline Monitor Measurements Graphs and Server-Centric Reports.</p> <p>The Annotation Options enable you to customize your snapshot. The Annotation Menu Bar contains elements that enable you to:</p> <ul style="list-style-type: none"> ▶ Change the appearance of the snapshot. ▶ Save, print, or email an annotation report. ▶ Customize the appearance of text annotated onto your snapshot. These elements are enabled only when the Text Tool button  is selected. <p>To access: Click the Annotate button  on the right side of the page.</p>
Important Information	<p>To use the Annotation Tool, the Sun JRE plug-in 1.6.0_x (latest version recommended) must be installed on your machine. If the plug-in is not installed on your machine, you are prompted to install it.</p>
Useful Links	<p>“Generating a Server-Centric Report” on page 416</p> <p>“Server-Centric Report” on page 440</p> <p>“Setting Status Thresholds Using a Baseline” on page 478</p>

Annotation Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Click to navigate the snapshot.
	Click to select a specific area of the snapshot.












GUI Element (A-Z)	Description
	<p>Click to add a shape to the snapshot. Clicking the shape tool button enables the following shape buttons:</p> <ul style="list-style-type: none"> ▶  Click to mark an area of the snapshot with a rectangle. ▶  Click to mark an area of the snapshot with a filled rectangle. ▶  Click to mark an area of the snapshot with an oval. ▶  Click to mark an area of the snapshot with a filled oval. ▶  Click to mark an area of the snapshot with a round rectangle. ▶  Click to mark an area of the snapshot with a filled round rectangle. <p>Customization. After selecting this button, you can customize your line appearance through the following parts of the interface:</p> <ul style="list-style-type: none"> ▶ Line Type. Choose the type of line you want to add. Options include: <ul style="list-style-type: none"> ▶ Solid Line ▶ Jagged Line ▶ Line Width. Select the width of the line, in pixels, in the annotation.












GUI Element (A-Z)	Description
	<p>Click to enable the line tool, which marks the selected area of the snapshot with a line.</p> <p>Customization. After selecting this button, you can customize your line appearance through the following parts of the interface:</p> <ul style="list-style-type: none"> ▶ Line Style. Choose the style of line you want to add. Options include: <ul style="list-style-type: none"> ▶ Regular line ▶ Line with endpoints ▶ Line with arrows ▶ Line Type. Choose the type of line you want to add. Options include: <ul style="list-style-type: none"> ▶ Solid Line ▶ Jagged Line ▶ Line Width. Select the width of the line, in pixels, in the annotation.
	<p>Click to add text to the snapshot.</p> <p>Example: Add, This is the problematic transaction above a line marking an area of the report.</p>

GUI Element (A–Z)	Description
Border and Fill Colors	<p>Select the relevant square to choose the color of the border and fill of your annotations. The available squares are:</p> <ul style="list-style-type: none"> ▶ Upper Square. Click to choose the color of lines, as generated by the line tool and displayed in unfilled shapes. ▶ Lower Square. Click to choose the color to fill shapes. Clicking either of the squares generates a dialog box with the following tabs where you choose the color: <ul style="list-style-type: none"> ▶ Swatches ▶ HSB ▶ RGB
Opacity	<p>Slide the opacity bar to choose the darkness level of the selected shape line, text line, or shape color in the annotation.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▶ A higher opacity percentage means that the selection appears darker. A lower opacity percentage means that the selection appears lighter. ▶ This field is enabled when either the shape tool, line tool, or text tool button is selected.

Annotation Menu Bar

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	<p>Click to save the snapshot on your local machine.</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ The snapshot is saved in .png format. ➤ You cannot select the New Folder icon  when saving in the My Documents directory or any of its subdirectories.
	<p>Click to select all of the annotations added to your snapshot.</p>
	<p>Click to clear all annotations.</p>
	<p>Click to undo the most recent action performed on the snapshot.</p>
	<p>Click to redo the most recent action performed on the snapshot.</p>
	<p>Click to bring the snapshot view closer.</p>
	<p>Click to set the snapshot view further away.</p>
	<p>Click to restore the snapshot to its original size.</p>
	<p>Click to print the snapshot.</p>
	<p>Click to send the snapshot via email.</p>

GUI Element (A–Z)	Description
	Click to upload the snapshot to the Report Repository. For details on the Report Repository, see “Report Manager Overview” on page 92. Note: This option is not available when accessing the Annotation Tool from the SiteScope feature.
	Click for help.
	Click to mark the text as bold. Note: This field is enabled only when selecting the Text Tool button  .
	Click to mark the text as italicized. Note: This field is enabled only when selecting the Text Tool button  .
	Click to mark the text as underlined. Note: This field is enabled only when selecting the Text Tool button  .
Anti-aliasing	Select to make adjust the pixel reading of text or annotation lines so that they appear smoother. Note: This field is only enabled when selecting the Text Tool button  .
	Select the font for the text in the report. Note: This field is only enabled when selecting the Text Tool button  .
	Select the size of the font in the report. Note: This field is only enabled when selecting the Text Tool button  .

Part IX

Advanced Information

52

Using Regular Expressions

SiteScope makes use of regular expressions to match text content. Several SiteScope monitors enable for content matching on the text returned from a monitor's request or action. This chapter includes reference information on using regular expressions to match text content in SiteScope monitors.

This chapter includes:

Reference

- ▶ Regular Expressions Overview on page 1494
- ▶ Defining a Regular Expression on page 1495
- ▶ Matching String Literals on page 1497
- ▶ Matching Patterns with Metacharacters on page 1499
- ▶ Search Mode Modifiers on page 1503
- ▶ Retaining Content Match Values on page 1505
- ▶ SiteScope Date Variables on page 1506
- ▶ Examples for Log File Monitoring on page 1511
- ▶ Problems Working with Regular Expressions on page 1516

Regular Expressions Overview

Regular expressions is a name given to a text parsing tool that was developed for use with scripting languages such as Awk and Perl as well as several programming environments such as Emacs, Visual C++, and Java. Regular expressions themselves are not a programming language. They do, however, make use of many special combinations of characters and symbols that often make them more difficult to interpret than some programming languages. The many different combinations of these special characters, known as metacharacters, make regular expressions a very powerful and flexible tool for parsing and isolating specific text within a larger body of text.

Including a regular expression in the **Match Content** text box of a monitor instructs SiteScope to parse the text returned to the monitor when it is run and look for content that satisfies the pattern defined by the regular expression. This document presents an overview of the syntax and metacharacters used in regular expressions for use in matching content for SiteScope monitors.

Defining a Regular Expression

The element of a match content expression in SiteScope is the forward slash (/) character. Entries in the **Match Content** text box of a SiteScope monitor must start and end with a forward slash to be recognized as regular expressions. For example, entering the expression `/website/` into the **Match Content** box of a monitor instructs SiteScope to search the text content received by the monitor for the literal text string: `website`. If a match is not found, the monitor reports an error status. When a match is found, the monitor reports a good status as long as all other monitor status threshold conditions are also met. If you type text or other characters into the **Match Content** box without delimiting the entry with forward slashes, the entry is either ignored or reported as a content match error by SiteScope.

Adding parentheses () within the forward slashes surrounding the regular expression is another very useful function for regular expressions in SiteScope. The parentheses are used to create a "back reference." As a back reference, SiteScope retains what was matched between the parentheses and displays the text in the **Status** field of the monitor detail page. This is very useful for troubleshooting match content. This is also a way to pass a matched value from one monitor to another or from one step of a URL Sequence Monitor to the next step of the same transaction. Parentheses are also used to limit alternations, as discussed below.

Generally, it is best to use an iterative approach when building regular expressions for content matching with SiteScope. The following are some general steps and guidelines for developing regular expressions for content matches:

- Create a regular expression using literal characters to match a single sample of the data you want to monitor. For example, `/value: 1022.5/`.
- Iteratively replace literal characters with character classes and metacharacters to generalize the literal into a pattern. For example, the literal in the example above could be changed to: `/value:\s\d\d\d\d\d.\d/` to match any four digits, a decimal point, and one more digit.

- ▶ Consider that the pattern of the data you want to match may vary. Adjust your pattern to match expected or possible variations in the target data. Continuing with the example used above, the expression `/value:\s\d\d\d\d\d\d\d\d/` might become `/value:\s[d]{1,8}\.[d]{1,2}/`. This pattern allows for variation in the number of digits to the left of the decimal point and the number of digits to the right of the decimal point. It expects that there is a decimal point. See the following sections for more information about the character classes used here.
- ▶ Consider that the literal string or pattern you want to match may appear more than once in the content. Identify unique content that precedes the content you want to match, and add regular expression patterns to ensure that the expression matches that unique content before it tries to match the content you are trying to monitor. In the example used here, the pattern may match the first of several entries that have a similar `/value: numbers/` pattern. By adding a literal to the pattern that matches some static content that delimits the particular data can be used to be sure the match is made for the target data. For example, if the data you want to match is preceded by the text `Open Queries`, this literal can be added to the pattern, along with a pattern for any intervening content: `/Open Queries[\s\W]{1,5} value:\s[d]{1,8}\.[d]{1,2}/`.

The following sections describe many of the different elements and patterns that can be used for creating regular expressions for content matching.

Matching String Literals

Finding and matching an exact or literal string is the simplest form of pattern matching with regular expressions. In matching literals, regular expressions behave much as they do in search/replace in word processing applications. The example above matched the text Web site. The regular expression `/Buy Now/` succeeds if the text returned to the monitor contains the characters Buy Now, including the space, in that order.

Note that regular expressions are, by default, **case-sensitive** and **literal**. This means that the content must match the expression in case and order, **including non-alphanumeric** characters. For example, a regular expression of `/Website/`, without any modifiers, succeeds only if the content contains the string Website exactly but fails even if the content on the page is `website`, `WEBSITE`, or `Web site`. (In the last case the match fails because there is space between the two words but not in the regular expression.)

There are cases where you may want to literally match certain non-alphanumeric characters which are special "reserved" metacharacters used in regular expressions. Some of these metacharacters may conflict with important literals that you are trying to match with your regular expression. For example, the period or dot symbol (`.`), the asterisk (`*`), the dollar sign (`$`), and back slash (`\`) have special meanings within regular expressions. Because one of these characters may be a key part of a particular text pattern you are looking for, you must "escape" these characters in your regular expression so that the regular expression processing treats them as literal characters rather than interpreting them as special metacharacters. To force any character to be interpreted as a literal rather than a metacharacter, add a back slash in front of that character.

For example, if you wanted to find the string 4.99 on a Web page you might create a regular expression of `/4.99/`. While this matches the string 4.99, it would also match strings like 4599 and 4Q99 because of the special meaning of the period character. To have the regular expression interpret the period as a literal, escape the period with a forward slash as follows: `/4\.99/`. You can add the back slash escape character in front of any character to force the regular expression processing to interpret the character following the back slash as a literal. In general, use this syntax whenever you want to match any punctuation mark or other non-alphanumeric character.

Using Alternation

Alternation allows you to construct either/or matches where you know that one of two or more strings should appear in the content. The alternation character is the vertical pipe symbol ("|"). The vertical pipe is used to separate the alternate strings in the expression. For example, the regular expression `/(e-mail|e-mail|contact us)/` succeeds if the content contains any one of the three strings separated by the vertical pipes. The parentheses are used here to delimit alternations. In this example, there are no patterns outside of the alternation that must be matched. In contrast, a regular expression might be written as `/(e-mail|e-mail|contact) us/`. In this case, the match succeeds only when any of the three alternates enclosed in the parentheses is followed immediately by a single white space and the word `us`. This is more restrictive than the previous example, but also shows how the parentheses limit the alternation to the three words contained inside them. The match fails even if one or more of the alternates are found but the word "us" is not the next word.

Matching Patterns with Metacharacters

Often you may not know the exact text you need to match, or the text pattern may vary from one session or from one day to another. Regular expressions have a number of special metacharacters used to define patterns and match whole categories of characters. While matching literal alphanumeric characters seems trivial, part of the power of regular expressions is the ability to match non-alphanumeric characters as well. Because of this, it is important to keep in mind that your regular expressions need to account for the presence of non-alphanumeric characters in the content you are searching. This means that characters such as periods, commas, hyphens, quotation marks and even white spaces, must be considered when constructing regular expressions.

Metacharacters Used in Regular Expressions

Metacharacter	Description
<code>\s</code>	Matches generic white space (that is, the Spacebar key). This metacharacter is particularly useful when combined with a quantifier to match varying numbers of white space positions that may occur between words that you are looking to match.
<code>\S</code>	Matches characters that are NOT white space. Note that the <code>\S</code> is capitalized versus the small <code>\s</code> used to match white space.
<code>.</code>	This is the period or dot character. Generally, it matches all characters. SiteScope considers the dot as a form of character class on its own and therefore it should not be included inside the square brackets of a character class.
<code>\n</code>	Matches the linefeed or newline character.
<code>\r</code>	Matches the carriage return character.
<code>\w</code>	Matches non-white space word characters, the same as what is matched by character class <code>[A-Za-z0-9_]</code> . It is important to note that the <code>\w</code> metacharacter matches the underscore character but not other punctuation marks such as hyphens, commas, periods, and so forth.

Metacharacter	Description
\W	Matches characters other than those matched by \w (lower case). This is particularly useful for matching punctuation marks and non-alphabetic characters such as ~!@#\$\$%^&*()+={[]];and including the linefeed character, carriage return, and white space. It does not match the underscore character which is considered a word constituent matched by \w.
\d	Matches digits only. This is equivalent to the [0-9] character class.
\D	Matches non-numeric characters (what \d does not match) plus other characters. Similar to \W but also matches on alphabetic characters. In SiteScope, this generally matches everything, including multiple lines, until it encounters a digit.
\b	Requires that the match have a word boundary (usually a white space) at the position indicated by the \b.
\B	Requires that the match not have a word boundary at the position indicated.

Defining Character Classes

An important and very useful regular expression construct is the character class. Character classes provide a set of characters that may be found in a particular position within a regular expression. Character classes may be used to define a range of characters to match a single position or, with the addition of a quantifier, may be used to universally match multiple characters and even complete lines of text.

Character classes are formed by enclosing any combination of characters and metacharacters in square brackets: `[]`. Character classes create an "any-or-all-of-these" group of characters that may be matched. Unlike literals and metacharacters outside character classes, the physical sequence of characters and metacharacters within a character class has no effect on the search or match sequence. For example, the class `[ABC0123abc]` matches the same content as `[0123abcABC]`.

The hyphen is used to further streamline character classes to indicate a range of letters or numbers. For example, the class `[0-9]` includes all digits from zero to nine inclusive. The class `[a-z]` includes all lower case letters from a to z. You can also create more restrictive classes with the hyphen such as `[e-tE-T]` to match upper or lower case letters from E to T or `[0-5]` to match digits from zero to five only.

The caret character (^) can be used within a character class as a negation or to exclude certain characters from a content match.

Example Character Classes

Example	Description
<code>[a-zA-Z]</code>	This matches any alphabetic character, both upper case and lower case, from the letter a to the letter z. To match more than one character, append a quantifier after the character class as described below.
<code>[0-9]</code>	This matches any digit from 0 to 9. To match more than one digit, append a quantifier after the character class as described below.
<code>[\w\s]</code>	This matches any alphanumeric character and/or any white space.
<code>[\w^_]</code>	This matches any alphanumeric character, excluding the underscore.

Using Quantifiers

Another set of metacharacters used in regular expressions provides character counting options. This adds a great deal of power and flexibility in content matching. Quantifiers are appended after the metacharacters and character classes described above to specify against which positions the preceding match character or metacharacter should be matched. For example, in the regular expression `/(contact|about)\s+us/`, the metacharacter `\s` matches on a white space. The plus sign quantifier following the `\s` means that there must be at least one white space between the words `contact` (or `about`) and `us`.

The following table describes the quantifiers available for use in regular expressions. The Quantifier applies to the single character immediately preceding it. When used with character classes, the quantifier is placed outside the closing square bracket of the character class. For example: `[a-z]+` or `[0-9]*`.

Quantifier	Description
?	The question mark means the preceding character or character class may appear once but is optional and not required to appear in the position indicated.
*	The asterisk requires that any number of the preceding character or character class appear in the designated position. This includes zero or more matches. Note: Care must be used in combining this quantifier with the dot (<code>.</code>) metacharacter or a character class including the <code>\W</code> metacharacter, as these are likely to "grab" more content than anticipated and cause the regular expression engine to use up all of the available CPU time on the SiteScope server.

Quantifier	Description
+	The plus sign requires that the preceding character or character class appear at least once.
{min,max}	Using curly braces creates a quantifier range. The range enumerator digits are separated by commas. This construct requires that the preceding character or character class appear at least as many times as specified by the min enumerator up to but no more than the value of the max enumerator. The match succeeds as long as there are at least as many matches as specified by the min enumerator. However, the matching continues up to the number of times specified by the max enumerator or until no more matches are found.

Match content in SiteScope is run against the entire HTTP response, including the HTTP header, which is not normally viewable by using the browser. The HTTP header usually contains several lines of text including words coupled with sequences of numbers. This may cause failure of some otherwise simple content matching on short sets of numbers and letters. To avoid this, identify a unique sequence of characters near the text you are trying to match and include them as literals, where applicable, in the regular expression.

Search Mode Modifiers

Regular expressions used in SiteScope may include optional modifiers outside of the slashes used to delimit the expression. Modifiers after the ending slash affect the way the matching is performed. For example, regular expression of `/website/i` with the `i` search modifier added makes the match content search insensitive to upper and lower case letters. This would match either `website`, `Website`, `WEBSite`, or even `WEBSITE`.

With the exception of the `i` modifier, some metacharacters and character classes can override search mode modifiers. In particular, the dot (`.`) and the `W` metacharacters can override the `m` and `s` modifiers, matching content across multiple lines despite the modifier.

More than one modifier can be added by concatenating them together after the closing slash of the regular expression. For example: `/matchpattern/ic` combines both the `i` and `c` modifiers.

Regular Expression Match Mode Modifiers

Mode Modifier	Description
<code>/i</code>	Ignore case mode. This makes the search insensitive to upper case and lower case letters. This is a useful option especially when searching for matches in the text content of Web pages.
<code>/c</code>	The matched pattern must NOT appear anywhere in content that is being searched. This is a "complement" match, returning an error if the pattern IS found, and succeeding if the pattern is NOT found.
<code>/m</code>	Match across multiple lines WITHOUT ignoring intervening carriage returns and linefeeds. With this modifier you may still need to account for possible linefeeds and carriage returns with a character class such as <code>[\w\W]*</code> or <code>[\s\S\n\r]*</code> . The <code>.*</code> does not match carriage returns or linefeed characters with this modifier.
<code>/s</code>	Consider the content as being on a single line, ignoring intervening carriage returns and linefeed characters. With this modifier, both the <code>[\w\W]*</code> character class and the <code>.*</code> pattern match across linefeeds and carriage returns.

Retaining Content Match Values

Some monitors, like the URL Monitor and URL Sequence Monitor, have a content match value that is logged and can be used to set error status thresholds. Another purpose of the parentheses `/(match pattern)/` used in regular expression syntax is to determine which text is retained for the Content Match Value. You use this function to use content match values directly as thresholds for determining the error threshold of a URL monitor or URL Sequence monitor.

For example, if the content match expression was

```
/Copyright (\d*)/
```

and the content returned to the monitor by the URL request included the string:

```
... Copyright 2007 by HP
```

then the match is made and the retained content match value would be:

```
2007
```

Under the error-if option at the bottom of the monitor set up page, you could then change the error-if condition from the default of `status != 200` to content match, then specify the relational operator as `!=`, and then specify the value 1998. This sets the error threshold for this monitor so that whenever the year in the string Copyright is other than 1998, the monitor reports an error. This mechanism could be used to watch for unauthorized content changes on Web pages.

Checking a Web page for links to other URLs can be an important part of constructing URL Sequence Monitors. The following regular expression can be used to match the URL text of a link on a Web page:

```
/a href="?([:\W\s\d\.]*)"?/i
```

This expression matches the `href="protocol://path/URLname.htm"` for many URLs. The question mark modifiers enable the quotation marks around the `HREF=` attribute to be optional. The `i` modifier allows the match pattern to be case-insensitive.

Retained or remembered values from content matches can be referenced and used as input for subsequent steps in a URL Sequence Monitor. See the Match Content section of the URL Sequence Monitor for the syntax used for Retaining and Passing Values Between Sequence Steps.

SiteScope Date Variables

SiteScope uses specially defined variables to create expressions that match the current date or time. These variables can be used in content match fields to find date-coded content. The General Date Variables are useful for matching portions of various date formats. The Language/Country Specific Date Variables enable you to automatically extend the language used for month names and weekday names to specific countries, based on ISO codes.

General Date Variables

The following table lists the general variables:

Variable	Range of Values
\$hour\$	0 - 23
\$minute\$	0 - 59
\$month\$	1 - 12
\$day\$	1 - 31
\$year\$	1000 - 9999
\$shortYear\$	00 - 99
\$weekdayName\$	Sun - Sat
\$fullWeekdayName\$	Sunday - Saturday
\$0hour\$	00 - 23
\$0minute\$	00 - 59
\$0day\$	01 - 31 (two-digit day format)
\$0month\$	01 - 12 (two-digit month format)

Variable	Range of Values
\$monthName\$	Jan - Dec (three-letter month format in English)
\$fullMonthName\$	January - December
\$ticks\$	milliseconds since midnight, January 1, 1970

For example, if the content match search expression was defined as:

```
/Updated on $0month$V$0day$V$shortYear$/
```

and the content returned by the request includes the string:

```
Updated on 06/01/98
```

then the expression would match when the monitor is run on June 1, 1998. The match fails if the content returned does not contain a string matching the current system date or if the date format is different than the format specified.

If you want the time to be before or after the current time, you can add a **\$offsetMinutes=mmmm\$** to the expression, and this offsets the current time by **mmmm** minutes (negative numbers are allowed for going backwards in time) before doing the substitutions.

For example, if the current day is June 1, 1998, and the search expression is:

```
/$offsetMinutes=1440$Updated on $0month$V$0day$V$shortYear$/
```

the content string that would match would be:

```
Updated on 06/02/98
```

Note that the date is one day ahead of the system date.

Language/Country Specific Date Variables

The following table lists the SiteScope special variables for use with international day and month name matching. The characters LL and CC are placeholders for two-letter ISO 639 language code characters and two-letter ISO 3166 country code characters (see the notes below the table for more details).

Variable	Range of Values
\$weekdayName_LL_CC\$	Abbreviated weekday names for the language (LL) and country (CC) specified (see notes below).
\$fullWeekdayName_LL_C C\$	Full weekday names for the language (LL) and country (CC) specified.
\$monthName_LL_CC\$	Abbreviated month names for the language (LL) and country (CC) specified.
\$fullMonthName_LL_CC\$	Full month names for the language (LL) and country (CC) specified.

CC - an uppercase 2-character ISO-3166 country code. Examples are: DE for Germany, FR for France, CN for China, JP for Japan, BR for Brazil. You can find a full list of these codes at a number of Internet sites, such as: <http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html>.

LL - a lowercase 2-character ISO-639 language code. Examples are: de for German, fr for French, zh for Chinese, ja for Japanese, pt for Portuguese. You can find a full list of these codes at a number of Internet sites, such as: <http://www.ics.uci.edu/pub/ietf/http/related/iso639.txt> or <http://www.dsv.su.se/~jpalme/ietf/language-codes.html>.

For example, if the content match expression was defined as:

```
/$fullWeekdayName_fr_FR$/i
```

and the content returned by the request includes the string:

```
mercredi
```

then this expression would match when the monitor was run on Wednesday.

If you are not concerned with the country-specific language variations, it is possible to use any of the above variables without including the country code. For example:

```
/$fullWeekdayName_fr$/
```

could be used to match the same content as `/$fullWeekdayName_fr_FR$/`.

Special Substitution for Monitor URL or File Path

SiteScope Date Variables are useful for matching content as part of a regular expression. The date variables can also be used as a special substitution to dynamically create URLs or file paths for specific monitors. This is useful for monitoring date-coded files and directories where the URL or file path is updated automatically based on system date information. SiteScope is an example of an application that creates date-coded log files. The log file names include some form of the year, month, and day as part of the file name, such as `File2001_05_01.log`, where the year, month, and date are included.

Based on this example, a new file is created each day. Monitoring the creation, size, or content of the current days file would normally require the file path or URL of the monitor to be manually changed each day. Using the SiteScope date variables and special substitution, SiteScope can automatically update the file path to the current day's log file. By knowing the pattern used in naming the files, you can construct a special substitution string similar to a regular expression that substitutes portions of the system date properties into the file path or URL.

For example if the absolute file path to the current day's log file in a file monitor is:

```
D:/Production/Webapps/Logs/File2001_05_01.log
```

the log file for the following day would be:

```
D:/Production/Webapps/Logs/File2001_05_02.log
```

You can construct a special substitution expression to automatically update the file path used by the monitor, with the following syntax:

```
s/D:\Production\Webapps\Logs\File$year$_$0month$_$0day$.log/
```

The substitution requires that the expression start with a lower-case `s` and that the expression is enclosed by forward slashes `/.../`. Forward slashes that are part of the file path must be escaped by adding the back slash (`\`) character as shown. The SiteScope date variables are separated by the underscore character literals. SiteScope checks the system time properties each time the monitor runs and substitutes with applicable values into the file path or URL before accessing the file.

SiteScope monitor types that support the special substitution are:

- eBusiness chain
- File Monitor
- Log Monitor
- URL Monitor
- URL Sequence Monitor
- Web server monitor

While the special substitution syntax is similar in syntax to the substitution syntax used in regular expressions, they are not the same. While all of the SiteScope date variables can be used in match content regular expressions, the special substitution discussed here can not be used as part of a match content expression.

Examples for Log File Monitoring

SiteScope's Log File Monitor and File Monitor check for entries in files created by other applications. These files may be data files created by a third-party application or they may be logs created by a custom system specially designed for your environment. Where the logs or files are written with a known, predictable format, SiteScope can be configured to regularly check the files for new entries and match on specific content strings. The following are several examples of log file entries and simple regular expression patterns that can be used to check the entries. You can use these examples or modify them to work with a specific case.

Note: All regular expressions must be entered on a single line in SiteScope. Some of the examples below may break across more than one line to fit on this page.

Searching Paths for Log Files

UNIX and Windows operating systems treat the case (“N” versus “n”) of file names in incompatible ways. Windows operating systems are case insensitive which means that when a file is being searched, its case is ignored. UNIX operating systems are case sensitive which means that the case of a name is significant at all times. To avoid log file errors when using regular expressions to search for path names on UNIX operating systems, you should use markers to change the character case in the path expression.

Marker	Description
\$L	Allows changing characters between the \$L marker and the \$E marker to lower case.
\$U	Allows changing characters between the \$U marker and the \$E marker to upper case.
\$E	The end marker used for changing character case.

Example

If you define the following path expression:

```
s/\tmp/logs/arcv.log.$weekdayName$/
```

for the `/tmp/logs/arcv.log.tue` log file on a Linux machine, you will get a log file error because SiteScope tries to find `tmp/logs/arcv.log.Tue`, and Linux is case sensitive.

To resolve this problem, define the path expression as follows:

```
s/>\tmp\logs\arcv.log.$L$weekdayName$$E/
```

The monitor converts the characters between `$L` and `$E` to lower case, `/tmp/logs/arcv.log.tue`.

Conversely, use `$U` and `$E` to allow SiteScope to change the characters between the markers to upper case. For example, if you define the path expression:

```
s/>\tmp\logs\arcv.log.$L$weekdayName$$E/
```

the monitor converts the path to `/tmp/logs/arcv.log.TUE`.

You can use `$L` and `$U` multiple times in a path expression, and you can use them both in the same expression.

For example:

```
s/\tmp/logs-$L$weekdayName$$E\arcv.log.$U$weekdayName$$E/
```

converts the path to `/tmp/logs-tue/arcv.log.TUE`

```
s/\tmp.$L$monthName$$E/logs-$L$weekdayName$$E\arcv.log.$U$weekdayName$$E/
```

converts the path to `/tmp.mar/logs-tue/arcv.log.TUE`

Matching Comma-Separated Values

The following is an example of log file entries that are comma-separated strings of digits and letters:

```
new,open,changed,12>alerts
new,open,changed,13>alerts
new,open,changed,13>alerts
new,open,changed,14>alerts
```

A regular expression to match on log file entries that are comma-separated strings of digits and letters.

```
/([\w\d]+,[\w\d]+,[\w\d]+,[\w\d]+)[\n\r]?/
```

Note: If the file entries include punctuation marks such as an underscore or a colon, add that character explicitly to the `[\w\d]` class pattern. For example, to include a colon character, change each of the `[\w\d]` patterns to `[\w\d:]`.

Matching Whitespace Separated Values

The following is an example of log file entries that are a sequence of strings and digits separated by spaces:

```
requests 12 succeeded 12 failed
requests 12 succeeded 12 failed
requests 11 succeeded 11 failed
requests 12 succeeded 12 failed
requests 10 succeeded 10 failed
```

The following is a regular expression to match on log file entries that are a sequence of strings and digits separated by spaces.

```
/([\w\d]+\s+[\w\d]+\s+[\w\d]+\s+[\w\d]+\s+[\w\d]+)[\n\r]?/
```

Note: The use of the + character forces the match to include the number of sequences per line included in the match pattern: in this example, five word or number sequences per line of the log file. If the sequences include punctuation marks such as an underscore or colon, add that character explicitly to the `[\w\d]` class pattern. For example, to include a colon character, change each of the `[\w\d]` patterns to `[\w\d:]`.

Matching and Retaining the Numbers in a Line of Text and Numbers

The following is an example of log file entries that are comma separated strings that combine digits and letters:

```
request handle number 12.56, series 17.5, sequence reported 97.45, 15.95 and 19.51
request handle number 15.96, series 27.5, sequence reported 107.45, 25.95 and 19.52
request handle number 11.06, series 36.5, system codes 9.45, 35.95 and 19.53
log reference number 12.30, series 17.5, channel reset values 100.45, 45.95 and 19.54
```

The following is a regular expression to match on log file entries that are comma-separated strings that combine digits and letters and retain the decimal numeric data:

```
/[, \w\s]+(d+\.\d+)[, \w\s]+(d+\.\d+)[, \w\s]+(d+\.\d+)[, \w\s]+(d+\.\d+)[, \w\s]+(d+\.\d+)[\n\r]?/
```

Note: If the file entries include punctuation marks such as an underscore or colon, add that character explicitly to the `[\w\s]` class pattern. For example, to include a colon character that appears embedded in the text sequences, change each of the `[\w\s]` patterns to `[,:\w\s]`.

The following example uses the SiteScope date variables to match on a more restricted set of entries that were created on the same day, month, year, and within the same hour as indicated by the system clock of the server on which SiteScope is running.

```
/$0day$V$0month$V$year$\s+$0hour$:d+:d+,[\w\d]+,[\w\d]+/
```

Problems Working with Regular Expressions

- ▶ Using the .* construct. This match construct presents a very large number of possible matches on any page of content. The use of the .* construct is known to cause the regular expression-matching engine used by SiteScope to take over all available CPU cycles on the SiteScope server. If this occurs, SiteScope is unable to function and must be restarted each time the monitor with the offending regular expression is run, until the expression has been corrected.

Note: Regular expression matching is run against the entire text content returned to the SiteScope monitor request. This includes HTTP headers that are normally not viewable in the browser window (for example, not visible using the **View > Source** option). This also means that you must account for other information that may not be displayed in the browser view. This includes text in META tags used by Internet search engines as well as client side-scripts.

- ▶ Text matching is done against the code lines of the script and not against the browser's output from the script for URLs that contain client side-scripts, such as Javascript. This means that if the script dynamically writes or replaces text on the Web page with values calculated by the script, it may not be possible to match this content with regular expressions. If the script is only changing text, you may be able to match the corresponding text strings that appear in the script code. A further pitfall would be that you are trying to check that a certain condition was met in the browser but the matching text string appears in the script content regardless of any user action.

- ▶ A regular expression match succeeds as soon as the minimum match requested is satisfied. After a match is made, no further matching is performed. Therefore, regular expressions are not well suited to count the number of occurrences of a repeating text pattern. For example, if you want to check a Web page with a catalog list of items and each item has a link next to it saying Buy Now! and you want to make sure that at least five items are listed, a regular expression of /Buy Now!/ would succeed in matching only the first Buy Now!. Likewise, if your regular expression searches the word catalog on the main browser screen, the match may succeed if the word appears as a META tag in the HTML header section or if it appears as a hyperlink in a site navigation menu that appears in the content before the occurrence you intend to match.
- ▶ Forgetting to account for non-alphanumeric content. Regular expressions need to be written to account for all of the characters that are and may be present. This includes white space, linefeed, and carriage returns. This is not normally a problem when matching a single-word literal. It can be a challenge when you need to create a match of several words separated by unknown amounts of white space and other non-alphanumeric characters and possibly span more than one line. The `[\s\n\r]+` character class can be useful between words used in the expression. Always check the format of the content you are trying to match to look for patterns and special characters, such as periods, commas, and hyphens, that may cause a seemingly simple match to fail.
- ▶ The use of excessive metacharacters can lead to problems. In some cases, overly generous quantifiers combined with the `.` or `\W` metacharacters can grab content that you were intending to match with a literal string elsewhere in your regular expression resulting in a match failure. For example, the following might be used to match the URL content of the hyperlink anchor reference: `/a href="([\W\w\s]*)"/`. When the monitor performs the check for this regular expression, however, the match grabs the first occurrence of the pattern `/a href="...` and continues matching multiple lines of text up to the last quotation mark found on the page. Without some other unique ending delimiter, the `[\W\w\s]*` class and quantifier combination is too excessive. A more successful syntax that narrows the class of expected characters would be: `/a href="?([:\W\w\s\d\.]*)"?`

Example Regular Expression Syntax

The following are some examples of syntax for use in regular expressions:

Example Expression	Description
<code>/CUSTID\s?=\s?([A-Z0-9]{20,48})/</code>	This example matches an ID string that is made of 20 or more digits and upper-case letters with no spaces or other non-alphanumeric characters. The <code>\s?</code> construct allows a white space on either side of the equals sign. Using the parentheses around the character class instructs SiteScope to retain this value (up to the maximum of 48 characters) as a content match value and the matched value is displayed in the monitor detail status column.
<code>/ahref="?([:\w\s\d\.]*)"?/i</code>	This example matches the URL string in an HTML hyperlink. The <code>"?</code> construct makes a quotation mark on either end of the URL string optional. Using the parentheses instructs SiteScope to retain this value as a content match value and the value is displayed in the monitor status. The <code>i</code> modifier tells the search to treat upper- and lower-case letters equally.
<code>/"[^"]*"/</code>	This example matches text sequences that are contained between quotation marks. Note the use of the negation caret (<code>^</code>) to define a character class of all characters other than the quotation mark.

As with programming and scripting languages, there is almost always more than one way to construct a regular expression to accomplish a particular match. There is not one right way to build regular expressions. You should plan to test and modify regular expressions as necessary until you get the results you need.

For an in-depth discussion of Perl regular expressions, consult a book about Perl programming, or find a Perl tutorial on the Web.

53

Monitoring XML Documents

This chapter includes reference information about SiteScope's content matching capabilities for XML documents.

This chapter includes:

Reference

- ▶ Monitoring XML Documents Overview on page 1519
- ▶ Content Matching for XML Documents on page 1520
- ▶ Using XML Content Match Values in Monitor Configurations on page 1522

Monitoring XML Documents Overview

SiteScope's content matching capabilities is an important function in monitoring networked information systems and content. For SiteScope monitors that provide content matching, the basic content matching is available through the use of Perl regular expressions. SiteScope also includes the capability of matching document content by traversing XML documents. For example, you can include an XML match content string using the URL Monitor and Web Services Monitor to match an XML element name, an attribute of an XML element, or the content of an element. You can use this to check for content in XML based Web pages, SOAP or XML-RPC documents, and even WML pages served to WAP-enabled devices.

Content Matching for XML Documents

The syntax of XML match content strings reflects the hierarchal structure of the XML document. Match content strings that start with "xml" are recognized as element names within an XML document. The element names are added, separated by periods, in the order of their relationship to the root element. For example, in the document `weather.xml` the root element is `<weather>`. This element includes child elements named `<area>`, `<skies>`, `<wind>`, `<forecast>`, and so forth. To access the content of these XML elements or their attributes, you would use a syntax like `xml.weather.area`.

To check that specific content or value is present, add an equals sign after the element name whose content you are testing and then add the value of the content. If there are multiple instances of an element name in the document, you can check a particular instance of that element by adding the number indicating the order of the element in the document in square brackets (see the example in the table below). You can also test for multiple elements or values by separating individual search strings with commas. The table below gives several examples of the syntax used to match content in XML documents.

Example Match Content	Description
xml.weather.temperature	Succeeds if any <code><weather></code> node in the document contains one or more <code><temperature></code> elements. The content of the <code><temperature></code> elements is returned by the monitor. If no <code><temperature></code> element is found within the <code><weather></code> node, an error is returned.
xml.weather.temperature=20	Succeeds if any <code><weather></code> node in the document contains one or more <code><temperature></code> elements where the content of the <code><temperature></code> element equals 20. The content of the <code><temperature></code> element is NOT returned by the monitor if the match is found. An error is returned if no <code><temperature></code> element is found within the <code><weather></code> node or if no <code><temperature></code> element contains the value 20.

Example Match Content	Description
xml.weather.forecast.[confidence]	Succeeds if any <weather> node in the document contains a <forecast> element that has an attribute called confidence. The value of the confidence attribute is returned by the monitor if the match is found. An error is returned if no <forecast> element is found within the <weather> node or if no confidence attribute is found.
xml.weather.forecast[3].[confidence]=50	Succeeds if any <weather> node in the document contains three or more <forecast> elements where the third <forecast> element has a confidence attribute with a value of 50. An error is returned if the <weather> node has fewer than three <forecast> elements or if the value of the confidence attribute is not equal to 50.
xml.weather.temperature=20, xml.weather.skies=rain	Succeeds if any <weather> node in the document contains one or more <temperature> elements where the content of the <temperature> element equals 20 AND if any <weather> node contains one or more <skies> elements where the content of the <skies> element equals rain. Returns an error if either of the matches fails.
xml.wml.card.p.table.tr.td.anchor=Home Page	Checks the content of <anchor> elements in the designated path of a WML document. Succeeds if any <card> node containing table cells with one or more <anchor> elements where the content of any of the <anchor> elements equals "Home Page."

Using XML Content Match Values in Monitor Configurations

Monitors like the URL Monitor have a content match value that is logged to the SiteScope monitor data log and can also be used to set error and warning status thresholds for the monitor. The values of the XML names are saved as the content match values for the monitor.

For example, if the match content expression was `xml.weather.temperature` and the document was the contents of the file `weather.xml`, then the content match value would be 46.

You can then set the error, warning, and good status thresholds in the Advanced Options section for the monitor to compare your specific thresholds to the value returned by the content match.

For example, if you were monitoring temperature values and wanted to be alerted when the temperature value dropped below 72 degrees, you could set the monitor status thresholds as follows:

Error if	<code>content match < <= 72</code>
Warning if	<code>content match == <= 72</code>
Good if	<code>content match >= > 72</code>

With this configuration, the monitor would check the content of the temperature element and then compare it to the error and warning thresholds. In the example above, the status of the monitor would be an **error** because the temperature value is 46, which is less than 72.

54

Writing Scripts for Script Alerts

This chapter includes reference information about how to write automated system recovery scripts for use with the SiteScope Script Alert.

This chapter includes:

Reference

- Writing Scripts for Script Alerts Overview on page 1523
- Working with Scripts in SiteScope on page 1524
- Passing Data from SiteScope to a Script on page 1526

Writing Scripts for Script Alerts Overview

SiteScope has the ability to run scripts or batch files when an error or warning status is detected. This is normally done by creating a Script Alert that acts as a trigger for the script. The script or batch file can run any system command or call other programs written in any language. You can use this to create recovery scripts to automatically respond to critical conditions or failures.

Working with Scripts in SiteScope

The script file that a SiteScope Script alert is to run must be located in the **<SiteScope root directory>\scripts** folder or on a remote UNIX machine (for remote scripts). For example, if SiteScope is installed in the directory C:\SiteScope and your script is called `actionTest.bat`, SiteScope tries to run the following command line in response to Script Alerts you have created:

```
C:\SiteScope\scripts\actionTest.bat C:\SiteScope\scripts monitor_name
```

where C:\SiteScope\scripts is the first command line parameter, `monitor_name` is the second command line parameter, and so forth.

Note: While the local script run by the Script Alert must reside in **<SiteScope root directory>\scripts**, the execution path is **<SiteScope root directory>\classes** directory. You should use full paths for any file system commands or programs called by the script to avoid problems with defining the current execution directory.

The action taken by a script is determined by the creator of the script. SiteScope passes several command line arguments to each script called by a Script Alert. You can use this to have program scripts take action based on information sent from SiteScope. By default, SiteScope passes the following parameters to each Script alert as command line arguments:

- The path of the scripts directory.
- The name of the monitor that caused the alert.
- The current status of the monitor.
- The path to the alert message file.
- The Id code of the monitor.
- The group in which the monitor is located.
- Any additional parameters specified in the **Parameters** box in the alert form.

These command line arguments can be accessed by the target script using the normal command line variable conventions. These conventions are %1, %2, %3 and so forth, for Windows NT systems, and \$1, \$2, \$3 and so forth, for UNIX scripts (depending on the scripting shell or language used). The first six parameters (that is, %1 through %6) are passed by default to each script. To pass other parameters, the property variables or parameters must be added to the Script Alert Settings in the Parameters box to make them available to the script. The first variable or text entered in the Parameters box is then accessible as %7 by the script, the second parameter is accessed as %8, and so forth.

An example script written in Perl to access Script Alert parameters:

```
print "pathname to scripts directory: $ARGV[0]\n";  
print "name of monitor causing alert: $ARGV[1]\n";  
print "current status monitor: $ARGV[2]\n";  
print "pathname to alert message file: $ARGV[3]\n";  
print "id code of monitor: $ARGV[4]\n";  
print "group for the monitor: $ARGV[5]\n";
```

The following is an example batch file for Microsoft Windows to echo the parameters passed to the script:

```
echo pathname to scripts directory: %1  
echo name of monitor causing alert: %2  
echo current status monitor: %3  
echo pathname to alert message file: %4  
echo id code of monitor: %5 echo group for the monitor: %6
```

Passing Data from SiteScope to a Script

In addition to the seven default parameters, there are two other mechanisms for passing parameters and data to scripts. One is to use the additional Parameters box in the Script Alert Settings. The other is to access the Alert Message file.

Passing Data Using the Script Alert Settings

The simplest way to send additional custom parameters and data to script is to use the Alert Action wizard. The seventh default parameter passed to the script, which is any additional parameters specified on the alert form, allows you to specify one or more custom parameters to be sent to the script. You specify these in the **Parameters** box in the Script Alert Settings on the Action Types Settings Page of the Alert Action wizard.

These parameters could be hard-coded values. You can include multiple parameters by separating the individual parameters by spaces. For example, assume you want to pass the four text strings shown below to a script. To do this you type them in the Parameters box as follows:

Parameters	customA customB customC customD
------------	---------------------------------

These would then become the seventh (7th) through tenth (10th) command line parameters sent to the script. The following Windows batch file script would print the default parameters as well as the additional example custom parameters entered in the Parameters box of the Action Types Settings Page:

```
echo pathname to scripts directory: %1
echo name of monitor causing alert: %2
echo current status monitor: %3
echo pathname to alert message file: %4
echo id code of monitor: %5
echo group for the monitor: %6
echo seventh parameter(customA): %7
echo eighth parameter(customB): %8
echo ninth parameter:(customC) %9
echo tenth parameter(customD): %10
```

Passing Data Using the Alert Message File

The other method for passing data and SiteScope monitor parameters to a script is to use the Alert Message file. This is a file that is created by SiteScope using the alert template specified in the Alert Action wizard. You can create your own custom alert templates and pass custom text strings or any of the SiteScope parameters available. The following shows the default NTEventLog template included with SiteScope. The parameters marked with < > brackets are replaced with the applicable values to and written to the Alert Message file each time the applicable Script Alert is triggered.

The NTEventLog Script Alert Template

```
Type: <eventType>
Event Time: <eventTime>
Source: <event>
Source ID: <eventID>
Category: <eventCategory>
Machine: <eventMachine>
Message: <eventMessage>
Monitor: <name>
Group: <group>
Sample #: <sample>
Time: <time>
<mainParameters>
<mainStateProperties>
```

To use this data in a script, your script needs to access the Alert Message file at the pathname location specified by the fourth default command line parameter (see “Working with Scripts in SiteScope” on page 1524). Then the script has to parse the content of the Alert Message file to extract the data you want to use in your script.

For more examples of how to write recovery scripts, look at the script files in the <SiteScope root directory>\scripts directory. You can use the **actionTest.bat** example template to create your own script. The **perlTest.pl** example shows how to call a Perl script. The **restartIIS.bat**, **restartService.bat**, and **restartServer.bat** scripts implement common recovery actions.

For the UNIX environment, the examples scripts are called action **Test.sh** and **perlTest.pl**.

55

UNIX Operating System Adapters

This chapter includes the main concepts, tasks, and reference information to enable SiteScope to monitor different versions of UNIX.

This chapter includes:

Concepts

- ▶ SiteScope UNIX Operating System Adapters Overview on page 1530

Tasks

- ▶ Add an Adapter on page 1530

Reference

- ▶ UNIX Adapters Provided with SiteScope on page 1531
- ▶ Adapter File Format on page 1532
- ▶ Adapter Command List on page 1534

SiteScope UNIX Operating System Adapters Overview

You can use SiteScope UNIX operating system adapters to extend SiteScope to connect to, and remotely monitor other versions of UNIX, in addition to those supported by default. This is done by configuring an adapter file to support the particular version of UNIX you want to monitor.

SiteScope uses adapter files to describe the commands that are needed to retrieve a variety of system resource information from servers running different versions of the UNIX operating system. These adapter files are written in plain text and are stored in the **SiteScope/templates.os** directory. For a list of the default UNIX adapters that are provided with SiteScope, see “UNIX Adapters Provided with SiteScope” on page 1531.

You can modify existing adapter files to adjust for specific system requirements in your environment. You can also create your own adapter files to enable SiteScope monitoring of other UNIX versions.

Add an Adapter

This task describes the steps involved in adding an adapter to specific versions of UNIX.

To add a UNIX adapter:

- 1** Read the Adapter Kit documentation thoroughly.
- 2** If the UNIX platform to which you want to add support is similar to one of the default SiteScope-supported UNIX platforms, make a copy of the adapter file for that UNIX version and use that as a starting point for your adapter.
- 3** Modify the adapter file to match the command line requirements for the UNIX version to which you want SiteScope to connect.
- 4** Save your adapter file to the **SiteScope/templates.os** directory. The filename must use the **.config** extension.
- 5** Open the installation SiteScope to which you have added the new adapter file.

- 6 In the left pane, expand **Preferences**. Right-click **UNIX Remote Preference**, and select **New UNIX Server**. The New UNIX Server page opens.
- 7 In the **OS** box, select the name of the UNIX adapter that you have created.
- 8 Click **OK**. SiteScope uses the new adapter file to try and retrieve that applicable data from the remote server.
- 9 If you make changes to the adapter file after you have configured one or more server connection profiles to use the adapter, you can use the **Detailed Test** option in the UNIX Remote Preferences to test your adapter. After adding the remote server, the Detailed Test displays the output of the command that SiteScope is running remotely, along with SiteScope's parsing of the output.

The amount of work required to modify a particular template depends on how different the new UNIX platform is from the supported UNIX platforms.

UNIX Adapters Provided with SiteScope

The default UNIX adapters that are provided with SiteScope, include:

Filename	Description
AIX.config	Adapter file for IBM AIX
Digital.config	Adapter file for Digital Tru64 UNIX (Pre 4.x)
FreeBSD.config	Adapter file for FreeBSD 3.x
HP.config	Adapter file for Hewlett-Packard HP/UX
HP64.config	Adapter file for Hewlett-Packard HP/UX 64-bit
Linux.config	Adapter file for Linux (Redhat and others)
MacOSX.config	Adapter file for Apple Macintosh OS X
OPENSERVER.config	Adapter file for SCO OpenServer
SCO.config	Adapter file for SCO UNIXWare
SGI.config	Adapter file for Silicon Graphics Irix

Filename	Description
Sun.config	Adapter file for Sun Microsystems Solaris
Tru64.config	Adapter file for Compaq Tru64 UNIX 5.x

Adapter File Format

Each UNIX platform supported for remote monitoring by SiteScope has an adapter file in the **SiteScope/templates.os** directory. These files use SiteScope's standard setting file format.

The first group of settings (those settings before the first # sign line) describe the platform:

```
id=yourPlatform
name=your Platform Name
```

The `id` is the SiteScope internal ID for the OS. This ID must be unique, contain no spaces, and can be alphanumeric. It is recommended that you use the name of the adapter file as the ID name. For example, if the name of your adapter file is `linux.config`, your ID would be `linux`.

The `name` is the name you want displayed in the drop-down list when adding or editing remote servers.

The rest of the template file contains groups of settings representing a single command, separated by a line of # characters. For example, the following settings represent the disk space command:

```
id=disks
command=/usr/bin/df -k
mount=6
name=1
```

Where:

`id=disks` is the id that SiteScope uses to look up a command. This must be one of the set of SiteScope commands (see “Adapter Command List” on page 1534). This entry is case sensitive.

`command=/usr/bin/df -k` means that the `usr/bin/df -k` command is run to get the information about the disks.

`mount=6` and `name=1` mean that the mount name is in column 6 and the name of the mount or file system is in column 1. The data names vary from command to command and are documented below.

Applying the above for the following command output:

```
Filesystem kbytes used avail capacity Mounted on /proc 0 0 0 0%
/proc /dev/dsk/c0t3d0s0 73049 42404 23341 65% /
```

where the `disks` command automatically skips lines not starting with `(/dev)` reads column 1 (`/dev/dsk/c0t3d0s0`) as the name of the file system, and column 6 (`/`) as the mount name.

Adapter Command List

SiteScope requires settings for each the following commands to operate properly. Each command description requires an ID and a command, one or more fields to specify where the data is being read from, and optionally a set of modifiers that are used to filter the output of the command to eliminate certain sets of lines (such as header lines).

Where the variable column is used below, it means the number of the column in which the data appears, where columns are space delimited sets of data.

In addition, there are certain fields that can be optionally applied to any command description. For details, see “Optional Adapter Command Details” on page 1538.

Disk Listing

ID	Description	Used by	Fields
disks	Returns a list of the file systems on the system. The <code>/usr/bin/df -k</code> command is the standard way to get this data. Lines returned that do not start with <code>/dev</code> are automatically skipped.	Disk Space Monitor	name. The column of the name of the file system. mount. The column of the name of the mount.

Disk Information

ID	Description	Used by	Fields
disk	Takes a disk as an argument and returns the total, free, and percent used for the disk.	Disk Space Monitor	total. The column of the total kilobytes capacity of the file system. free. The column of the free kilobytes of the file system.

Memory

ID	Description	Used by	Fields
memory	The amount of swap spaced used and available.	Memory Monitor	<p>swapUnit. The multiplier applied to used, free, or total swap space to give bytes.</p> <p>used. The amount of swap space used.</p> <p>free. The amount of swap space free.</p> <p>total. The amount of total swap space.</p> <p>Note: Only two of used, free, and total fields need to read. The other is computed.</p>

Page Faults

ID	Description	Used by	Fields
pageFault	The number of page faults/sec. If multiple page faults lines are matched, they are added up.	Memory Monitor	<p>pageFaults. The column of the number of page faults.</p> <p>inPageFaults. The column of the number of page in faults.</p> <p>outPageFaults. The column of the number of page out faults.</p> <p>units. pages (default), pages/sec, or k/sec units for the paging data.</p> <p>pageSize. If units are k/sec, the pageSize is used to compute the number of pages. Otherwise it is ignored.</p> <p>Note: Either use pageFaults, if there is a single column of data, or inPageFaults and outPageFaults, if there are two columns of page fault data. inPageFaults and outPageFaults are added together to get the total page faults.</p>

CPU Usage

ID	Description	Used by	Fields
cpu	Returns the wait and idle % of the CPU.	CPU Monitor	<p>idle. The idle % for the CPU.</p> <p>wait. The wait % for the CPU (optional).</p>

Process List

ID	Description	Used by	Fields
process	A list of processes with long process names. Typically this is <code>/usr/bin/ps -ef</code>	Service Monitor	name . The column of the names of the processes.

Process List with Details

ID	Description	Used by	Fields
process Detail	A list of processes with size of the process. Typically this is <code>/usr/bin/ps -el</code>	Service Monitor (with Check Memory option enabled)	name . The column of the names of the processes size . The column of the size of the processes. pageSize . Page size on the system (optional). The default is 8192.

Optional Adapter Command Details

The following fields can optionally be applied to any command description:

Process List with Details

ID	Description
startLine	The line number where the command starts looking for data.
endLine	The line number where the command ends looking for data.
skipLine	The pattern that if matched, skips the line.
matchLine	The pattern that if matched, looks for data in that line.
startMatch	The pattern that if matched, starts the command looking for data.
endMatch	The pattern that if matched, ends the command looking for data.
reverseLines	If true, the command output lines are reversed and read back to front. This is useful if there is data at the end of the command and it is too difficult to work out when to start reading.

If a field name has the format, `fieldnameColumnName=COLUMN`, the adapter searches the headers (first line) for `COLUMN` and records the columns containing the data, and then use those settings to read the `fieldname` field. This is useful where the width of the columns varies, and the data has spaces in it.

For example, to read the my data information from the following command output:

```
MEM NAME DESC
12K my data some of my data
```

you would specify the name field in the command description as:

```
nameColumnName=NAME
```

The adapter reads the header line, finds `NAME`, and records where the previous column ends (`MEM` in this case) and where the specified column ends (`NAME`), and uses that to read, in this case, the text in character columns 6 through 22.

To see an example of the `ColumnName` reading in action, look at the `process` and `processDetail` commands for the supported UNIX platforms. They use this method to get the process name and the size of the process.

56

SiteScope Monitoring Using Secure Shell (SSH)

SiteScope supports a number of security capabilities. One of these is support for remote server monitoring using Secure Shell (SSH) connections. You can use SSH to connect to a server and automatically send a command, so that the server runs that command and then disconnects. This is useful for creating automated processing and scripting.

This chapter includes:

Concepts

- ▶ SiteScope and SSH Overview on page 1542
- ▶ Configuring Remote Windows Servers for SSH Monitoring on page 1545

Tasks

- ▶ Configure Remote UNIX Servers for SSH monitoring on page 1546
- ▶ Configure Remote Windows Servers for SSH monitoring on page 1549

SiteScope and SSH Overview

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely accessing a remote computer. It is widely used by network administrators to remotely control Web and other kinds of servers. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by encryption. Secure Shell client machines make requests of SSH daemons or servers on remote machines.

Monitoring with SiteScope over SSH has the following basic requirements:

- 1** The servers that you want to have monitored by SiteScope using SSH must have a SSH daemon (or server) installed and active.
- 2** The machine on which SiteScope is running needs to be configured with an SSH client. There are two SSH client options for use on the server or machine on which SiteScope is running:
 - ▶ SiteScope includes a SSH client written in Java and native to the SiteScope application code. This client eases the setup of SSH connections and generally uses fewer system resources than external SSH clients.
 - ▶ SiteScope on Windows includes a third-party SSH client called plink. Plink is part of a set of SSH tools called PuTTY. SiteScope on UNIX and Linux require that an external SSH be installed on the machine where SiteScope is running.

SSH Connectivity Options

The following table outlines the SSH connectivity options currently supported with SiteScope. For important information about configuring and managing SSH connectivity, see “Guidelines and Limitations” on page 1544.

SiteScope Platform and Client Options	Monitored Server Platform and Daemon
Windows PuTTY SSH client (included with SiteScope) or SiteScope integrated Java SSH Client	UNIX/Linux SSH host daemon (sshd - either proprietary or OpenSSH)
UNIX/Linux SSH client (/usr/local/bin/ssh or usr/bin/ssh) or SiteScope integrated Java SSH Client	UNIX/Linux SSH host daemon (sshd - either SunSSH, proprietary or OpenSSH)
Windows PuTTY SSH client (included with SiteScope) or SiteScope integrated Java SSH Client	Windows 1. SSH server (Cygwin OpenSSH, F-Secure, or OpenSSH for Windows) 2. RemoteNTSSH package (included with SiteScope), to be installed into the required directory on the remote server

Guidelines and Limitations

- ▶ There are two different versions of the SSH protocol: version 1 and version 2. Version 1 and version 2 are different protocols and are not compatible with each other. This means that the SSH clients and SSH hosts must be configured to use the same protocol version between them to communicate. In many cases, SSH version 1 (SSH1) is the default version used. Some security vulnerabilities have been found in SSH version 1. Also, the SSH1 protocol is not being developed anymore and SSH2 is considered the current standard. We recommend using SSH version 2 (SSH2) for all SSH connections.
- ▶ The release version number of the SSH utilities and libraries you have installed must not be confused with the version of the SSH protocol that you want to be using. For example, OpenSSH release 3.5 supports both SSH1 and SSH2 protocols. The release version 3.5 does not mean that the libraries use an SSH version 3.5 protocol. You must configure the OpenSSH software to use either SSH1 or SSH2.
- ▶ If you have set up SiteScope remote monitoring using SSH connections and then make configuration changes or upgrades to the SSH daemon or server software deployed on remote servers in the environment, it may be necessary to reconfigure the SSH connectivity between the machine on which SiteScope is running and the remote servers that are being monitored.
- ▶ The availability of the Integrated Java SSH Client is indicated by using the drop-down menu in the **SSH Connection Method** of the Advanced Settings section of the UNIX Remote Preferences and Microsoft Windows Remote Preferences page. If the option for Internal Java Libraries does not appear in the list, you can still use the Plink external SSH Client for SSH connections. You can also contact an HP sales representative to upgrade to a later version of SiteScope that includes the Integrated Java SSH Client.

Configuring Remote Windows Servers for SSH Monitoring

The default remote connection method used by SiteScope for Windows-to-Windows connectivity and monitoring in Windows NT/2000/2003 networks is NetBIOS. While this has provided ease of connectivity, it does have several disadvantages. One is that NetBIOS is relatively vulnerable in terms of network security. Another is that it does not support remote execution scripts. Running commands on remote servers requires that scripts be run locally with commands to the remote machine being written using the UNC syntax of remote servers. Even then, some parameters are not returned from the remote server by using NetBIOS.

SiteScope supports monitoring of remote Windows NT/2000 servers using SSH. This technology has been tested with the OpenSSH binaries from Cygwin (available at <http://www.cygwin.com/>) installed as the SSH server on the remote server. It has also been tested with the server available from F-Secure. You may also try OpenSSH for Windows (formerly Network Simplicity "OpenSSH on Windows") which is available on SourceForge (available at <http://sshwndows.sourceforge.net/>).

The following is a comparison overview of two of the packages.

OpenSSH Package	Advantages	Disadvantage
Cygwin OpenSSH	<ol style="list-style-type: none"> 1. Provides access to either Windows or UNIX-style scripting on a Windows machine. 2. Provides access to UNIX-style system tools and utilities. 3. SiteScope can access the remote server both as a Windows Remote and /or a UNIX Remote. 	Complicated setup procedure.
OpenSSH for Windows	Simple setup procedure.	Only provides access to Windows commands, scripts, and utilities.

Note:

- ▶ OpenSSH for Windows and the Cygwin SSH implementations are incompatible with each other. They should not be installed on the same machine.
 - ▶ If there is more than one version of the Cygwin utilities or more than one SSH server installed on a machine, there may be conflicts that prevent the SSH connections from working. An error message such as `could not find entry point` is one indication of this kind of conflict. If you suspect this error, search the machine for multiple copies of `cygwin1.dll`. It may be necessary to remove all versions of the utilities and then reinstall only a single installation to resolve this problem.
-

For details on configuring remote Windows servers for SSH monitoring, see “Configure Remote Windows Servers for SSH monitoring” on page 1549.

Configure Remote UNIX Servers for SSH monitoring

SiteScope for Solaris or Linux supports remote monitoring by using SSH. This task describes the steps involved in configuring remote UNIX Servers for SSH monitoring with SiteScope.

Note: Setting up the SSH hosts on the remote servers you want to monitor in the UNIX environment can be very complex and is beyond the scope of this document. Some suggested resources on installation of the OpenSSH daemon are <http://www.sunfreeware.com/openssh.html> (for Solaris) and <http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/ref-guide/s1-ssh-configfiles.html> for Redhat Linux.

This task includes the following steps:

- “Prerequisites” on page 1547
- “Configure the SSH Client to Connect to the Remote Servers” on page 1547
- “Configure UNIX Remote Settings to Use the SSH Connection Method” on page 1547

1 Prerequisites

For details on the requirements for configuring remote UNIX servers for SSH monitoring with SiteScope in a UNIX environment, see “Configuration Requirements” on page 1548.

2 Configure the SSH Client to Connect to the Remote Servers

After you have set up SSH servers or daemons on remote servers, you must configure the SSH client that SiteScope uses to connect to the remote servers. For details on how to perform this task, see “SiteScope SSH Client Connection Options” on page 1561.

3 Configure UNIX Remote Settings to Use the SSH Connection Method

Once you have confirmed SSH connectivity, create or configure UNIX Remote settings in SiteScope to use SSH as the connection method. For details on the user interface, see Main Settings in “UNIX Remote Preferences” on page 220.

Configuration Requirements

The following are requirements for configuring remote UNIX servers for SSH monitoring with SiteScope in a UNIX environment:

- ▶ Secure Shell daemons or servers (**sshd**) must be installed on each remote server you want to monitor with SiteScope.
- ▶ The SSH daemons on the remote servers must be running and the applicable communication ports must be open. For example, the default for SSH is port number 22.
- ▶ A SSH client must be installed on the server where SiteScope is running. The SiteScope integrated Java SSH client normally fills this requirement.
- ▶ If you use an external SSH client on Solaris or Linux, the SSH client binaries must be accessible to SiteScope. When SiteScope runs the SSH client process, it searches in both **/usr/bin** and **/usr/local/bin** for the **ssh** command. The **ssh** binaries must be in one of these two locations and SiteScope must have permissions to run the **ssh** command.

You should verify SSH client-to-server connectivity from the machine where SiteScope is running to the remote machine you want to monitor. You should check SSH connectivity outside of the SiteScope application before setting up remote server connections using SSH in SiteScope. For example, if SiteScope is running on Solaris or Linux, use the following command line to request an SSH connection using SSH2 to the server `<remotehost>`:

```
ssh -2 <remotehost>
```

This normally returns text information that indicates the version of SSH protocol that is being used. Also, this attempts to authenticate the current user. Use the `-l username` switch to request a login as a different user.

For SiteScope running on Windows, see the section on “Testing SSH Connectivity with PuTTY Utilities” on page 1568 for information about testing SSH connectivity outside of the SiteScope application on Windows NT/2000 machines.

Once you have confirmed SSH connectivity, create or configure UNIX Remote settings in SiteScope to use SSH as the connection method.

Configure Remote Windows Servers for SSH monitoring

This task describes the steps involved in configuring remote Windows Servers for SSH monitoring with SiteScope.

This task includes the following steps:

- ▶ “Install and Configure a SSH Server” on page 1549
- ▶ “Install SiteScope Remote NT SSH Files” on page 1549
- ▶ “Configure the SSH Client to Connect to the Remote Servers” on page 1550
- ▶ “Configure Windows Remote Settings to Use the SSH Connection Method” on page 1550

1 Install and Configure a SSH Server

Install and configure a SSH server on each remote server to which you want SiteScope to connect. There are two software packages generally available that enable SSH capability:

- ▶ Cygwin environment available from RedHat at <http://www.cygwin.com/>. For details on how to perform this task, see “Install Cygwin OpenSSH on Windows” on page 1550.
- ▶ OpenSSH for Windows available at OpenSSH for Windows. For details on how to perform this task, see “Install OpenSSH for Windows” on page 1558.

Note: These setup steps must be performed for each server that runs the SSH daemon or server.

2 Install SiteScope Remote NT SSH Files

Install the SiteScope remote SSH files on each remote Windows server to enable commonly used server monitoring functions. For details on how to perform this task, see “Install SiteScope Remote NT SSH Files” on page 1560.

3 Configure the SSH Client to Connect to the Remote Servers

After you have set up SSH servers or daemons on remote servers, you must configure the SSH client that SiteScope uses to connect to the remote servers. For details on how to perform this task, see “SiteScope SSH Client Connection Options” on page 1561.

4 Configure Windows Remote Settings to Use the SSH Connection Method

After confirming SSH connectivity between SiteScope and the remote server, you can set up Windows Remote settings in SiteScope to use SSH as the connection method. You can then configure CPU, Disk, Memory, Microsoft Windows Performance Counter, and Script monitors to use the SSH connectivity. For details on selecting SSH as the connection method in the user interface, see Main Settings in “Microsoft Windows Remote Preferences” on page 219.

Install Cygwin OpenSSH on Windows

This task describes the steps involved in installing and configuring a Cygwin OpenSSH server on Windows servers.

Important: The following instructions assume that no other Cygwin or other ssh utilities are installed on the machine and that the machine has Internet access.

Note: The user login account used to install and run the SSH daemon needs adequate permissions to install the necessary programs, configure several file options, and control Windows services. It does not need to be the account that SiteScope uses to connect to the subject server, although that account must be configured within the Cygwin installation before you can monitor that server with SiteScope.

To install and configure a Cygwin OpenSSH server on Windows NT/2000 servers:

- 1** Create a new System Environment variable with the following definition:
CYGWIN = ntsec tty.
- 2** Add the string ;C:\cygwin\bin to your PATH variable. Save the changes to the variables.
- 3** Download the Cygwin setup program into a temporary folder. For example: C:\temp. The setup program is used to select, download, and install different packages and components available with Cygwin.
- 4** Run the downloaded setup program and choose the **Install from Internet** option when prompted to Choose A Download Source. Click **Next** to continue.
- 5** If prompted, select a root install directory where the Cygwin package should be installed. This is where the SSH daemon and related files are installed. For example, C:\cygwin. Click **Next** to continue.
- 6** If prompted, select a temporary directory where the Cygwin installation files should be stored. For example, C:\temp. Click **Next** to continue.
- 7** If prompted, select an Internet Connection option. Normally, **Direct Connection** can be used. Click **Next** to continue.
- 8** Select a suitable mirror site from which to retrieve the files using the selection list when prompted. Click **Next** to continue.
- 9** The Setup program queries the mirror site for the packages available and displays a hierarchy tree of package categories. To view and select the packages to download, click on the plus (+) symbol to the left of the category name to expand any of the package trees. Packages that are selected for download and installation display a version number in the **New** column. If a version number is not displayed for a particular package, it is not downloaded and installed. Click **Skip** to the left of package name to select the package for download.

Note: Many of the development (Devel) and database (Database) tools that may be selected by default for download are not necessary to run the SSH daemon and can be deselected to reduce download time and installation space.

Select each of the following packages for download and installation:

- cygrunsrv from the Admin branch
- cygwin-doc from the Doc branch
- pdksh from the Shells branch
- openssh and openssl from the Net branch
- your choice of UNIX-style text editor from the Editors branch (for example: vim or emacs)

Then click to download the files as prompted.

- 10** Depending on your installation options, the Cygwin setup downloads and installs the selected packages. You may be prompted to choose to have a shortcut to the Cygwin terminal window added to the Desktop or Program Start menu. Click to continue and complete the installation.
- 11** After the Cygwin setup is complete, open a Cygwin terminal window by clicking on the **Cygwin** desktop shortcut or Program Start menu item.

Note: Depending on the user profile in the Windows system, the default directory that opens in the terminal window may not be within the root Cygwin installation tree. Use the `pwd` command to display the current directory. Typing in the command string `cd /` normally changes the directory to the Cygwin root, which by default corresponds to the Windows `C:\cygwin` directory.

Update the default Cygwin group file with the group names in use on the machine and on your network. Use the `mkgroup` utility to update the default Cygwin group file with the groups defined on the server and in your domain. Examples of the commands to use are as follows:

```
mkgroup -l >> ../etc/group
mkgroup -d >> ../etc/group
```

Note:

- ▶ To have Cygwin recognize both domain and local group accounts, run the `mkgroup` utility twice, once for local users (`-l` option) and once for domain users (`-d` option). Remember to use `>>` syntax and not just `>`, to append entries to the file.
- ▶ If you use both the local and domain options, you must manually edit the `/etc/group` file (using the UNIX style text editor you downloaded) to remove any duplicate group entries. You may also want to remove group entries that are not needed for monitoring or should not have access to this machine.

Update the default Cygwin user (`passwd`) file with the users defined on the local machine plus any individual domain users you want to grant access to Cygwin on this machine. Use the `mkpasswd` utility to update the default Cygwin user file.

Examples of the commands to use are as follows:

```
mkpasswd -l >> ../etc/passwd
mkpasswd -d -u username >> ../etc/passwd (domain users)
```

Note:

- ▶ By default, Cygwin is set to run the OpenSSH daemon as the local user called **SYSTEM**. To have Cygwin recognize both domain and local machine user accounts, run the `mkpasswd` using the `-l` option to add all local users, and run it with the `-d` and `-u` options to add individual domain users. Remember to use `>>` syntax and not just `>`, to append entries to the file.
 - ▶ If you use both the local and domain options, you must manually edit the `/etc/passwd` file (using the UNIX style text editor you downloaded) to remove any duplicate user entries. You may also change the default `/home` path and default shell for individual users. This may be necessary to install the `RemoteNTSSH` package in the `/home/sitescopeaccount/` directory of the user account to be used by SiteScope.
-

- 12** Change the active directory to the `/bin` directory by typing `cd /bin`.
- 13** Create a symbolic link in the `/bin` directory that points to the Windows Command (CMD) shell by entering the following command line (be sure to include the trailing space and period):

```
ln -s /cygdrive/c/winnt/system32/cmd.exe .
```

- 14** It is recommended that you change permissions and ownership of several Cygwin files and directories. Also create a log file for the SSH daemon. Type the following command lines in the Cygwin terminal command line and press ENTER after each command line entered:

```
cd /  
chmod -R og-w .  
chmod og+w /tmp  
touch /var/log/sshd.log
```

Note:

- ▶ Exact syntax is required, including spaces.
 - ▶ Inconsistent and incorrectly assigned file and directory permissions can be one reason that the SSH daemon can not be started or that SiteScope is unable to connect to and run commands or scripts on the remote server.
-

- 15** Configure the SSH daemon to run as a Windows service by entering the following command:

```
ssh-host-config -y
```

When presented with the CYGWIN= prompt, type `ntsec tty` to match the environment variable you set at the beginning of this procedure. Normally, this configures the SSH daemon or service to restart automatically if the server needs to be restarted.

- 16** Configure the encryption keys and files for the SSH daemon using the following command:

```
ssh-user-config -y.
```

Type required passphrases for several keystore files when prompted. The program asks you to re-type the passphrase for confirmation.

- 17** You must change the ownership of several files and folders for use by the SSH daemon. The program does not normally run if the permissions on these files enable them to be changed or run by group or "world" level users. Type the following command strings to restrict access to these files:

```
chown SYSTEM:Users /var/log/sshd.log /var/empty /etc/ssh_h*  
chmod 755 /var/empty
```

- 18 Check the installation by starting and then stopping the CYGWIN sshd service using the **Programs -> Administrative Tools -> Services** panel.

Note: Cygwin includes a server utility to start the SSH daemon. However, there have been a number of situations where this method failed to start the server, whereas using the Windows Services panel was able to start the server.

- 19 Configure the default shell or command environment for the user account you use for monitoring with SiteScope. The shell you select effects what types of scripts or commands can be run remotely using the SSH connection. Use the UNIX-style text editor and edit the `/etc/passwd` file. Find the entry for the SiteScope login account you intend to use and change the shell from `/bin/bash` to the shell you want to use as described below. This is normally the last entry in the line for that account entry.
 - a If you chose to have SiteScope interact with the remote server using the Windows Command shell, change the default shell entry to `/bin/cmd`. Use this option when you plan to use Windows-style batch files and scripts. You must also include the symbolic link to the Windows `cmd.exe` kernel in the `/bin` directory as described in a previous step of this procedure.
 - b If you chose to have SiteScope interact with the remote Windows server using a Cygwin UNIX shell, change the default shell entry to be `/bin/pdksh`. The SiteScope SSH client may not accurately parse Cygwin's default `bash` shell. You must also configure a Remote UNIX server connection to this (Windows) server that connects to the Cygwin SSH daemon.

Save the changes to the file.

- 20 Edit the `PATH` and the default prompt commands in the `/etc/profile` file to ensure that Cygwin can find certain files and that SiteScope can parse the output from the remote shell. Use the UNIX-style text editor and edit the `/etc/profile` file. Find the `PATH` definition entry near the top of the file. For example:

```
PATH=/usr/local/bin:/usr/bin:/bin:$PATH
```

Change this to include the following:

```
PATH=./usr/local/bin:/usr/bin:/bin:$PATH
```

- 21** To change the default prompt commands, edit the `/etc/profile` file, and find the section similar to the following:

```
;;
sh | -sh | */sh | \
sh.exe | -sh.exe | */sh.exe )
#Set a simple prompt
PS1='$ '
;;
```

Immediately under this entry, add the following:

```
;;
pdksh | -pdksh | */pdksh | \
pdksh.exe | -pdksh.exe | */pdksh.exe )
#Set a simple prompt
PS1='> '
;;
```

- 22** Save the changes to the file.
- 23** Change the active directory to the home directory of the user you have created for SiteScope monitoring.

After making these changes and starting the SSH daemon, you should be able to connect to the server using an SSH client. For information about testing SSH connectivity outside of the SiteScope application on Windows NT/2000 machines, see the section on “Testing SSH Connectivity with PuTTY Utilities” on page 1568.

Note: Any time you run the `mkpasswd -l /etc/passwd` command (for example, when adding a new user), edit the `/etc/passwd` file again to make sure that the default shell for that user is set to the required value for any account being used by SiteScope.

Install OpenSSH for Windows

This task describes the steps involved in installing and configuring an OpenSSH server on Windows servers.

The OpenSSH for Windows package is an alternative to the Cygwin SSH package and can be easier to install. Like most products, the Cygwin product and the Open SSH for Windows are subject to change. There are cases where some versions of the Cygwin SSH server have not returned the data needed for SiteScope monitoring. If the OpenSSH for Windows package can solve this problem, you should use this package in place of the Cygwin package.

To install and configure an OpenSSH for Windows server on Windows NT/2000 servers:

- 1** Download and install the OpenSSH for Windows package.
- 2** Open a command prompt and change to the installation directory (C:\Program Files\OpenSSH is the default installation path).
- 3** Change the active directory to the OpenSSH\bin directory.
- 4** You must update the default group file with the group names in use on the machine and in your network. Use the `mkgroup` utility to update the default OpenSSH group file with the groups defined on the server and in your domain. Examples of the commands to use are as follows:

```
mkgroup -l >> ..\etc\group
mkgroup -d >> ..\etc\group
```

Note:

- ▶ To have OpenSSH recognize both domain and local group accounts, run the **mkgroup** utility twice, once for local users (-l option) and once for domain users (-d option). Remember to use >> syntax and not just >, to append entries to the file.
 - ▶ If you use both the local and domain options, you must manually edit the `/etc/group` file (using the UNIX style text editor you downloaded) to remove any duplicate group entries. You may also want to remove group entries that are not needed or should not have access to this machine.
-

- 5** You must update the default OpenSSH user (`passwd`) file with the users defined on the local machine plus any domain user you want to grant access to the SSH server on this machine. Use the **mkpasswd** utility to update the default user file. Examples of the commands to use are as follows:

```
mkpasswd -l >> ..\etc\passwd
mkpasswd -d -u username >> ..\etc\passwd
```

Note:

- ▶ To have OpenSSH recognize both domain and local machine user accounts, run the **mkpasswd** utility using the -l option to add all local users and run it with the -d and -u options to add individual domain users. Remember to use >> syntax and not just >, to append entries to the file.
 - ▶ If you use both the local and domain options, you must manually edit the `/etc/passwd` file (using the UNIX style text editor you downloaded) to remove any duplicate user entries. You may also change the default `/home` path and shell for individual users (see instructions below).
-

- 6** Check the installation by starting the **OpenSSH Server** service using the **Programs > Administrative Tools > Services** panel.

Install SiteScope Remote NT SSH Files

This task describes the steps involved in installing SiteScope remote NT files on each remote Windows server according to the SSH package you are working with.

To install the SiteScope SSH Files on Cygwin installations:

- 1** Verify that a `\sitescope_login_account_name` directory exists within the `<install_drive>:\cygwin\home` directory on each machine that is monitored by SiteScope using SSH. Replace `sitescope_login_account_name` with the user account name you use to connect to the machine using the SSH server.
- 2** One of the advantages of using SSH on Windows is that it allows SiteScope to run scripts on the remote server running the SSH daemon. To be able to use the Script Monitor to run remote scripts, create a `scripts` subdirectory in the `/home/sitescope_login_account_name` directory. Scripts you create for execution by the SiteScope Script Monitor must be placed inside this directory.
- 3** On the machine where SiteScope is installed, find the file called `RemoteNTSSH.zip` in the `<SiteScope_root_directory>\tools` directory.
- 4** Copy this file to the `<install_drive>:\cygwin\home\sitescope_login_account_name` directory on each of the remote Windows NT/2000 servers where you have installed the SSH server or daemon software.
- 5** Unzip the `RemoteNTSSH.zip` file on the remote server. Place the contents of the zip file into the `<install_drive>:\cygwin\home\sitescope_login_account_name` directory. This should create a `<install_drive>:\cygwin\home\sitescope_login_account_name\scripts` subfolder. You use this subfolder to hold scripts that can be run by the SiteScope Script Monitor.
- 6** Start the CYGWIN `sshd` service on the remote server.

After you have completed the steps above, it is recommended that you test SSH connectivity from your SiteScope server by using `plink.exe` or `PuTTY.exe` as described in the “Testing SSH Connectivity with PuTTY Utilities” on page 1568.

To install the SiteScope SSH Files on OpenSSH for Windows installations:

- 1** On the machine where SiteScope is installed, find the file called **RemoteNTSSH.zip** in the `<SiteScope_root_directory>\tools` directory.
- 2** Copy this file to the `<install_drive>:\WINNT` directory on each of the remote Windows NT/2000 servers where you have installed the SSH server or daemon software.
- 3** Unzip the **RemoteNTSSH.zip** file on the remote server. Extract the contents of the zip file into the `<install_drive>:\WINNT` directory. This should create an `<install_drive>:\WINNT\scripts` subfolder. You use this subfolder to hold scripts that can be run by the SiteScope Script Monitor.
- 4** Start the OpenSSH server service on the remote server.

After you have completed the steps above, it is recommended that you test SSH connectivity from your SiteScope server by using **plink.exe** or **PuTTY.exe** as described in the “Testing SSH Connectivity with PuTTY Utilities” on page 1568.

SiteScope SSH Client Connection Options

After setting up SSH servers or daemons on remote servers, configure the SSH client that SiteScope uses to connect to the remote servers using one of the following options:

- **Configure SiteScope to use the integrated Java SSH client.** SiteScope includes an integrated SSH client written in Java. This is the recommended option for SSH connectivity because it uses fewer system resources than the external clients and configuration is usually simpler. For details on how to configure remote servers using an external client, see “Integrated Java SSH Client Overview” on page 1564.
- **Configure SiteScope to use an external SSH client.** SiteScope on Windows includes a third-party SSH client called **plink**. SiteScope for Solaris and Redhat Linux make use of the SSH utilities normally bundled with those operating systems or available for download. For details on how to configure remote servers using an external client, see “External SSH Client Overview” on page 1566.

57

Working with SSH Clients

If you need to use Secure Shell (SSH) to connect to remote UNIX or Windows servers, SiteScope must have access to a SSH client to make the connection and transmit data. This section contains some of the client configuration possibilities and issues involved in using SSH for SiteScope monitoring.

This chapter includes:

Concepts

- Integrated Java SSH Client Overview on page 1564
- External SSH Client Overview on page 1566

Tasks

- Configure the Integrated Java SSH Client on page 1569
- Configure the External SSH Client on page 1572

Integrated Java SSH Client Overview

SiteScope provides a SSH client written in Java that is integrated into the SiteScope application. This client significantly reduces the required system resources used by SiteScope when connecting to servers by using SSH. The Java client supports both SSH version 1 (SSH1) and version 2 (SSH2) protocols as well as both password-based and key-based authentication. The SiteScope configuration for the client is identical for UNIX, Linux, and Windows SiteScope.

Working with the Integrated SSH Client

While SSH1 and SSH2 are both Secure Shell protocols, they are considered to be two different protocols and are not compatible with each other. Some security vulnerabilities have been found in SSH1 that has resulted in SSH2 being considered the current standard. Most SSH software supports both protocols. However, to be sure that a request for a SSH connection uses SSH2 instead of SSH1, it is necessary to configure SSH clients and SSH hosts to use the same protocol version between them to communicate. In many cases, SSH1 is the default version used for connections, as it is considered the lowest common denominator between a SSH client and a SSH host.

There are two ways to force SSH2 connections:

- ▶ **Configure all SSH daemons or servers to accept only SSH2 connection requests.** This is the most secure option but may be the most time-consuming unless each server was configured for this option when it was installed and activated.
- ▶ **Configure the SSH client on the SiteScope server to only make SSH2 requests.** Requires changes only to the client on the SiteScope server. For the integrated Java SSH client, this can be controlled by a setting in the Advanced Options section on the remote server setup page.

Setting Up Key-Based Authentication

Another part of SSH security is authentication. The integrated SSH client for SiteScope can be configured to use one of two authentication options:

- ▶ **Password Authentication.** Password Authentication is the default method for SSH connections in SiteScope.
- ▶ **Key-Based Authentication.** Key-Based Authentication adds an additional level of security through the use of a passphrase and a public-private key authentication.

To use Key-Based Authentication for SSH remotes, you must first create a pair of public/private keys. The public key resides on the remote and the private key is kept on the SiteScope machine. Both Cygwin OpenSSH and OpenSSH for Windows come with a key generation tool called `ssh-keygen`. The `ssh-keygen` tool allows you to create both protocol version 1 and version 2 keys. When setting up a UNIX or Windows remote server using the Internal Java Libraries Client, use the key generation tool called `MindTerm` to create a public/private key pair for RSA (version 1 and version 2) and DSA (version 2).

Using SSH Version 2 Protocol

By default, the SiteScope Java client uses the SSH1 Protocol if the server it is trying to connect to allows SSH1 connections. If this negotiation fails, SiteScope attempts to connect using version 2 protocol. The SiteScope Java client can be configured to use only SSH2 connections. Making the change on the SiteScope machine may be easier than having to reconfigure a large number of remote SSH servers.

For details on configuring the Integrated Java SSH Client, see “Configure the Integrated Java SSH Client” on page 1569.

External SSH Client Overview

SiteScope provides the capability of connecting to remote servers using an external SSH client. On Windows platforms, the plink client is included with SiteScope. On UNIX and Linux platforms, SiteScope can use a standard SSH client such as SunSSH or OpenSSH.

Working with External SSH Clients

There are two different versions of the SSH protocol: version 1 and version 2. While they are both Secure Shell protocols, they are considered to be two different protocols and are not compatible with each other. Some security vulnerabilities have been found in SSH1 that has resulted in SSH2 being considered the current standard. Most SSH software supports both protocols. However, to be sure that a request for a SSH connection uses SSH2 instead of SSH1, it is necessary to configure SSH clients and SSH hosts to use the same protocol version between them to communicate. In many cases, SSH version 1 (SSH1) is the default version used for connections, as it is considered the lowest common denominator between a SSH client and a SSH host.

There are two ways to force SSH2 connections:

- ▶ **Configure all SSH daemons or servers to accept only SSH2 connection requests.** This option is perhaps the most secure but may be the most time-consuming unless each server was configured for this option when it was installed and activated.
- ▶ **Configure the SSH client on the SiteScope server to make only SSH2 requests.** This option requires changes only to the client on the SiteScope server. For external SSH client, this is usually controlled by using the client settings.

Setting Up SSH Authentication

Another part of SSH security is authentication. The integrated SSH client for SiteScope can be configured to use one of the following two authentication options:

- ▶ **Password Authentication.** Password Authentication is the default method for SSH connections in SiteScope.
- ▶ **Key-Based Authentication.** Key-Based Authentication adds an additional level of security through the use of a passphrase and a public-private key authentication.

Monitoring with SSH on Windows Platforms

SiteScope for Windows platforms includes a SSH client to handle connections to remote SSH-enabled servers. SiteScope includes the PuTTY SSH utilities for SSH connectivity to both UNIX and Windows servers. These utilities are found in the `<SiteScope_root_directory>\tools` directory.

By default, SiteScope SSH connections uses the SSH1 protocol (less secure) unless the server it is connecting to accepts only SSH2 sessions. To force SiteScope to use the SSH2 protocol (more secure), you must configure the SSH client on the machine where SiteScope is running and possibly the SSH daemons/hosts on the remote servers to communicate using the SSH2 protocol. For SiteScope on Windows, configure the PuTTY SSH client utility and SiteScope as described in “Set up SSH2 on SiteScope for Windows Platforms” on page 1574.

Note: The PuTTY and plink tools supplied with SiteScope are not the latest release versions of these tools. SSH connectivity is handled by the internal Java libraries by default. Consider checking for newer versions and replacing the files supplied with SiteScope with updated versions. More information about the PuTTY SSH client can be found at <http://www.chiark.greenend.org.uk/~sgtatham/putty/> or <http://www.openssh.org/windows.html>.

Testing SSH Connectivity with PuTTY Utilities

It is recommended that you test SSH connectivity from SiteScope on Windows to remote hosts using either the **PuTTY.exe** or **plink.exe** tools. This is also useful for troubleshooting connectivity. You can use utilities to test connectivity with a SSH host. The plink utility is run from the command line.

Setting Up SSH on SiteScope for Windows Platforms

SiteScope for the Windows platform uses plink, part of the PuTTY suite of SSH tools, to create its SSH connections for remote monitoring. By default, the plink utility uses the SSH1 Protocol if the server it is trying to connect to allows SSH1 connections. The SiteScope SSH client can be configured to use only the SSH2 protocol for connections. Making the change on the SiteScope machine may be easier than having to reconfigure a large number of remote SSH servers.

Setting up SiteScope for Windows to use only SSH2 to communicate with remote UNIX or remote Windows servers requires two actions:

- 1** Create settings in the SSH client on the SiteScope server to use only SSH2.
- 2** Modify SiteScope remote server connection profiles to use the SSH2 connection profile.

For details on configuring the external SSH2 client, see “Configure the External SSH Client” on page 1572.

Configure the Integrated Java SSH Client

This task describes the steps involved in configuring the integrated Java SSH client.

This task includes the following steps:

- “Select an Authentication Option for SSH Connections” on page 1569
- “Configure the SiteScope Java Client to Use Only SSH2 Connections” on page 1569

1 Select an Authentication Option for SSH Connections

Select an authentication option for integrating SSH client for SiteScope: password authentication (the default method in SiteScope) or key-based authentication. For details on how to set up key-based authentication for SSH connections, see “Set Up Key-Based Authentication” on page 1570.

2 Configure the SiteScope Java Client to Use Only SSH2 Connections

When configuring your remote server profile in Microsoft Windows/UNIX Remote Preferences, select the **SSH Version 2 Only** check box in the Advanced Settings.

Set Up Key-Based Authentication

This task describes the steps involved in setting up Key-Based Authentication for SSH remotes using MindTerm.

Note: When using F-Secure, the F-Secure client creates an SEC SSH formatted key and the F-Secure server understands a SEC SSH formatted key. To use the key generated using the Internal Java Libraries client (which is in openSSH key format), you must convert the openSSH key to SEC SSH format.

To create a public or private key pair:

- 1 Open a command window on the SiteScope server, and run the following command to launch MindTerm:

```
<SiteScope root directory>\java\bin\java -jar c:\<SiteScope root directory>\WEB-INF\lib\mindterm.jar
```

Note: For SiteScope 7.9.5.x and earlier, type the command: <SiteScope root directory>\java\bin\java -jar c:\<SiteScope root directory>\java\lib\ext\mindterm.jar.

- 2 In MindTerm, select **File > Create Keypair > DSA (or RSA)**. Also select OpenSSH .pub format.
- 3 The key pair is written to the <USER_HOME>\mindterm directory. Copy the **identity.pub** file to the <SiteScope root directory>\groups directory.
- 4 Copy the **identity.pub** file to the <USER_HOME>/.ssh directory on the remote machine and rename it **authorized_keys** (or **authorized_keys2** for SSH2).

- 5 On the remote machine, run the following command in the `<USER_HOME>/ssh` directory, and make sure that `User` has read, write, and execute permissions, and that `Group` and `Other` have read permissions on the `authorized_keys` file.
- 6 Create a remote connection in SiteScope for the remote server using key file authentication and Internal Java Libraries.

The private key goes in the `<SiteScope root directory>\groups` directory and the public key in the `<USER_HOME>/ssh/authorized_keys` file on the remote machines.

The key generated from MindTerm is in **OpenSSH** format.

Note: You must verify that the server key and the MindTerm key are at the same level. For example, if the server key is 768 bit and the MindTerm key is 1024 bit, the authentication procedure fails.

To find out what your server is using:

- 1 Stop the `sshd` service on the remote server. On a Red Hat Linux server, run the command:

```
/etc/rc.d/init.d/sshd stop
```

- 2 Start the `sshd` service in debug mode on the remote server. On a Red Hat Linux server, run the command:

```
/usr/sbin/sshd -d
```

You should see output similar to **Generating 768 bit RSA key**.

Note: When using the **Key File for SSH connections** box in SiteScope, if there is a trailing space after the information entered, this causes an "unknown error (-1)" failure. Remove the trailing space to fix the problem.

To convert the openSSH key to SEC SSH format:

- 1** Create a RSA key in MindTerm (which is an openSSH key pair).
- 2** Run the following command on the remote server to convert the openSSH key to SEC SSH format:

```
ssh-kegen -e -f <public key>
```
- 3** Leave the private key on the SiteScope server in the openSSH format.

Note: When using Key-Based authentication, the Key File supplied must be a version 2 private key.

Configure the External SSH Client

This task describes the steps involved in configuring the external SSH client.

This task includes the following steps:

- “Set the SiteScope PuTTY Client to Use SSH2” on page 1573
- “Configure SiteScope to Use SSH2” on page 1573
- “Test SSH Connectivity with PuTTY Utilities” on page 1573
- “Configure SiteScope to Use SSH2” on page 1573

1 Set the SiteScope PuTTY Client to Use SSH2

Create settings in the SSH client on the SiteScope server to use only SSH2. For details on how to perform this task, see “Set up SSH2 on SiteScope for Windows Platforms” on page 1574.

2 Select an Authentication Option for SSH Connections

Select an authentication option for integrating SSH client for SiteScope: password authentication (the default method in SiteScope) or key-based authentication. For details on how to set up key-based authentication for SSH connections, see the instructions for creating Public Keys using the PuTTYGen tool at <http://the.earth.li/~sgtatham/putty/0.60/html/doc/Chapter8.html#pubkey>.

Note: SSH uses DES, BLOWFISH, RSA, or other public key cryptography for both connection and authentication. Public Keys are stored on a per-user basis so if you are using key-based logins instead of password-based logins, you should log in and run the PuTTYGen tool using the same account that is used by the SiteScope service.

3 Test SSH Connectivity with PuTTY Utilities

Test SSH connectivity from SiteScope on Windows to remote hosts using either the **PuTTY.exe** or **plink.exe** tools. For details on how to perform this task, see “Test SSH Connectivity with PuTTY” on page 1576.

4 Configure SiteScope to Use SSH2

Modify SiteScope remote server connection profiles to use the SSH2 connection profile. For details on how to perform this task, see “Configure SiteScope to Use SSH2” on page 1577.

Set up SSH2 on SiteScope for Windows Platforms

This task describes the steps involved in setting up the PuTTY client on the SiteScope server to use only SSH2.

To set up PuTTY to use SSH2:

- 1** Log on to the server where SiteScope is running as the user who runs the SiteScope service. To see which user this is, open the Services control panel, right-click the SiteScope service, select **Properties**, and click the **Log On** tab.
- 2** Find the **PuTTY.exe** tool in the `<SiteScope_root_directory>\tools` directory. Alternatively, you can download an updated PuTTY version from the Internet.
- 3** Launch the PuTTY utility by double-clicking the icon in Windows Explorer (or typing **putty** in a command window with a path to the `<SiteScope_root_directory>\tools` directory). No installation steps are needed. The Putty Configuration console opens.
- 4** With the **Session** tab or tree selected, type the hostname or IP address of the remote machine to be monitored in the **Host Name** box. Select the SSH radio button below the hostname in the Protocol section.
- 5** Select the **Connection** tab or tree, and type the username on the remote machine in the Auto-login username box. This should be a user account with permissions to monitor processes and hardware statistics on the remote server. Optionally, this user account might also have execution privileges to enable SiteScope to run scripts on the remote server.
- 6** Select the **SSH** tab or tree under the Connection tree, and then choose the **2** radio button in the Preferred SSH Protocol Version section.

- 7 Return to the Session tab. In the Saved Sessions text box, type a name for these settings. Any previously saved settings appear in the list box below.

Note: The Saved Session name should not be a resolvable hostname on your network, nor can it contain a white space character. For instance, if these settings are for a machine named `myhost.mydomain.com`, the session settings name cannot be `myhost`, `myhost.mydomain.com`, or `myhost settings` (the latter is not allowed because of the white space between the words). Choose a name, such as `myhost-settings`.

- 8 Click the **Save** button. The name of your new settings should appear in the list of saved settings.

Repeat this process to create settings for each remote machine you wish to monitor with SiteScope using SSH2.

Note: Make a note of the Saved Session name for each machine that you configure, to type this name into the SiteScope configuration file.

Test SSH Connectivity with PuTTY

This task describes the steps involved in testing SSH connectivity from SiteScope on Windows to remote hosts using either the **PuTTY.exe** or **plink.exe** tools.

To test SSH connectivity with PuTTY:

- 1 Log on to your Windows machine as the user who runs the SiteScope service.
- 2 Open a command window to the `<SiteScope_root_directory>\tools` directory.
- 3 Run the plink utility with the following syntax:

```
plink -ssh <remoteuser>@<hostname>
```

where `<remoteuser>` is the login username for a valid user account on the `<hostname>` server.

- 4 Follow the prompts in the terminal window to confirm that the remote login is successful. Log out of the terminal session when you are satisfied that the connection is working correctly.

If you want to use the SSH2 protocol for connections, you must use the PuTTY utility to configure the PuTTY client to use SSH2 instead of the default SSH1. This requires that you save session settings as described in the section “Set up SSH2 on SiteScope for Windows Platforms” on page 1574. After you have done this, you can also use PuTTY to test SSH connectivity.

To test SSH2 connectivity with PuTTY:

- 1 Log on to your Windows machine as the user who runs the SiteScope service.
- 2 Launch the PuTTY utility.
- 3 From the Session tab or tree, select the Saved Session name of the remote connection you want to test and click the **Load** button to the right of the selection box.
- 4 Click the **Open** button near the bottom of the dialog box. This launches a terminal emulation window.

- 5 Follow the prompts in the terminal window to confirm that the remote login is successful.
- 6 Log out of the terminal session when you are satisfied that the connection is working correctly.

Configure SiteScope to Use SSH2

This task describes the steps involved in configuring SiteScope to use SSH2 for connecting to remote UNIX or remote Windows servers.

To configure SiteScope to use SSH2:

- 1 Open SiteScope in a Web browser.
- 2 In the monitor tree, expand the **Preferences** container and click **Microsoft Windows/Unix Remotes Preferences**.
- 3 Click the **New Microsoft Windows/UNIX Server** button and configure the remote server settings as follows:
 - **Host.** Type the name of the settings you saved. For example, to use the settings for myhost.mydomain.com, type myhost-settings in the box.
 - **Login.** Leave the box empty.
 - **Password.** Type the password to log in to the remote machine.

For UNIX Remotes:

- **OS.** Select the applicable operating system of the target remote server.
- **Prompt.** If the shell prompt for the remote UNIX server is something other than #, type that prompt in the box.
- **Login Prompt.** Leave the box empty.
- **Password Prompt.** Leave the box empty.

Click **OK** to add the remote server profile.

Note: The remote connection test fails. You may see a message similar to the following error message:

```
Connecting to myhost-settings...
Waiting for prompt(#)...
Unable to open connection:
Host does not exist
Remote command error: unknown host name (-997)
```

Go to the `<SiteScope_root_directory>\groups` directory and make a backup copy of the `master.config` file. Rename the backup file to `master.config.SAV`.

- 4 Open the `master.config` file in a text editor, and locate the section of entries or lines beginning with the string `_remoteMachine`. If you have configured multiple remote server connections, there are multiple entries that begin with this string. Locate the line that includes the string `_host=myhost-settings`, where `myhost-settings` is the name of the host settings you entered in the Server Address box in PuTTY Configuration tool.
- 5 Add the following string to the end of that line:

```
_sshCommand=<SiteScope root directory>\tools\plink.exe_-ssh_$host$_-pw_$password$
```

Note: This string must be entered on the same line. Do not add any carriage returns, new lines, or extra spaces.

Replace `<SiteScope_root_directory>` with the path to your SiteScope installation. For example, if SiteScope is installed at `C:\SiteScope`, the string would read:

```
_sshCommand=C:\SiteScope\tools\plink.exe_-ssh_$host$_-pw_$password$
```

After you have finished making modifications, the entire line should look similar to the following example:

```
_remoteMachine=_os=Linux_id=11_trace=_method=ssh  
_password=(0x)MGJJKDKLKJNINPNJMJ_login=_host=myhost-settings  
_name=_sshCommand=C:\SiteScope\tools\plink.exe_-ssh_$host$_  
pw_$password$
```

Note: This example wraps across multiple lines to fit on this page. When entering this setting into the SiteScope configuration file, be sure that it is entered all a single line.

- 6** Repeat this step to modify each `_remoteMachine` entry, using the applicable host name setting created for each host using the PuTTY Configuration tool in the previous section.
- 7** Save and close the `master.config` file.
- 8** Stop and restart the SiteScope service.
- 9** Open a Web browser to the SiteScope server, expand the **Preferences** container, and click **Microsoft Windows/UNIX Remote Preferences**.
- 10** In the Servers table for the remote you configured, click the **Test** button (for Windows remotes) or **Detailed Test** button (for UNIX Remotes) to test the connection and verify that it works.

58

Creating Custom Properties

You can customize SiteScope to extend and adapt it to a wide variety of environments and needs. This section describes how you can add custom property settings to SiteScope monitors and how you can add custom content to real-time Dashboard views in the SiteScope interface.

This chapter includes:

Concepts

- ▶ Custom SiteScope Properties Overview on page 1582
- ▶ Working with Custom Monitor Properties on page 1582
- ▶ Working with Custom Display Columns on page 1584
- ▶ Displaying Custom Properties in Custom Columns on page 1585

Tasks

- ▶ Create Custom Properties on page 1585

Reference

- ▶ Custom Monitor Property and Column Definition Syntax on page 1590

Custom SiteScope Properties Overview

Each monitor type in SiteScope includes a number of properties. You access these properties using the monitor's Properties view. You can add your own custom properties to SiteScope monitors. For details, see “Working with Custom Monitor Properties” on page 1582.

The Dashboard view displays real-time monitor results and related information in a table format. You can add a custom column for display in the Dashboard view. For details, see “Working with Custom Display Columns” on page 1584.

You can link custom properties to custom columns to have the values of your custom properties displayed in real-time SiteScope views. You can also have other SiteScope monitor properties displayed in custom columns. For details, see “Displaying Custom Properties in Custom Columns” on page 1585.

Working with Custom Monitor Properties

Each SiteScope monitor instance consists of a set of properties that define what action the monitor is to perform and how it is to perform these actions. Monitor properties also store information that may be passed to the system that is being tested.

The custom monitor property function allows you to define and store additional information you associate with a monitor. For example, you may want to enable users to define property values that categorize monitors according to their importance, or actions that need to be taken if the monitor reports an error. You may add more than one custom monitor property to SiteScope.

Defining a custom monitor property adds a new form entry item to the add and edit view for monitors in the Custom Property panel. A new form entry item is added for each custom property defined. The custom property definition fields are added to all monitor types.

Note: Custom monitor properties do not have default values and may be blank until you have defined a value for a property. Values are defined only when you explicitly type or select a value and then update the monitor.

Custom monitor property definitions are added as single line entries to the `master.config` file in SiteScope. The default custom property form element is a text box. You can also standardize custom property values and define a selection list as the input control. This allows you to define a set of values that can be assigned to a custom property.

It is not necessary to restart the SiteScope service to activate the custom properties. There may be a delay of several minutes for SiteScope to update its configuration data.

Using Custom Properties in Alert Templates

You can reference custom monitor properties in alert templates. This allows you to include custom information about monitors in alerts sent by SiteScope. You use the `_propertyName` from the custom property definition as a variable reference in alert templates.

Configuring Custom Monitor Properties

For details on how to configure custom monitor property, see “Create Custom Properties” on page 1585. For details on the syntax of the definition string for a custom monitor property, see “Custom Monitor Property and Column Definition Syntax” on page 1590.

Working with Custom Display Columns

The Custom Column function of SiteScope provides a flexible tool for customizing the information and functionality available through the SiteScope interface. The custom column can be used to display information as text, provide a hyperlink to a specific URL, call Javascript code, and even include a monitor-specific CGI request to an external resource. At present, only one custom column is supported in SiteScope.

Custom columns can be created without creating a custom property. For example, You can create a custom column to display a fixed hyperlink to an external resource in the SiteScope interface. You can display custom monitor properties in a custom column. For details, see “Displaying Custom Properties in Custom Columns” on page 1585.

You can also embed short Javascript code into a custom column. A script can call other custom scripts that you can add or reference by using the `headerHTML` parameter in the `master.config` file. For example, you can write a script as an external file called `sscopecustom.js` in the `<install_path>\SiteScope\` folder and then reference this file by adding the following to the `headerHTML` entry:

```
_headerHTML=<script language="Javascript" src="sscopecustom.js"></script>
```

Note: When adding Javascript using the `headerHTML` parameter, use the existing entry in the `master.config`. Only one `headerHTML` parameter is allowed.

For details on how to configure custom display columns, see “Create Custom Properties” on page 1585.

Displaying Custom Properties in Custom Columns

By default, custom monitor properties are displayed only in the Properties view of an individual monitor. This means that they are not normally visible in real-time views. In some cases, a custom monitor property is useful only if the value is displayed in the interface. You can display custom properties in Dashboard views by adding a reference to the property in a custom column.

When you define a custom monitor property, SiteScope adds the name of the property to its list of properties for the monitor. You can display these properties in custom columns by adding a reference to one or more property variables in the column content definition string.

For details on how to link monitor properties to custom columns, see “Create Custom Properties” on page 1585.

Create Custom Properties

This task describes the steps involved in creating custom properties.

This task includes the following steps:

- “Create a Custom Property Definition” on page 1585
- “Create a Custom Column Definition” on page 1586
- “Display Custom Properties in Custom Columns” on page 1586

1 Create a Custom Property Definition

You can define and store additional information associated with a monitor by adding a custom monitor property definition.

- For details on how to add a text or numeric custom property, see “Add a Text or Numeric Custom Property” on page 1586.
- For details on how to define a selection list input for a custom property, see “Define a Selection List Input for a Custom Property” on page 1587.

2 Create a Custom Column Definition

Add a custom column to real-time views in the SiteScope Dashboard. For details on how to perform this task, see “Add a Custom Column” on page 1588.

3 Display Custom Properties in Custom Columns

To link monitor properties to custom columns, you must reference the custom property variable in the custom column definition. For details on how to perform this task, see “Reference Property Values in Custom Columns” on page 1589.

Add a Text or Numeric Custom Property

This task describes how to add a simple custom property.

Note: For details on the syntax of the definition string for a custom monitor property, see “Custom Monitor Property Syntax” on page 1590.

To add a text or numeric custom property:

- 1 Make a backup of the master configuration file in a safe location. The file is found at `<install_path>\SiteScope\groups\master.config` on the machine where SiteScope is running.
- 2 Open the `master.config` file using a text editor.
- 3 Add a `_monitorEditCustom=` entry as a new line to the file.
- 4 On the same line, type the text string to define the `_propertyName`, the `display_title` and the `display_description`. Separate each of the entries with the vertical pipe (`|`) symbol.
- 5 If you want to define a default value for the property, add the default value in the place of the `input_definition` entry.
- 6 Save the changes to the file.

Example

To standardize custom property values, you can define a selection list as the input control. This allows you to define a set of values that can be assigned to a custom property. The following example defines a custom property named `_actiongroup` with an option selection menu having three options: SysDev, TestDev, and Production.

```
_monitorEditCustom=_actiongroup|Team|Select which support team has responsibility
for this monitor.|SysDev|<select name="$NAME$"><OPTION selected
value="$VALUE$">$VALUE$</option> <option>TestDev</option>
<option>Production</option></select>
```

Define a Selection List Input for a Custom Property

This task describes how to add an option selection list input control to a custom property definition.

Note: For details on the syntax of the definition string for a custom monitor property, see “Custom Monitor Property Syntax” on page 1590.

To define a selection list input for a custom property:

- 1** Make a backup of the master configuration file in a safe location. The file is found at `<install_path>\SiteScope\groups\master.config` on the machine where SiteScope is running.
- 2** Open the `master.config` file using a text editor.
- 3** Add a `_monitorEditCustom=` entry as a new line to the list of parameters.
- 4** On the same line, type the string to define the `_propertyName`, the `display_title` and the `display_description`. Separate each of the entries with the vertical pipe (`|`) symbol.

- 5 For the `input_definition` item, type the option selection code using the following syntax:

```
<select name="$NAME$"><OPTION selected  
value="$VALUE$">$VALUE$</option>  
<option>option_value_1 Group</option>  
<option>option_value_2</option>  
<option>option_value_3</option>...</select>
```

Where `$NAME$` and `$VALUE$` are required, internal reference variables and `option_value_1`, `option_value_2`, and so forth, are the text strings for the options in the selection menu.

- 6 Save the changes to the file.

Add a Custom Column

This task describes how to add a custom column to the SiteScope real-time views.

Note: For details on the syntax of the definition string for a custom column, see “Custom Column Definition Syntax” on page 1592.

To add a custom column:

- 1 Make a backup of the master configuration file in a safe location. The file is found at `<install_path>\SiteScope\groups\master.config` on the machine where SiteScope is running.
- 2 Open `master.config` using a text editor.
- 3 Add a `_monitorTableCustom=` entry as a new line to the file.
- 4 On the same line, type the text string to define the `_referenceValue`, the `column_title` and the `column_content_definition`. Separate each of the entries with the vertical pipe (`|`) symbol.
- 5 Save the changes to the file.

Reference Property Values in Custom Columns

This task describes how to reference the custom property variable in the custom column definition.

Note: For details on how to create custom property and column definitions, see the steps described in “Create Custom Properties” on page 1585.

To reference property values in custom columns:

- 1** Make a backup of the master configuration file in a safe location. The file is found at `<install_path>\SiteScope\groups\master.config` on the machine where SiteScope is running.
- 2** Open `master.config` using a text editor.
- 3** Add one or more `_monitorEditCustom=` entries including the `_propertyName`, the `display_title` and the `display_description` strings. Separate each of the entries with the vertical pipe (`|`) symbol.
- 4** Add a `_monitorEditCustom=` entry including the `_referenceValue`, the `column_title` and the `column_content_definition`. Separate each of the entries with the vertical pipe (`|`) symbol.
- 5** Within the string for the `column_content_definition`, include a reference to a custom property by adding the `_propertyName` surrounded with dollar signs (`$`). For example, if a custom property is defined with the name `_NOCAction`, add a reference to this property in the `column_content_definition` as `$_NOCAction$`.
- 6** Save the changes to the file.

You may include references to some other internal SiteScope property variables in the `column_content_definition` string. This is limited to property variables specific to each monitor type.

Custom Monitor Property and Column Definition Syntax

You define custom monitor property definitions and custom column definitions using the following syntax:

Custom Monitor Property Syntax

Custom monitor property definitions are added as single line entries to the `master.config` file in SiteScope. The default custom property form element is a text box. You can also define a custom property to use selection menu entries. The syntax of the definition string for a custom monitor property that accepts plain text values is as follows:

```
_monitorEditCustom=_propertyName|display_title|display_description|default_definition
```

The syntax of the definition string for a custom monitor property that an option selection menu is as follows:

```
_monitorEditCustom=_propertyName|display_title|display_description|default_definition|input_code
```

The custom elements of the definition string are separated by the vertical pipe (|) symbol. The following table describes the elements of the custom property definition string:

Element	Description
<code>_monitorEditCustom</code>	The parameter name that signals SiteScope to add a custom monitor property to monitors.
<code>_propertyName</code>	The variable name for the property. Generally, this should begin with an underscore character to signal that it is a property variable. This name can be referenced elsewhere within SiteScope. Do not include spaces or punctuation marks as part of the property name.

Element	Description
display_title	The item title text to be displayed in the interface with the custom property entry or selection field. This string may include HTML markup code.
display_description	An optional text description to be displayed in the interface below the property entry field. Use this to describe the purpose and usage for the property. The string may include spaces and punctuation marks.
default_definition	An optional string to define a default value for the property. The default input object is a text field.
input_code	This field contains the HTML code for an option selection input object for setting the custom property value. This must include the \$NAME\$ and \$VALUE\$ special internal reference variables used by SiteScope to work with the list.

Note: The entire definition string must be on a single line of text. Do not insert any linefeeds or soft or hard returns in the definition.

Custom Column Definition Syntax

You define a custom column definition using the following syntax:

```
_monitorTableCustom=_referenceValue|column_title|column_content_definition
```

The custom elements of the definition string are separated by the vertical pipe (|) symbol. The following table describes the elements of the custom property definition string.

Element	Description
<code>_monitorTableCustom</code>	The parameter name that signals SiteScope to add a custom display column property to monitors.
<code>_referenceValue</code>	The variable name for the property. Generally, this is a placeholder name although it can be referenced in other places within SiteScope.
<code>column_title</code>	The text to display as the column title.
<code>column_content_definition</code>	The text string or markup code to be displayed in the custom column for each monitor. This can include HTML and Javascript code.

Note: The entire definition string must be on a single line of text. Do not insert any linefeeds or carriage returns in the column definition.

59

Tools for Troubleshooting

When SiteScope reports a problem with a monitored system or you are having difficulty configuring a monitor, it is useful to have some resources to troubleshoot and diagnose problems. SiteScope provides a number of tools to help you uncover issues and facilitate monitor configuration.

This chapter includes:

Concepts

- ▶ SiteScope Tools Overview on page 1593

Reference

- ▶ SiteScope Tools User Interface on page 1597

SiteScope Tools Overview

The SiteScope Tools node contains a number of utilities that are useful to test the monitoring environment. Use these tools to make a variety of requests and queries of systems you are monitoring and to view detailed results of the action. Requests may include simply testing network connectivity or verifying login authentication for accessing an external database or service.

The following tables list the diagnostic tools that are available. See the applicable sections for more information about these tools.

Application Diagnostic Tools

Tool Name	Description
DNS Lookup	Test a DNS server to verify that it can resolve a domain name. (Includes access to a Traceroute tool to test network routing.). For more information, see “DNS Lookup Tool” on page 1597.
Database Connection	Check connectivity and configuration of JDBC or ODBC database connections. For more information, see “Database Connection Tool” on page 1598.
Database Information	Retrieve and display database server metadata such as product and driver version, SQL compatibility level information, and supported SQL functions. For more information, see “Database Information Tool” on page 1601.
FTP Server	Check the availability of an FTP server and whether a file can be retrieved. For more information, see “FTP Server Tool” on page 1603.
Get URL and URL Content	Request a URL from a server and prints the returned data. Includes access to a Trace Route Tool to test network routing. For more information, see “Get URL and URL Content Tool” on page 1605.
Mail Round Trip Test	Test a mail server by sending and retrieving a test message. For more information, see “Mail Round Trip Test Tool” on page 1609.
Ping	Perform a round-trip Ping test across the network. Includes access to a Traceroute tool to test network routing. For more information, see “Ping Tool” on page 1616.
Trace Route	Perform a traceroute from your server to another location. For more information, see “Trace Route Tool” on page 1626.
SNMP Browser	Browse an SNMP MIB and view available OIDs. For more information, see “SNMP Browser Tool” on page 1620.

Tool Name	Description
SNMP	Performs a SNMP get command to a specified SNMP host to retrieve a list of OIDs. For more information, see “SNMP Tool” on page 1623.
SNMP Trap	View the log of SNMP Traps received by SiteScope from SNMP-enabled devices. For more information, see “SNMP Trap Tool” on page 1624.
URL Sequence	Retrieve a sequence of URLs. For more information, see “URL Sequence Tool” on page 1627.
Web Service	Test the availability of SOAP enabled Web Services. For more information, see “Web Service Tool” on page 1630.
XSL Transform	Test custom XSL transformation of XML data to be monitored with the Browsable XML Monitor. For more information, see “XSL Transform Tool” on page 1634.

Server Diagnostic Tools

Tool Name	Description
Network	Display the server's network interface status and active connections. For more information, see “Network Tool” on page 1612.
Processes	Show a list of currently running processes either locally or on a remote server. For more information, see “Processes Tool” on page 1617.
Services	Show a list of currently running Windows Services. For more information, see “Services Tool” on page 1625.

Advanced Diagnostic Tools

Tool Name	Description
News Server	Check whether a News Server is operational. For more information, see “News Server Tool” on page 1613.
Event Log	Display portions of the Windows Event Log locally or on a remote server. For more information, see “Event Log Tool” on page 1602.
LDAP Authentication	Test an LDAP server by requesting a user authentication. For more information, see “LDAP Authentication Tool” on page 1607.
Performance Counters	Check connectivity to and values in Win NT Performance Counter registries. For more information, see “Performance Counters Tool” on page 1614.
Regular Expression	Test a regular expression for content matching against a sample of the content you want to monitor. For more information, see “Regular Expression Tool” on page 1618.

SiteScope Tools User Interface

This section includes the pages that are part of the SiteScope diagnostic tools user interface.

DNS Lookup Tool

Description	<p>Looks up names from a Domain Name Server and shows you the IP address for a domain name. It also shows you information about the name servers for a domain.</p> <p>You can use this utility to verify that your DNS server is returning the correct addresses for your own servers. You can also use it to verify that it is able to look up the addresses for external domains. The DNS Lookup form provides a gateway to the standard nslookup program.</p> <p>To access: Expand the Tools container in the monitor tree, and click DNS Lookup.</p>
Useful Links	"SiteScope Tools Overview" on page 1593

The DNS Lookup Tool page includes the following elements:

GUI Element	Description
DNS Address	Type the IP address of a DNS server. To check the local DNS server, type LOCAL.
Host Name	Type the domain name.
DNS Lookup	Click to initiate the test. The tool sends the request to the DNS server entered in the DNS Address text box and displays the IP address for the host name entered in the Host Name text box. The results of DNS Lookup are displayed beneath the button.

Database Connection Tool

<p>Description</p>	<p>The Database Connection diagnostic tool is used to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database. This diagnostic tool checks to see if:</p> <ul style="list-style-type: none"> ▶ the supplied database driver can be found and loaded ▶ a connection can be made to the database ▶ an optional SQL query can be run and the results displayed ▶ the database connection and resources can be closed <p>This tool can be useful in verifying connection parameter values needed to set up database monitors, database alerts, and database logging.</p> <p>To access: Expand the Tools container in the monitor tree, and click Database Connection.</p>
<p>Important Information</p>	<p>If exceptions or errors occur during the test, the information is printed along with suggested actions to help with troubleshooting.</p>
<p>Useful Links</p>	<p>“SiteScope Tools Overview” on page 1593</p>

The Database Connection Tool page includes the following elements:

GUI Element	Description
Database Connection URL	<p>Type the connection URL to the database you want to connect to. The syntax is <code>jdbc:oracle:thin:@<server name or ip address>:<database server port>:<sid></code>.</p> <p>Example: To connect to the ORCL database on a machine using port 1521, type <code>jdbc:oracle:thin:@206.168.191.19:1521:ORCL</code>. The colon (:) and @ symbols must be included as shown.</p> <p>Note: If you want to access the database using Windows authentication, type <code>jdbc:mercury:sqlserver://<server name or IP address>:1433DatabaseName=<database name>; AuthenticationMethod=type2</code> as the connection URL, and <code>com.mercury.jdbc.sqlserver.SQLServerDriver</code> as your database driver. Leave the Database User Name and Database Password boxes empty so that the credentials of the currently logged on Windows user (the account from which SiteScope service is running) are used to establish a connection to the database.</p>
Database Driver	<p>Type the JDBC or ODBC driver that SiteScope should use. The .jar file or library containing the .class file must be installed in the <code><SiteScope root directory>\java\lib\ext</code> directory. To use a database other than <code>jdbc:odbc:orders</code>, you must install the driver files into the proper directory before SiteScope can use them.</p>
Database User Name	<p>Type the user name required to connect to the database.</p>
Database Password	<p>Type the password required to connect to the database.</p>
Query	<p>(Optional) Type a SQL query to run on the database. If you do not supply a SQL query string, the driver is loaded and the connection to the database is tested but no query is run.</p>
Results Set Max Columns	<p>If you have entered a SQL Query, type the maximum number of columns to display in the query result set.</p>

GUI Element	Description
Results Set Max Rows	If you have entered a SQL Query, type the maximum number of rows to display in the query result set.
Connect and Execute Query	Click to run the connection test. Connection results are shown beneath the button.

The following is an example of the data returned from a successful database connection with a SQL query (limited to one row).

server Name	group ID	frame Index	frame ID	setting Name	setting Line	line Chunk	chunk Value
10.0.0.157	master.config	1	_config	_database Max Summary	1	1	200

Database Information Tool

Description	The Database Information diagnostic tool is used to display database server metadata such as product and driver version, SQL compatibility level information, and supported SQL functions. To access: Expand the Tools container in the monitor tree, and click Database Information .
Important Information	Different database drivers and user names can significantly change what information is displayed.
Useful Links	“SiteScope Tools Overview” on page 1593

The Database Information Tool page includes the following elements:

GUI Element	Description
Database Connection URL	Type the connection URL to the database you want to connect to. The syntax is <code>jdbc:oracle:thin:@<server name or ip address>:<database server port>:<sid></code> . Example: To connect to the ORCL database on a machine using port 1521, type <code>jdbc:oracle:thin:@206.168.191.19:1521:ORCL</code> . The colon (:) and @ symbols must be included as shown.
Database Driver	Type the JDBC or ODBC driver that SiteScope should use. The .jar file or library containing the .class file must be installed in the <code><SiteScope root directory>\java\lib\ext</code> directory. To use a database other than <code>jdbc:odbc:orders</code> , you must install the driver files into the proper directory before SiteScope can use them.
Database User Name	Type the user name required to connect to the database.
Database Password	Type the password required to connect to the database.
Get Database Info	Click to display database information. Connection results are shown beneath the button.

Event Log Tool

Description	Displays portions of the Windows event log locally or on a remote server. To access: Expand the Tools container in the monitor tree, and click Event Log .
Important Information	Different database drivers and user names can significantly change what information is displayed.
Useful Links	“SiteScope Tools Overview” on page 1593

The Event Log Tool page includes the following elements:

GUI Element	Description
Server Name	Type the name of that server for which you want to view event logs. Default value: The Event Log tool displays entries for the server on which SiteScope is installed.
Event Log	Choose which type of log file you want to view: <ul style="list-style-type: none"> ➤ System ➤ Application ➤ Security ➤ Directory Service ➤ DNS ➤ File Replication Service Default value: System
Entries To Show	The number of entries to list for this event log. The most recent entries in the log are displayed first. Default value: 10
Show Event Log Entries	Click to complete the action and refresh the log entry listing. Log entries are displayed beneath the button.

FTP Server Tool

Description	Use to access an FTP server and view the interaction between SiteScope (acting as an FTP client) and the FTP server. For example, if you receive an alert from SiteScope indicating that your FTP server is not working properly, the first step is to use this tool to help track down the problem. To access: Expand the Tools container in the monitor tree, and click FTP Server .
Useful Links	“SiteScope Tools Overview” on page 1593

The FTP Server Tool page includes the following elements:

GUI Element	Description
FTP server	Type the IP address or the name of the FTP server that you want to test. Example: 206.168.191.22 or ftp.thiscompany.com
File name	Type the file name to retrieve. Example: /pub/docs/mydoc.txt
User name	Type the name used to log into the FTP server.
Password	Type the password used to log into the FTP server.
Use Passive	Select this check box to have SiteScope use a passive FTP connection. This is commonly required to access FTP servers through a firewall.
Proxy	Type the proxy name or IP address if you want to use a proxy server for the FTP test.
Proxy User Name	Type the name used to log into the proxy server.
Proxy Password	Type the password used to log into the proxy server.
Check FTP Server	Click to initiate the test. Check FTP server results are displayed beneath the button.

The following is a sample output from the Check FTP Server tool. In this case, the FTP server allowed us to log on without a problem, indicating that the server is running and accepting requests. The failure is caused when the server was unable to locate the file that was requested: file.txt. Correcting this particular problem may be as easy as replacing the missing file or verifying the file location.

```
Received: 220 public Microsoft FTP Service (Version 2.0).  
Sent: USER anonymous  
Received: 331 Anonymous access allowed, send identity (e-mail name) as password.  
Sent: PASS anonymous  
Received: 230 Anonymous user logged in.  
Sent: PASV  
Received: 227 Entering Passive Mode (206,168,191,1,5,183).  
Connecting to server 206.168.191.1 port 1463  
Sent: RETR file.txt  
Received: 550 file.txt: The system cannot find the file specified.  
Sent: QUIT  
Received: 221
```

Get URL and URL Content Tool

Description	<p>Use to retrieve an item from a Web server. The URL specifies the server to contact and the item to return. Because SiteScope displays the content of the requested URL, this tool also functions to check URL Content. You can use this utility to verify that a given URL can be accessed from a Web server. You can also use it to see how long it takes for the page to be returned.</p> <p>To access: Expand the Tools container in the monitor tree, and click Get URL and URL Content.</p>
Useful Links	"SiteScope Tools Overview" on page 1593

The Get URL Tool page includes the following elements:

GUI Element	Description
URL	<p>Type the URL that you want to test.</p> <p>Example: http://demo.company.com</p>
URL Content Encoding	<p>Encoding compresses the content before it is sent to the client. The content is decoded by the client. If you use more than one encoding, they must be separated by commas (,) and in the exact order in which they are to be performed on the URL content.</p> <p>Example: ISO8859-1</p>
User name	If the URL specified above requires a name and password for access, type the user name.
Password	If the URL specified requires a name and password for access, type the password.
Domain (only on Windows platform)	Type the domain name of the SiteScope server.
Use NTLM V2	Check this parameter if you want to use NTLM (Windows NT LAN Manager) version 2 to authenticate user logon.
Proxy	Optionally, a proxy server can be used to access the URL. Type the address or domain name and port of an HTTP Proxy Server.

GUI Element	Description
Proxy User Name	Type the name used to log into the proxy server.
Proxy Password	Type the password used to log into the proxy server.
Proxy Use NTLM V2	Check this parameter if the proxy uses NTLM (Windows NT LAN Manager) version 2 to authenticate user logon.
Content Match	Type a string of text to check for in the returned page or frame set. If the text is not contained in the page, the content match fails. The search is case sensitive. HTML tags are part of a text document, so you must include the HTML tags if they are part of the text you are searching for (for example, "< B> Hello< /B> World").
Error Content Match	Type a string of text to check for in the returned page or frame set. If the text is contained in the page, the test indicates an error condition. The search is case sensitive.
Retrieve Frames	Check this option to have SiteScope display the HTML code of a frame linked to the URL being requested.
Retrieve Images	Check this option to have SiteScope list the images such as graphics, logos, and so on linked to the URL being requested.
Get URL	Click to initiate the test. URL results are displayed beneath the button. The results include statistics on the URL retrieval as well as a text representation of the URL content.

LDAP Authentication Tool

Description	Verifies that a Lightweight Directory Access Protocol (LDAP) server can authenticate a user by performing a simple authentication. To access: Expand the Tools container in the monitor tree, and click LDAP Authentication .
Useful Links	"SiteScope Tools Overview" on page 1593

The LDAP Authentication Tool page includes the following elements:

GUI Element	Description
Security Principal	Type the constant that holds the name of the environment property for specifying the identity of the principal that authenticates the caller to the service. The format of the principal depends on the authentication scheme. If this property is unspecified, the behavior is determined by the service provider. This should be in the format: uid=testuser,ou=TEST,o=mydomain.com. Note: SiteScope does not support users that contain one or more of the following character inside the users name: equal ("="), semi-colon (";"), inverted commas ("").
Security Credential	Type the constant that holds the name of the environment property for specifying the credentials of the principal for authenticating the caller to the service. The value of the property depends on the authentication scheme. For example, it could be a hashed password, clear-text password, key, certificate, and so on. If this property is unspecified, the behavior is determined by the service provider.

GUI Element	Description
URL Provider Address	<p>Type the constant that holds the name of the environment property for specifying configuration information for the service provider to use. The value of the property should contain a URL string. This property may be specified in the environment, an applet parameter, a system property, or a resource file. If it is not specified in any of these sources, the default configuration is determined by the service provider.</p> <p>Example: ldap://<somehost>:389</p>
LDAP Query	<p>Use this box to type an object query to look at a LDAP object other than the default user dn object. You must type a valid object query in this text box if you are using a LDAP filter. For details about the search filter, see the description below.</p> <p>Example: Type the mail object to check for an e-mail address associated with the dn object entered above.</p>
Search Filter	<p>Type a search filter in this text box to perform a search using a filter criteria. The LDAP filter syntax is a logical expression in prefix notation meaning that logical operator appears before its arguments.</p> <p>Example: The item sn=Freddie means that the sn attribute must exist with the attribute value equal to Freddie.</p> <p>Multiple items can be included in the filter string by enclosing them in parentheses, such as (sn=Freddie) and combined using logical operators such as the & (the conjunction operator) to create logical expressions.</p> <p>Example: The filter syntax (& (sn=Freddie) (mail=*)) requests LDAP entries that have both a sn attribute of Freddie and a mail attribute.</p>
Authenticate User	<p>Click to initiate the test. LDAP Authentication test results are displayed beneath the button.</p>

Mail Round Trip Test Tool

Description	<p>Checks a Mail Server by using the network and verifies that the mail server is accepting requests and that a message can be sent and retrieved. It does this by sending a standard mail message using SMTP and then retrieving that same message by using a POP user account. Each message that SiteScope sends includes a unique key which it checks for to insure that it does not retrieve the wrong message and return a false OK reading.</p> <p>To access: Expand the Tools container in the monitor tree, and click Mail Round Trip Test.</p>
Useful Links	<p>“SiteScope Tools Overview” on page 1593</p>

The Mail Round Trip Test Tool page includes the following elements:

GUI Element	Description
Message	<p>Select the action to take:</p> <ul style="list-style-type: none"> ▶ Send & Receive. Allows you to send a test message to an SMTP server and then receive it back from the POP3 or IMAP4 server to check that the mail server is up and running. (Default) ▶ Receive Only. Checks the incoming POP3 or IMAP4 mail servers for a message that was sent previously. This check is done by matching the content of the previously-sent message. <p>Note: If this option is selected, the Content Match text box must have a value to match against.</p> ▶ Send Only. Checks that the receiving mail server has accepted the message.
Send To Address	<p>Type the mail address to which the test message should be sent. This should be the address for the POP account specified in the Mail Server User Name box.</p> <p>Example: If you specified support as the Mail Server User Name, the Send To Address might be support@mycompany.com.</p>

GUI Element	Description
Sending Mail Server (SMTP)	Type the hostname of the SMTP mail server to which the test mail message should be sent. Example: mail.thiscompany.com
Receiving Server Type	Select the protocol used by the receiving mail server. Use the POP3 option to check the POP3 mail server for a sent message. Use the IMAP4 option to check the IMAP mail server for a sent message. Default value: POP3
Receiving Mail Server	Type the hostname of the POP mail server that should receive the test message. This can be the same mail server to which the test message was sent. Example: mail.thiscompany.com
Receiving Mail Server User Name	Type a POP user account name. A test e-mail message is sent to this account and the Mail monitor logs in to the account to verify that the message was received. No other mail in the account is touched. You can use your own personal mail account or another existing account for this purpose. Note: If you use an e-mail reader that automatically retrieves and deletes messages from the server, there is a chance that the Mail Monitor never sees the mail message and reports an error.
Receiving Mail Server Password	Type a password, if necessary, for the test mail account.
NTLM Authentication	If NTLM authentication is used by the e-mail server, select the NTLM version (version 1 or 2). Default value: none
Timeout	The number of seconds to wait for a mail message to be received before timing-out. Default value: 300

GUI Element	Description
Retrieve Pause	<p>After SiteScope sends the test message, it immediately logs into the mail account to verify that the message has been received. If the message has not been received, SiteScope automatically waits a specified number of seconds before it checks again.</p> <p>Default value: 10</p>
Content Match	<p>Type a string of text to match against the contents of the incoming message. If the text is not contained in the incoming message, the monitor is in error. This is for the receiving only option (for example, Subject:MySubject). The search is case sensitive.</p> <p>HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, "< B> Hello< /B> World"). This works for XML pages as well.</p> <p>You can perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching. An example might be <code>"/href=Doc\d+\.html/"</code> or <code>"/href=doc\d+\.html/i"</code>.</p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a regular expression (for example, <code>/Temperature: (\d+)/</code>). This returns the temperature as it appears on the page and can be used when setting an Error if or Warning if threshold.</p>
Show Details	<p>Select this box if you want details of the round trip test to be displayed</p>
Check Mail Server	<p>Click to initiate the test. Check mail server test results are displayed beneath the button.</p>

Network Tool

<p>Description</p>	<p>The Network Tool reports the current network interface statistics and lists the active network connections. This information can be useful to determine the health of your network interface. You can also use this tool to track down problems where network connections are being left open or runaway conditions where an increasing number of connections are being opened without being closed.</p> <p>To access: Expand the Tools container in the monitor tree, and click Network.</p>
<p>Useful Links</p>	<p>“SiteScope Tools Overview” on page 1593</p>

The Network Tool page includes the following elements:

GUI Element	Description
<p>Run Network</p>	<p>The Network Tool runs once when it is opened and reports the network information. Click to update the data returned by the network tool. The data is displayed beneath the button.</p>

News Server Tool

Description	You can use the Check News Server as a tool to access a news server and view the NNTP interaction between SiteScope (acting as a news client) and the news server. To access: Expand the Tools container in the monitor tree, and click News Server .
Useful Links	“SiteScope Tools Overview” on page 1593

The News Server Tool page includes the following elements:

GUI Element	Description
News Server	Type the name of the News server in the format news.sitescope.com or news.sitescope.com:7777.
News groups	(Optional) Type one or more news groups. Separate multiple news group names by commas (",").
User name	If the News server specified above requires a name and password for access, type the user name.
Password	If the News server specified above requires a name and password for access, type the password.
Check News Group	Click to initiate the test. The results of the test are displayed beneath the button.

Performance Counters Tool

Description	<p>The Performance Counter Test is a tool that you can use to check performance counters on a specific machine in a Windows NT/2000 network. It provides an interface to the perfex.exe executable supplied as part of SiteScope.</p> <p>To access: Expand the Tools container in the monitor tree, and click Performance Counter.</p>
Useful Links	"SiteScope Tools Overview" on page 1593

The Performance Counters Tool page includes the following elements:

GUI Element	Description
Machine Name	<p>Type a machine name to list all NT performance counter objects available on that machine. A double slash ("\\") is automatically prefixed to any machine name supplied.</p> <p>Default value: localhost</p>
Admin User Account/ Password	<p>Type the administrative user name and password for the machine you want to query. This is only necessary if you running SiteScope under an account that does not have administrative privileges to access performance counters for the domain or workgroup to which you are trying to connect.</p> <p>If the test indicates you are required to supply a password, it means that the remote machine requires authorization to access the performance counter registry.</p>

GUI Element	Description
Counter Object Name	<p>Select the counters to list. This box displays one of the following values:</p> <ul style="list-style-type: none"> ▶ Choose a counter object. Click the List Objects and Enumerate Counters button to display the individual NT performance counters and corresponding values for the selected counter object. ▶ NO COUNTER OBJECTS AVAILABLE using this user name and password. You must provide a user name and password to see the counter objects. The remote machine you are connecting to does not recognize the user that the SiteScope service is currently running as VALID user with local admin rights. If you have the correct user name and password, click the List Objects and Enumerate Counters button to update the display. ▶ <One of the counter objects available on the machine named in the Machine Name box>. A counter selection has already been made. The data for that counter is displayed in the table in the lower portion of the page. The table shows the counter name, the value, and a description of the counter provided by the counter registry.
List Objects and Enumerate Counters	<p>Click to display the individual NT performance counters and corresponding values for the selected counter object. This information is displayed beneath the button.</p>

Ping Tool

Description	<p>Ping is a tool that sends a packet to another location and back to the sender. It shows you the round-trip time along the path. When there is a problem with the network, ping can tell you if another location can be reached. The Ping tool does a ping from the current server to another location.</p> <p>To access: Expand the Tools container in the monitor tree, and click Ping.</p>
Useful Links	<p>“SiteScope Tools Overview” on page 1593</p>

The Ping Tool page includes the following elements:

GUI Element	Description
Domain Name or IP address	<p>Type the domain name or IP address of the location you want to ping in the text box.</p> <p>Example: demo.thiscompany.com or 206.168.112.53</p>
Ping	<p>Click to ping the domain name or IP address. The results of the test are displayed beneath the button.</p>

Processes Tool

Description	<p>The Processes tool displays processes running on the server where SiteScope is installed. This can be useful to confirm that critical processes are available.</p> <p>To access: Expand the Tools container in the monitor tree, and click Processes.</p>
Useful Links	“SiteScope Tools Overview” on page 1593

The Processes Tool page includes the following elements:

GUI Element	Description
Server	<p>By default, SiteScope displays the processes running on this server. To view the processes running on another NT server, type the name of that server. For example, \\TEST. If there are remote UNIX machines defined they are displayed in a drop-down selection. You can select a Remote UNIX to see the processes running on the remote computer. You cannot type a Remote UNIX in the entry box.</p>
Show Processes	Click to initiate the test. The results of the test are displayed beneath the button.

Regular Expression Tool

Description	Enables you to perform a regular expression match. To access: Expand the Tools container in the monitor tree, and click Regular Expression .
Useful Links	“SiteScope Tools Overview” on page 1593

The Regular Expression Tool page includes the following elements:

GUI Element	Description
Your Text that will be matched	<p>Cut and paste a portion of text containing the string or values on which you want to perform a regular expression match into this box.</p> <p>For efficiency in developing regular expressions, you should include all of the content that would precede the target data or pattern that you want to match. For example, when developing a regular expression for content matching on a Web page, you should use the Get URL and URL Content Tool to retrieve the entire HTTP content including the HTTP header.</p>
Your Regular Expression	<p>Type a regular expression between the slashes //, to match some part of the text you entered.</p> <p>Note: For content with multiple lines with carriage returns and line feeds, consider adding the s search modifier to the end of the expression to have the content treated as a single line of text.</p> <p>Example: /value:\W[\d]{2,6}/s</p>
Test Your Match	<p>Click to perform the test. The results of the match test are displayed beneath the button. If there is a problem with your regular expression, an error message is displayed.</p>

Parsed Parentheses and Matches Table

This section includes a table that displays any matches requested as retained values or back references by pairs of parentheses inside the regular expression. If your expression does not include parentheses, this table is empty. The columns of the parsed parentheses table are:

GUI Element	Description
Parentheses counted from left	Displays any patterns in the regular expression delimited by parentheses as counted from the left-hand side of the expression.
Matching text	Displays the text that matched the parenthesis marked patterns listed in the column to the left.
Whole Match Between Slashes	This is the text area below the table. It echoes the entire content entered in the Your Text that will be matched box. The content that matched the pattern in your regular expression is highlighted within this content, normally using a blue font. This is useful for showing possible problems with wildcard expressions like the .* pattern that match too much content. It can also uncover problems of duplicate patterns within the content that require you to add other unique patterns to your expression to match the desired portion of the content.

SNMP Browser Tool

<p>Description</p>	<p>The SNMP Browser Tool provides a browsable tree representation of an SNMP agent's MIB. It can be used to verify the connection properties of an SNMP agent and to gain more information about the MIBs which that agent implements.</p> <p>This tool operates by traversing all of the OIDs on a given agent and then using the MIB information in the <SiteScope root directory>\templates.mib directory to build a tree-structured XML representation of the OIDs. Included in the XML tree are the textual and numeric names of the OIDs, their descriptions (if available), and their values at the time of traversal.</p> <p>The XML is displayed in a separate browser window, using the browser's default display for XML data. For IE and Netscape/Mozilla browsers, this default display is in the form of a collapsible, hierarchical tree. If errors occur during the MIB traversal, an error message describing the problem is printed in the new window (instead of XML).</p> <p>The SNMP by MIB Tool is intended to help in configuring any of the SNMP-based monitors, including, SNMP by MIB Monitor, SNMP Monitor, Cisco Works Monitor, and F5 SNMP Monitor.</p> <p>To access: Expand the Tools container in the monitor tree, and click SNMP Browser.</p>
<p>Useful Links</p>	<p>“SiteScope Tools Overview” on page 1593</p>

The SNMP Browser Tool page includes the following elements:

GUI Element	Description
<p>Host or IP Address</p>	<p>Type the hostname or IP address of the device on which the SNMP agent is running.</p>
<p>Port</p>	<p>Type the port on which the SNMP agent is listening. Default value: 161</p>

GUI Element	Description
MIB	<p>Choose the MIB that you want to view. If you select All MIBs, then all data obtained during the MIB traversal is displayed. If you select a specific MIB, then only the OIDs within that MIB are displayed. This list of MIBs can be updated or extended by placing new MIB files in the <SiteScope root directory>\templates.mib directory.</p> <p>Default value: All MIBs</p>
Starting OID	<p>Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered in this box. The default value is 1, which is commonly used and applicable to most applications. You should edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value of 1 did not enable retrieving any counters, then you may have to type a different value in this box.</p>
Version	<p>Select the version of SNMP which the tool should use when connecting to the agent.</p> <p>Default value: V1</p>
V1/V2 Community	<p>For version 1 or 2 connections, type the community string to use when connecting to the SNMP agent.</p> <p>Default value: public</p>
V3 Authentication Type	<p>Select the type of authentication to use for a version 3 connection.</p> <p>Default value: MD5</p>
V3 Username	<p>Type the user name for a version 3 connection.</p>
V3 Authentication Password	<p>Type the password to use for authentication in a version 3 connection.</p>
V3 Privacy Password	<p>Type the password to use for DES privacy encryption in a version 3 connection. Leave this box blank if no privacy is desired.</p>

GUI Element	Description
V3 Context Engine ID	Type a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.
V3 Context Name	Type the Context Name to use for this connection. This is applicable for SNMP V3 only.
Browse	Click to open a new window containing a browsable view of the MIB (in XML).

SNMP Tool

Description	The SNMP tool lets you query a SNMP Management Information Base (MIB) and retrieve a set of OIDs. To access: Expand the Tools container in the monitor tree, and click SNMP .
Useful Links	“SiteScope Tools Overview” on page 1593

The SNMP Tool page includes the following elements:

GUI Element	Description
IP Address	Type the IP Address of the server that hosts the SNMP MIB you want to query.
Next OID	Type the OID of the next OID that should be retrieved.
Index	Type the index of the SNMP object. Values for an OID come as either scalar or indexed (array) values. For a scalar OID, the index value must be set to 0. For an indexed value, you must provide the index (a positive integer starting with 1) to the element that contains the value you want. Example: OID 1.3.6.1.2.1.2.2.1.17 is an indexed value that contains four elements. To access this second element of this OID, type an index of 2 in this text box. Default value: 0
Community	Type the Community string for the SNMP device. Default value: public
Version (V1 or V2)	Select the SNMP version used by the SNMP host you want to test. SiteScope supports both SNMP version 1 and version 2. Default value: V1
Number of Records to get	Type the number of OID records to retrieve. Default value: 1
Next Block of OIDs	Click to perform the query. The results of the test are displayed beneath the button.

SNMP Trap Tool

Description	Lets you view SNMP Traps received by SiteScope's SNMP listener. The tool is only enabled if you have already created one or more SNMP Trap Monitors. Creating an SNMP Trap Monitor enables the SiteScope SNMP Trap Log. To access: Expand the Tools container in the monitor tree, and click SNMP Trap .
Important Information	The message Receiving SNMP Traps is not active is displayed at the top of the tool page if the SNMP Trap Log is not currently active.
Useful Links	"SiteScope Tools Overview" on page 1593

The SNMP Trap Tool page includes the following elements:

GUI Element	Description
Traps To Show	Type the number of SNMP Traps to list. The most recent SNMP Traps received by SiteScope are displayed first. Default value: 10
Content Match	Type an optional text string or regular expression to be used to match entries in the SNMP Trap Log. Content matching can be done for data from any of the columns of the log such as OID, Community, Agent, and so on. The SNMP traps in the SiteScope SNMP Trap Log are displayed in the SNMP Trap Log table. The number of traps matching the search criteria are displayed in the SNMP Trap Log table title displayed in the lower part of the page.
Show SNMP Trap Log Entries	Click to view the log based on the search criteria you have entered. The results of the test are displayed beneath the button.

Services Tool

Description	<p>Displays services running on the server where SiteScope is installed. This can be useful to confirm that critical services are available. If Remote UNIX machines have been defined, they are listed in a drop-down menu.</p> <p>To access: Expand the Tools container in the monitor tree, and click Services.</p>
Useful Links	"SiteScope Tools Overview" on page 1593

The Services Tool page includes the following elements:

GUI Element	Description
Server	<p>By default, SiteScope displays the services running on this server. To view the services running on another NT server, type the name of that server. For example, \\TEST. If there are remote UNIX machines defined they are displayed in a drop-down selection. You can select a Remote UNIX to see the services running on the remote computer. You cannot type a Remote UNIX in the entry box.</p>
Show Services	<p>Click to initiate the test. The results of the test are displayed beneath the button.</p>

Trace Route Tool

Description	<p>Trace Route is a tool that shows you the network path between two locations and how long it takes to get to each hop in the path. When there is a problem with the network, traceroute can often be used to narrow down where the problem is occurring. This tool performs a traceroute from your server to another location.</p> <p>You can use this utility to verify connectivity of a host and to determine how the host is connected to the Internet. You can also determine the path taken from your server to the specified host. This helps you to determine where packet loss may be occurring when you attempt to connect to hosts elsewhere on the Internet.</p> <p>To access: Expand the Tools container in the monitor tree, and click Trace Route.</p>
Important Information	<p>You can use this tool to perform a traceroute on Windows platforms only. For UNIX, you must stop the SiteScope process, add the path of the traceroute utility (for example <code>/usr/sbin/traceroute</code>) to the Traceroute command box in Infrastructure Settings Preferences, and then restart SiteScope.</p>
Useful Links	<p>“SiteScope Tools Overview” on page 1593</p>

The Trace Route Tool page includes the following elements:

GUI Element	Description
Domain Name or IP address	<p>Type the domain name or IP address of the other location.</p> <p>Example: demo.thiscompany.com or 206.168.112.53</p>
Trace Route	<p>Click to initiate the action. The results of the test are displayed beneath the button.</p>

URL Sequence Tool

<p>Description</p>	<p>Simulates a user's session across several pages. An example of this would be entering an account name by using a Web form, checking an account status for the page that is returned, and then following a sequence of links through several more pages.</p> <p>A URL Sequence is specified by giving a URL to start at and then specifying either additional URLs, or more commonly, links or buttons to follow. For each step you may specify a match or error string to search for, a user name and password to type, and POST data for that step.</p> <p>The URL Sequence tool returns the status and time taken for each step in the sequence. It also embeds a copy of the page returned at each step of the sequence in its output so that a more graphical view of the sequence can be viewed.</p> <p>To access: Expand the Tools container in the monitor tree, and click URL Sequence.</p>
<p>Useful Links</p>	<p>"SiteScope Tools Overview" on page 1593</p>

The URL Sequence Tool page includes the following elements:

GUI Element	Description
<p>Step 1 - Reference</p>	<p>Select the type of object or target from the drop-down list in the first column. This represents the either a Web page, a hyper link, form element, and so on, that defines the sequence path. The type for Step 1 should always be a URL. Type the specific URL of the first page in the sequence that you want SiteScope to complete.</p> <p>Example: If you want SiteScope to test your order process, you might type a URL such as https://www.securecompany.com/order.html.</p>
<p>Step (2 thru N) - Reference</p>	<p>From Step 2 on, you must tell SiteScope what you want it to do next. In the Type column, tell SiteScope what type of item to look for in this step. For example, if SiteScope is to do the equivalent of selecting a submit button, you would choose the Form - match the displayed name of a Submit button. SiteScope uses this information to scan the HTML for the proper text matches.</p> <p>Type the URL, link, or Submit button to be followed in the second column for this step. For example, if SiteScope should follow the Submit button on the page and the name on the button (its value) is <i>Place My Order</i>, type <i>Place My Order</i> in this text box. To instruct SiteScope to follow a link on the page, type the text of the link. For example, if the link says <i>Next</i>, type the word <i>Next</i> in this text box. You can also type in a full URL.</p> <p>If an image is used as the Submit button, you must type the name value for the image. You find this name value by looking at the HTML for the form.</p> <p>The Advanced Settings section gives you the ability to customize error and warning thresholds, or complete other optional settings.</p>

GUI Element	Description
POST Data	If this step contains a URL for a POST request, type the post variables, one per line as name=value pairs. This option is used to verify that a form is working correctly by performing the same request that occurs when a user submits a form. See also the Match Content box for a way to verify that the correct form response was received. If this item is blank, a GET request is performed.
Match Content	Type an expression describing the values to match in the returned page. If the expression is not contained in the page, the message no match on content is displayed. A regular expression can be used to define the values to match.
Error If Match	Type an expression describing the values that, if found on the page returned, indicate an error in the sequence process. For example, if the phrase Login Error appears, there may be a problem with user profile data. If the Error If Match expression is found in the page, the monitor signals an error. A regular expression can be used to define the values to match.
User Name	Type the user name, if any, required for this step.
Password	Type the password, if any, required for this step.
Delay	Type an optional delay period that SiteScope waits before executing the next step.
Title	Type an optional title to be associated with this step of the sequence. It is best to select a title that describes what is being accomplished in this step.
Check URL Sequence	Click to test the transaction. The results of the test are displayed beneath the button.

Web Service Tool

<p>Description</p>	<p>Checks Simple Object Access Protocol (SOAP) enabled Web services for availability, stability, or to see what an actual SOAP response looks like. It is also useful for diagnosing a Web service request failure, or for picking out match strings for use with a specific Web Service Monitor. The Web Service Test sends a SOAP request to the server and checks the HTTP response codes to verify that the service is responding. The actual SOAP response is displayed, but no further verification is done on this returned message.</p> <p>SOAP is a way for a program running under one operating system to communicate with another program running under the same or different operating system (such as a Windows 2000 program talking to a Linux-based program). SOAP uses the Hypertext Transfer Protocol (HTTP) and Extensible Markup Language (XML) for information exchange with services in a distributed environment.</p> <p>To access: Expand the Tools container in the monitor tree, and click Web Service.</p>
<p>Important Information</p>	<ul style="list-style-type: none"> ▶ The following specification features are currently supported: WSDL 1.2, SOAP 1.1, Simple and Complex Types based on XML Schema 2001, SOAP binding with the HTTP(s) protocol only. SOAP with Attachments is not supported. ▶ SOAP and WSDL technologies are evolving. As a result, some WSDL documents may not parse accurately and some SOAP requests may not interact with all Web service providers.
<p>Useful Links</p>	<p>“SiteScope Tools Overview” on page 1593</p>

The Web Service Tool page includes the following elements:

GUI Element	Description
WSDL Path or URL	Type the URL or the file path of the WSDL file to be used for this monitor. If a WSDL file path is specified it must be relative to <SiteScope root directory>\templates.wsdl\ . In addition, your WSDL files must have an extension of .wsdl.
Web Service URL	Type the URL of the Web service to be tested.
Method Name	Type the name of the method to be run.

GUI Element	Description
Arguments	<p>Type the arguments to the method specified above and their types. Specify simple type parameters in the format <code>parm-name(parm-type) = value</code>, where the <code><param-name></code> and <code><param-type></code> must match the service method specifications of its WSDL file exactly. The <code><value></code> must agree with the <code><param-type></code>, otherwise the request fails. Strings with embedded spaces should be enclosed in double quotes (" "). Each parameter must be on a separate line by adding a carriage return at the end of each value.</p> <p>Example: <code>stockSymbol (string) = MERQ</code> <code>numShares (int) = 10</code></p> <p>A complex type parameter must be represented as one long string (line breaks are for readability purposes only):</p> <pre>stocksymbol[COMPLEX] = <stocksymbol xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fw100="urn:ws-stock" xsi:type="fw100:getQuote"> <ticker xsi:type="xsd:string">MERQ </ticker> </stocksymbol></pre> <p>Note: SiteScope does not perform any validation on your input parameter lists, so make sure that the complex type values are valid and well-formed XML strings. Do not add any carriage returns within a complex type parameter—only at the end.</p> <p>If the Web service method does not take any parameters, the text box should be left empty.</p>
SOAP Action URI	<p>The SOAP Action URI in the header of the SOAP request to the Web Service. During initial setup this is extracted from the WSDL file.</p>
User-Agent	<p>Type the user agent that sends the request (Mozilla, Internet Explorer, and so on).</p>

GUI Element	Description
Method Namespace	The XML name space for the method in the SOAP request. During initial setup this value is extracted from the WSDL file.
User Name	If the URL specified requires a name and password for access, type the name.
Password	If the URL specified requires a name and password for access, type the password.
NTLM Domain	Type the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL.
Proxy	Optionally, a proxy server can be used to access the URL. Type the domain name and port of the HTTP Proxy Server.
Proxy User / Proxy Password	If the proxy server requires a name and password to access the URL, type the user name. Your proxy server must support Proxy-Authenticate for this options to function.
Web Service Request	Click to test the Web Service request. The results of the test are displayed beneath the button.
Status	<p>The possible status values returned by the test are:</p> <ul style="list-style-type: none"> ➤ OK ➤ unknown host name ➤ unable to reach server ➤ unable to connect to server ➤ timed out reading ➤ content match error ➤ document moved ➤ unauthorized ➤ forbidden ➤ not found ➤ proxy authentication required ➤ server error ➤ not implemented ➤ server busy

XSL Transform Tool

Description	<p>Use this tool to test a user defined XSL file that can be used to transform an XML file or output. This might be a file from a Web application that contains performance metrics data. The use of an XSL transform may be necessary to process the XML data into an acceptable format for use by the Browsable XML Monitor type.</p> <p>To access: Expand the Tools container in the monitor tree, and click XML Transform.</p>
Useful Links	“SiteScope Tools Overview” on page 1593

The XML Transform Tool page includes the following elements:

GUI Element	Description
XML URL	Type the URL of the XML file that is the input for the transformation.
XSL File	Type the path to the XSL file you want to test.
User Name	If access to the target XML file requires authentication, type the user name needed to access the content.
Password	If access to the target XML file requires authentication, type the password needed to access the content.
Proxy	If you are using a proxy to access the target XML content, type the address of the proxy.
Proxy User Name / Proxy Password	If you are using a proxy to access the target XML content, type the user name needed to use the proxy in this box.

Index

A

- Absolute Schedule Preferences 224
- Acknowledge dialog box 430
- acknowledgements
 - events 195
 - monitor status 195
- Active Directory
 - monitoring solution 1279
- Active Directory solution template
 - deploying 1281
- adaptors
 - adding SiteScope UNIX adaptors 1530
 - SiteScope UNIX adaptor command list 1534
 - SiteScope UNIX adaptor file format 1532
 - SiteScope UNIX adaptors 1530
 - SiteScope UNIX default adaptor file list 1531
- Add Dashboard Favorite dialog box 432
- adherence levels, fine-tuning 532
- administrator, login account 33
- advanced settings
 - for Management reports 1453
 - for Monitor reports 1466
 - for Quick reports 1461
- Affected Objects page, Global Search and Replace 359
- aggregation 115
- AIX Host solution template
 - deploying 1287
- AIX Host, monitoring solution 1285
- Alert action wizard 1421
- alert actions, creating 1389
- Alert log 405
- Alert report
 - example 1471, 1473
 - Alert Report page 1447
 - Alert Settings 268
 - Alert Settings, Infrastructure Settings Preferences 268
 - Alert table, in reports 1451, 1465
- Alerts
 - Configuring SiteScope 508, 1415
 - SiteScope Alert Action wizard 1421
- alerts
 - copying and pasting 1409
 - creating 1409
 - creating alert actions 1389
 - customizing message content 1411
 - database 1396
 - editing 1415
 - E-mail 1398
 - enable-disable monitor 1397
 - Log Event 1399
 - Pager 1400
 - Post 1401
 - script 1402
 - SMS 1406
 - SNMP Trap 1407
 - sound 1408
 - table of, in reports 1451, 1465
 - testing 1410
 - triggering 1390
 - understanding 1386
- Annotation Tool
 - Baseline Monitor Measurement Graphs 543
 - Server-Centric Reports 442
 - settings 1484
- Apache Server Monitor Settings 629
- ASP Server Monitor Settings 627
- audit log
 - alerts 392

- applying templates 388
- categories 394
- change password 394
- configuring 382
- create templates 389
- delete templates 389
- failed login 393
- global search and replace operations 393
- group operations 385
- login and logout 393
- modify templates 389
- monitor operations 386
- overview 376
- reports 392
- SiteScope startup 385
- template alerts 391
- template containers 388
- template groups 390
- template monitors 391
- template remote objects 390
- template variables 389
- update to general Preferences 386
- update to other Preferences 387

Audit log troubleshooting 409

auto template deployment 1253

- deployment results 1262
- global variables 1257
- instance variables 1257
- limitations 1272
- mandatory variables 1257
- publishing template changes 1259
- template update report 1261
- troubleshooting 1272
- variables 1257
- XML attributes reference 1271
- XML elements reference 1269
- XML file example 1255
- XML tag reference 1269
- XML validator 1259

B

- BAC Integration Statistics 395
- baseline
 - disable baseline mode 511

- monitor status 511
 - setting error boundaries 532
- baseline properties 546
- Baseline Settings 273
- Baseline Settings, Infrastructure Settings Preferences 273
- baseline status 546
- Best Case Calculation option, in reports 1453, 1466
- BroadVision Application Server Monitor 554
- BroadVision Application Server Monitor Settings 631
- browser language preference 214
- Business Availability Center 216, 234
 - changing the Gateway server 218
- Business Availability Center Preferences 216
- Business Availability Center-SiteScope connection, using SSL 217

C

- Check Point Firewall-1 Monitor Settings 632
- Choose Changes page, Global Search and Replace 356
- Cisco Works Monitor Settings 634
- Citrix Server Monitor
 - troubleshooting tips 557
- Citrix Server Monitor Settings 638
- Classic UI Settings 271
- Classic UI Settings, Infrastructure Settings Preferences 271
- ColdFusion Server Monitor Settings 640
- COM+ Server Monitor Settings 642
- configuration files
 - enabling use of 212
- configuring BAC integration preferences
 - limitations and troubleshooting 340
- connection methods for UNIX servers 299
- Content Changes dialog box 1244
- content match
 - examples for log files 1511
 - using metacharacters 1499
 - using regular expressions 1493
 - using string literals 1497
 - using system date variables 1506

- contents tab
 - monitor tree navigation 170
 - context menu options
 - SiteScope objects 176
 - count warning as good, in report uptime
 - readings 1449, 1463
 - Credential Preferences
 - concept 229
 - configuring 243
 - user interface 332
 - custom columns
 - about 1582
 - creating 1581
 - syntax 1592
 - working with 1584
 - custom formatting
 - for SiteScope reports 1451, 1465
 - custom monitor properties
 - syntax 1590
 - working with 1582, 1585
 - custom properties
 - about 1582
 - creating 1581
 - displaying in columns 1585
 - in alert templates 1583
 - selection list for 1587
 - custom reports
 - SiteScope Data over Time 148
 - SiteScope Group Performance 148
 - SiteScope Monitor Performance 147
 - SiteScope Overall Performance 148
 - System Availability Management
 - reports in 147
 - cygwin OpenSSH, installing on Windows 1550
- D**
- Dashboard Filter page 433
 - Dashboard Layout page 437
 - data aggregation 115
 - database alerts
 - working with 1396
 - Database logging 221, 301
 - troubleshooting database connections 341
 - Delete Dashboard Favorites dialog box 433
 - Deploy Monitors Using the Monitor
 - Deployment Wizard 90
 - description property, in reports 1454
 - detailed monitor information, in reports 1453, 1466
 - DHCP Monitor 850
 - diagnostic tools 1593
 - Get URL and URL Content 1605
 - LDAP Authentication 1607
 - Mail Round Trip 1609
 - Network 1612
 - News Server 1613
 - NT Performance Counter 1614
 - Ping 1616
 - Processes 1617
 - Regular Expression 1618
 - Services 1625
 - SNMP 1623
 - SNMP Browser 1620
 - SNMP Trap 1624
 - TraceRoute 1626
 - URL Sequence 1627
 - Web Service 1630, 1634
 - XSL Transform 1634
 - disabling
 - reports 1454
 - Disk Space Monitor Settings 646
 - Display Columns, Monitor report 1460
 - DNS Monitor 825
 - Dynamo Application Server Monitor Settings 644
- E**
- e-mail
 - integration with 222, 304
 - E-mail alerts
 - working with 1398
 - E-mail Preferences 222
 - e-mail, configuring SiteScope to use 33
 - Enable/Disable alerts
 - working with 1397
 - end of report period, for reports 1454
 - Error log 405

Index

Event Logs

- customizing 154
- displaying 153
- viewing 151
- viewing common event data 156
- working with event details 158
- working with event history 160
- working with reports 153

Exchange 2000/2003 Message Traffic Monitor Settings 662

Exchange 2003 Mailbox Monitor Settings 656

Exchange 2003 Public Folder Monitor Settings 659

Exchange 2007 Monitor Settings 664

Exchange 5.5 Message Traffic Monitor 666

Export to File, Monitor report 1461

F

F5 Big-IP Monitor Settings 648

Failover

- integration with 283

Failover Preferences 219

failure as good, in report uptime readings 1450, 1463

File Format, Monitor report 1461

File Name, Monitor report 1461

filters

- Event Logs 153

format template, for reports 1452

formatting report options 1451, 1465

Formula Composite Monitor 828

FTP Monitor 826

Full and Partial Monitor Coverage 87

G

General Preferences 211

- configuring SiteScope for non-English locale 231
- defining Web Script monitor file directory 213
- enabling configuration files 212
- setting locale data and time settings 231

suspending monitors 212

- viewing UI in a specific language 232, 233

General Settings 256

General Settings, Infrastructure Settings Preferences 256

generate report at property 1456

Get URL and URL Content Tool 1605

Global Search and Replace 343

Override Status Condition 344

threshold settings 344

Global Search and Replace wizard 351

Affected Objects page 359

Choose Changes page 356

Replace Mode page 354

Review Summary page 360

Select SiteScope page 352

Select Subtype page 353

Select Type page 352

Summary page 362

graph of measurements, in reports 1450, 1464

groups 250

configuring SiteScope 462

groups—aster.config 232

H

headerHTML property 1584

Health of SiteScope Server Monitor 400

counters on UNIX 401

counters on Windows 402, 403

HP Business Availability Center

SiteScope integration with 44

HP OVO Event Monitor 1063, 1079

configuration files 1064

configuring Integration Add-on 1069

installing Integration Add-on 1067

log files for Integration Add-on 1074

starting and stopping Integration

Add-on 1072

support in HP OVO cluster 1074

tuning Integration Add-on 1070

uninstalling Integration Add-on 1073

versions supported 1063

HTTPS, accessing primary SiteScope using
284

I

i18N

See Internationalization 211

IIS Server Monitor Settings 651

Infrastructure Settings Manager

changing settings for SiteScope
reports 128

displaying history button 158

Infrastructure Settings Preferences 216, 256,
261, 262, 268, 269, 271, 272, 273

Integration Monitor logs 1059

Integration Monitor troubleshooting 1059

Integration Monitors

field mapping 1161

field mapping, action directive 1182

field mapping, conditional
expressions 1182

field mapping, event handler
structure 1177

field mapping, events 1164, 1173

field mapping, events example 1169,
1176

field mapping, examples 1184

field mapping, matching condition
1178

field mapping, measurements 1170

field mapping, measurements
example 1171

field mapping, string expressions
1182

field mapping, structure 1163

field mapping, tags 1183

list of deprecated 1057

replacing deprecated 1058

working with 1045

interface

customizing SiteScope 1584

Internationalization

SiteScope limitations 211

SiteScope support 211

SiteScope UNIX supported monitors
245

SiteScope user interface 211

SiteScope Windows supported
monitors 244

iPlanet Server Monitor Settings 653

J

JavaScript in URL sequences 975

JBoss Application Server

host monitoring solutions 1291

JBoss Application Server solution template
deploying 1293

L

language preference 214

LDAP Authentication tool 1607

Linux Host solution template

deploying 1301

Linux host, monitoring solution 1299

list of errors, in reports 1450, 1464

list of goods, in reports 1450, 1464

list of warnings, in reports 1450, 1464

localization

matching local date formats 1508

Log Event alerts

working with 1399

Log Event Health Monitor 396

Log files

data columns 383

log files

database table 246

for alerts 405

of monitor data 406

of operator acknowledgments 406

of post requests 405

preferences 221, 301

run monitor 405

setting how much data is stored 33

SiteScope restarts 405

URL monitor details 405

Log Files tab 404

log files, viewing 376

Log Preferences 221, 301

logs

Integration Monitors 1059

M

- Mail Monitor 834
- Mail Round Trip tool 1609
- main settings
 - for Alert reports 1447
 - for Management reports 1449
 - for Monitor reports 1463
 - for Quick reports 1460
- Management Report page 1448
- management reports
 - working with 1443
- MAPI Monitor 830
- match content
 - using regular expressions 1493
- max value on graph, for reports 1454, 1467
- Microsoft Exchange
 - monitoring solution 1305
- Microsoft Exchange solution template
 - deploying 1308
 - settings 1310
- Microsoft IIS
 - host monitoring solutions 1313
- Microsoft IIS solution template
 - deploying 1315
- Microsoft SQL Server
 - host monitoring solutions 1319
- Microsoft SQL Server solution template
 - deploying 1321
- Microsoft Windows Dial-up Monitor 834
- Microsoft Windows Host solution template
 - deploying 1327
- Microsoft Windows Host, monitoring
 - solution 1325
- Microsoft Windows Remote Preferences 219
- Microsoft Windows servers
 - about monitoring remote 219
- Microsoft Windows solution template
 - deploying 1333
- Modify Variables page 1246
- monitor
 - baseline status 511
 - creating using templates 1189
 - disable baseline mode 511
- monitor categories
 - SiteScope 469
- Monitor Deployment wizard
 - categories 96
 - template reference 96
- Monitor Deployment Wizard Concepts and Tasks 81
- Monitor Deployment Wizard Features and Options 85
- Monitor Deployment Wizard for Siebel 89
- Monitor History tab 453
- Monitor Load Monitor 399
- monitor logs 406
- monitor readings, in reports 1450, 1464
- Monitor report
 - example 1477, 1480
- Monitor Report page 1459, 1462
- Monitor Settings 262
- Monitor Settings, Infrastructure Settings
 - Preferences 262
- monitor templates 1189
- monitor tree 526
 - contents tab 170
 - navigating 170
 - view filters 196
- monitor tree user interface 170
- monitor types 469
 - ports used 501, 503
- monitoring
 - configuring user permissions on
 - Windows 2000 242
 - Windows XP,2003 241
 - deployment using templates 1189
 - DHCP 850
 - DNS 825
 - Formula Composite 828
 - FTP 826
 - Mail 834
 - MAPI 830
 - Microsoft Windows Dial-up 834
 - Network Bandwidth 837
 - Ping 838
 - Port 839
 - RTSP 840
 - setting domain privileges 239
 - SiteScope server health 365
 - SNMP 844

- SNMP by MIB 846
- SNMP Trap 845
- monitoring remote servers 471
- monitoring remote UNIX servers 291
 - connection methods 299
 - overview 220
- monitoring remote Windows servers 219
 - limitations and troubleshooting 335
- monitoring using Secure Shell (SSH) 1541
- monitors
 - acknowledging events 195
 - adding to group 489
 - custom properties for 1590
 - disabling based on a schedule 225
 - for .NET 1331
 - for Active Directory 1279
 - for AIX H 1285
 - for JBoss Application Server 1291
 - for Linux host 1299
 - for media files 840
 - for Microsoft Exchange 1305
 - for Microsoft IIS 1313
 - for Microsoft SQL Server 1319
 - for Microsoft Windows Host 1325
 - for Oracle databases 1337
 - for Siebel servers 1353
 - for Solaris host 1363
 - for WebLogic servers 1369
 - for WebSphere servers 1377
 - range schedules for 225, 321
 - schedule to run once 224
 - security, using default authentication
 - credentials 212
 - supported in Windows environments
 - only 501
 - suspending 212
 - troubleshooting skipped 405
- Monitors and Groups to report on
 - Management report 1449, 1463
 - Monitor report 1460
- multi-lingual user interface support 214

N

NET

- host monitoring solutions 1331

- NetScout Event Monitor 1089
 - system requirements 1091
- Network Bandwidth Monitor 837
- Network Node Manager
 - forwarding events from 1157
 - writing scripts to export data 1158
- Network Node Manager Integration
 - about 1157
- Network Tool 1612
- New Alert Report page 1447
- New Management Report page 1448
- New Monitor Report page 1459, 1462
- new SiteScope page
 - System Availability Management
 - administration 65
- New SiteScope Report page 1446
- News Monitor Settings 668
- News Server tool 1613
- NT Performance Counter Test 1614

O

- OpenSSH for Windows, installing 1558
- Operator log 406
- Oracle
 - monitoring solution 1337
- Oracle 10g Application Server Monitor
 - Settings 672
- Oracle 9i Application Server Monitor Settings
 - 670
- Oracle Database solution template
 - deploying 1340
 - settings 1344
 - template tools for 1340
- Overview of the Monitor Deployment
 - Wizard 82
- OVO Event Monitor
 - See HP OVO Event Monitor 1063, 1079

P

- pager
 - connectivity with 309
- Pager alerts
 - working with 1400

Index

- Pager Preferences 222
- password
 - changing 228
 - configuring length, configuring
 - alphanumeric, configuring
 - punctuation 247
 - configuring requirements 247
- permissions
 - SiteScope in System Availability Management 51
- Persistency Settings 269
- Persistency Settings, Infrastructure Settings Preferences 269
- Ping Monitor 838
- Ping tool 1616
- Port Monitor 839
- Post alerts
 - working with 1401
- POST Data Password Key 1034
- POST Data Password Value 1034
- Post log 405
- Preferences
 - Absolute Schedule 224
 - Business Availability Center 216
 - E-mail 222
 - Failover 219
 - General 211
 - Infrastructure Settings 216
 - Log 221
 - Microsoft Windows Remote 219
 - Pager 222
 - Range Schedule 225
 - SNMP Trap 223
 - UNIX Remote 220
 - Users 226
- Prerequisites for Running the Monitor
 - Deployment Wizard 84
- Processes tool 1617
- Publish Results Summary Page 1247
- Publish Template Changes Summary Report 1248
- Publish Template Changes Wizard
 - Content Changes dialog box 1244
 - Modify Variables page 1246
 - Publish Results Summary Page 1247
 - Review Compliancy page 1242
- Select Deployed Groups page 1240
- publishing template changes 1206
 - auto template deployment 1259

R

- Radius Monitor Settings 674
- Range Schedule Preferences 225
- Range Schedules
 - adding 322
- registering SiteScope 216, 234
- Regular Expression tool 1618
- regular expressions 1493
 - character classes 1500
 - defining 1495
 - examples for log files 1511
 - general date variables 1506
 - ignoring character case 1504
 - ignoring line breaks 1504
 - in template monitors 1203
 - language and country specific date variables 1508
 - matching date coded log entries 1515
 - matching delimited log file entries 1513
 - matching numbers in log files 1515
 - matching patterns with
 - metacharacters 1499
 - matching punctuation marks 1500
 - matching string literals 1497
 - metacharacters 1499
 - pitfalls in working with 1516
 - preserving line breaks 1504
 - quantifiers 1502
 - retaining match values 1505
 - search mode modifiers 1503
 - SiteScope date variables 1506
 - special substitution for monitor URL
 - or file path 1509
 - the * quantifier 1502
 - using alternation 1498
- remote Windows server profiles
 - defining 239
- remove warning, from report uptime readings 1449, 1463

- Replace Mode page, Global Search and Replace 354
 - report period, Quick reports 1464
 - Report Settings 272
 - Report Settings, Infrastructure Settings Preferences 272
 - reports
 - access and permissions 114
 - amount of data for 1440
 - color coding 116
 - controlling when reports are generated 1456
 - formatting with templates 1452
 - HTML format option 1452
 - introduction 1439
 - log files used by 406
 - logging data to external database 1440
 - New Alert Report page 1447
 - New Management Report page 1448
 - New Monitor Report page 1459, 1462
 - New SiteScope Report page 1446
 - sending by e-mail 1451, 1465
 - sending XML file by e-mail 1456
 - showing monitor thresholds 1449, 1463
 - SiteScope Cross-Performance 126
 - SiteScope Data over Time 141, 148
 - SiteScope Error Details 146
 - SiteScope Error Summary 146
 - SiteScope Group Performance 139, 148
 - SiteScope Monitor Performance 123, 147
 - SiteScope Over Time 120
 - SiteScope Overall Performance 148
 - SiteScope Performance 139
 - SiteScope Status Summary 143
 - SiteScope Uptime Details 143
 - SiteScope Warning Summary 144
 - System Availability Management 115, 119
 - Review Compliancy page 1242
 - Review Summary page, Global Search and Replace 360
 - RTSP Monitor 840
 - about 840
 - Run Monitor log 405
- ## S
- SAP
 - monitoring solution 1347
 - SAP CCMS Alerts Monitor 585
 - software requirements 585
 - user authorization settings 581, 586
 - SAP CCMS Alerts Monitor Settings 679
 - SAP CCMS monitor
 - Topology Settings 583
 - SAP CCMS Monitor Settings 676
 - SAP Java Web Application Server Monitor Settings 681
 - SAP NetWeaver solution template settings 1351
 - SAP Performance Monitor
 - Java connector installation 590
 - SAP Performance Monitor Settings 683
 - SAP R/3 solution template 1350
 - settings 1351
 - system requirements 1350
 - SAP Work Processes monitor
 - Topology Settings 595
 - SAP Work Processes Monitor Settings 685
 - schedule filter, in reports 1453, 1466
 - script alerts
 - alert message file 1527
 - passing data to 1404
 - passing data to SiteScope 1526
 - troubleshooting 1405
 - working with 1402
 - writing 1524
 - Script Monitor
 - setting a timeout value for script execution 784
 - secure monitoring with SSH 1542
 - security
 - changing user password 228
 - default login account 33
 - user accounts 226, 324
 - using default authentication credentials 212

Index

- Select Deployed Groups page 1240
- Select SiteScope page, Global Search and Replace 352
- Select Subtype page, Global Search and Replace 353
- Select Type page, Global Search and Replace 352
- Server Centric Report
 - how to create 426
- Server Centric report 440
- Server Settings 261
- Server Settings, Infrastructure Settings Preferences 261
- Server-Centric Report
 - generating 416
- Services tool 1625
- Show Page button 1037
- Show Parameters, Monitor report 1460
- Show Source button 1037
- Show which monitors, in reports 1453, 1466
- Siebel
 - monitoring solution 1353
- Siebel Application Server Monitor
 - system requirements 597
- Siebel Application Server monitor
 - Topology Settings 600
- Siebel Application Server Monitor Settings 687
- Siebel Application Server Solution
 - deploying 1356
 - settings 1359
 - system requirements 1357
- Siebel Gateway Server Solution
 - settings 1361
- Siebel Log File Monitor Settings 691
- Siebel Web Server monitor
 - Topology Settings 603
- Siebel Web Server Monitor Settings 695
- Siebel Web Server Solution
 - settings 1362
- SilverStream Server Monitor
 - about 597, 601, 602, 604
- SilverStream Server Monitor Settings 699
- SiteScope
 - accessing administrator account 33 and SSH 1542
 - architecture 30
 - auto template deployment 1253
 - Categories page 203
 - configuration data files 212
 - contents tab 191
 - creating templates 1208
 - customizing display 1582
 - key features 29
 - monitor types 469
 - New Category/Edit Category page 204
 - New View/Edit View page 201
 - scheduling restarts 213
 - SNMP Preferences 316
 - solution templates 1273
 - SSH clients 1563
 - views and categories user interface 200
 - Views page 200
- SiteScope Alert Action wizard 1421
- SiteScope Categories page 203
- SiteScope Cross-Performance report 126
 - generating 128
 - rescaling 136
 - summary tables 135
- SiteScope Dashboard 445
 - accessing SiteScope tools 418
 - Acknowledge dialog box 430
 - acknowledging monitor status 417
 - Add Dashboard Favorite dialog box 432
 - analyze data in SiteScope Dashboard 421
 - concepts and tasks 413
 - customize SiteScope Dashboard 419
 - Dashboard filter overview 415
 - Dashboard Filter page 433
 - Dashboard Layout page 437
 - Delete Dashboard Favorites dialog box 433
 - monitor history tab 453
 - monitor your Windows/UNIX server's resources 424
 - overview 414
 - Server Centric report 440
 - Server-Centric Report 416
- SiteScope Dashboard user interface 430

- SiteScope Data over Time report 141
 - in custom reports 148
- SiteScope E-mail Preferences 304
- SiteScope Error Details report 146
- SiteScope Error Summary report 146
- SiteScope Failover Preferences 283
- SiteScope Group Performance report 139
 - in custom reports 148
 - table 139
- SiteScope groups 462
 - working with 457
- SiteScope Health 365
 - adding monitors 376
 - BAC integration 367
 - BAC Integration Statistics Monitor 395
 - Health of SiteScope Server Monitor 400
 - Log Event Health Monitor 396
 - log events 368
 - monitor group 366
 - monitor load 370
 - Monitor Load Monitor 399
 - server health 370
- SiteScope integration
 - HP Business Availability Center with 44
- SiteScope log database table 246
- SiteScope monitor categories 469
- SiteScope Monitor Performance report 123
 - generating 123
 - in custom reports 147
 - understanding 124
- SiteScope monitoring
 - ports used for 501, 503
 - remote servers 471
- SiteScope monitoring model 31
- SiteScope monitors
 - working with 467
- SiteScope objects
 - context menu options 176
 - monitor tree 170
- SiteScope Over Time graphs
 - consolidated 133
 - non-consolidated 134
- SiteScope Over Time reports 120
- SiteScope Overall Performance report
 - in custom reports 148
- SiteScope overview 28
- SiteScope Pager Preferences 309
- SiteScope Performance report 139
- SiteScope Preferences 207
- SiteScope Range Schedule Preferences 321
- SiteScope reports 440, 1439
 - group filters 153
 - monitor type filters 153
 - profile filters 153
 - showing monitor errors 1450, 1464
 - showing monitor good results 1450, 1464
 - showing monitor readings 1450, 1464
 - showing monitor warnings 1450, 1464
 - showing time in error 1450, 1463
 - working with additional filters 155
- SiteScope restart schedule 213
- SiteScope Status Summary report 143
 - table 143
- SiteScope Uptime Details report 143
- SiteScope User Profiles 324
- SiteScope Views page 200
- SiteScope Warning Details report 145
- SiteScope Warning Summary report 144
 - table 144
- SiteScope-Business Availability Center
 - connection, using SSL 217
- SMS alerts
 - working with 1406
- SNMP
 - configuring SiteScope properties 223
 - integration with 223, 316
- SNMP Browser tool 1620
- SNMP by MIB Monitor 846
- SNMP Monitor 844
- SNMP Preferences 223
- SNMP Recipient Settings 223
- SNMP tool 1623
- SNMP Trap alerts
 - working with 1407
- SNMP Trap Monitor 845
- SNMP trap settings 223, 316
- SNMP Trap tool 1624

Index

- Solaris Host solution template
 - deploying 1365
 - Solaris host, monitoring solution 1363
 - solution templates
 - deploying 1276
 - for Active Directory 1279
 - SAP monitors 1347
 - SiteScope 1273
 - solutions sets
 - for .NET 1331
 - for AIX Host 1285
 - for BEA WebLogic 1369
 - for IBM WebSphere 1377
 - for JBoss Application Server 1291
 - for Linux host 1299
 - for Microsoft Exchange 1305
 - for Microsoft IIS 1313
 - for Microsoft SQL Server 1319
 - for Microsoft Windows Host 1325
 - for Oracle database 1337
 - for Siebel servers 1353
 - for Solaris host 1363
 - Sort By, Monitor report 1460
 - sound alerts
 - working with 1408
 - SSH clients
 - external 1566
 - internal Java 1564
 - using SSH version 2 1566
 - SSH monitoring 1541
 - configuration options 1543
 - configuring UNIX servers for 1546
 - configuring Windows servers for 1545
 - cygwin OpenSSH 1545
 - external SSH client 1566
 - installing and configuring SSH server 1549
 - installing Remote NT SSH files 1560
 - internal Java SSH client 1564
 - key based authentication 1570
 - OpenSSH for Windows 1545
 - password authentication for clients 1565
 - SSH client options 1561
 - using SSH2 1566
 - using SSH2 with internal client 1565, 1569
 - version compatibility 1566
 - working with SSH clients 1563
 - SSL
 - Business Availability Center-SiteScope connection 217
 - SSL, accessing SiteScope using 284
 - Summary page, Global Search and Replace 362
 - SunONE Server Monitor Settings 701
 - suspending monitor processes 212
 - Sync SiteScopes wizard 71
 - System Availability Management
 - permissions model 51
 - System Availability Management
 - administration 57
 - new SiteScope page 65
 - overview 42
 - Sync SiteScopes wizard 71
 - troubleshooting 77
 - System Availability Management reports
 - 113, 115, 119
 - improving report generation times 117
 - in custom reports 147
 - overview 113
 - SiteScope Cross-Performance 126
 - SiteScope Data over Time 141
 - SiteScope Error Summary 146
 - SiteScope Group Performance 139
 - SiteScope Monitor Performance 123
 - SiteScope Performance 139
 - SiteScope Status Summary 143
 - SiteScope Uptime Details 143
 - SiteScope Warning Summary 144
 - working with 116
 - system values
 - accessing in regular expressions 1506
- ## T
- Technology Database Integration Monitor
 - 1097, 1145
 - setup requirements 1099, 1147

- step-by-step integration guide 1102
 - troubleshooting 1114, 1149
 - Technology Log File Integration Monitor 1115
 - setup requirements 1117
 - step-by-step integration guide 1118
 - troubleshooting 1129
 - Technology SNMP Trap Integration Monitor 1131
 - about 1132
 - configuring 1133
 - setup requirements 1133
 - step-by-step integration guide 1134
 - troubleshooting 1142
 - verify SNMP trap reception 1143
 - Technology Web Service Integration Monitor
 - troubleshooting 1156
 - template
 - add regular expression matching 1221
 - auto deployment 1253
 - copying configurations into 1214
 - counter selection examples 1204
 - counter selection using regular expressions 1203
 - creating 1206, 1208
 - examples 1194
 - monitor counter selection in 1202, 1221
 - objects 1193
 - planning 1195
 - publishing changes 1206
 - referencing variables example 1201
 - referencing variables in 1200
 - SERVER_LIST variable 1199
 - system variables 1199
 - to import or export 1222
 - understanding 1192
 - user-defined variables 1198
 - variables 1197
 - template updates
 - Content Changes dialog box 1244
 - Modify Variables page 1246
 - Publish Results Summary Page 1247
 - Publish Template Changes Summary Report 1248
 - Review Compliancy page 1242
 - Select Deployed Groups page 1240
 - templates 1189
 - Export Template page 1238
 - Generate Auto-Deploy XML page 1250
 - Import Template page 1239
 - New Template Alert page 1237
 - New Template Container page 1224
 - New Template Group page 1226
 - New Template Monitor page 1236
 - New Template page 1225
 - New Template Remote page 1229
 - New Template Variable page 1227
 - reserved template groups 1223
 - updating 1206
 - Thresholds property, in reports 1449, 1463
 - Time Between Samples 1454, 1467
 - Time in error, in reports 1450, 1463
 - time period for reports 1451
 - toolsplink.exe 300
 - TraceRoute tool 1626
 - troubleshooting
 - a monitored system 1593
 - Audit log 409
 - database connections 341
 - Integration Monitors 1059
 - monitor configuration 1593
 - System Availability Management administration 77
 - Tuxedo Monitor Settings 703
- ## U
- UDDI Monitor Settings 705
 - UNIX adaptors
 - adaptor command list 1534
 - adaptor file format 1532
 - adding 1530
 - default adaptor file list 1531
 - working with 1530
 - UNIX Remote Preferences 220
 - UNIX servers
 - about monitoring remote 220
 - connection methods 299

Index

- uptime and readings options, in reports
 - 1449, 1463
- URL Content Monitor
 - SSL connectivity 967
- URL details log 405
- URL Monitor
 - security, using default authentication credentials 212
 - SSL connectivity 964, 970
- URL Sequence Monitor
 - beginning a new 994
 - copying HTML source in steps 1037
 - defining the next step 995
 - dynamic content 977
 - limitations on embedded scripts 975
 - SSL connectivity 976
 - viewing steps in a browser 1037
- URL Sequence tool 1627
- user interface
 - multi-lingual support 214
- user preferences 324
- user profiles 226, 324
- user types 227
- Users Preferences 226
 - changing user password 228
- V**
- variables
 - in templates 1197
- View Manager
 - understanding 195
- view settings 195
- views
 - monitor tree 196
- VMware Performance Monitor Settings 706
- W**
- Web Script counter metrics 1041
- Web Script Monitor
 - counters 991
 - measurements 991
 - setting up 986
 - transaction breakdowns 991
 - VuGen scripting 986
 - VuGen supported protocols 988
 - workflow 986
- Web Service monitor
 - Topology Settings 790
- Web Service tool 1630, 1634
- WebLogic
 - monitoring solution 1369
- WebLogic Application Server Monitor
 - Settings 709
- WebLogic solution template
 - deploying 1371
 - selecting modules to monitor 1372
 - settings 1374
 - using 1372
- WebSphere
 - monitoring solution 1377
- WebSphere Application Server Monitor
 - Settings 712
- WebSphere MQ Status Monitor
 - authentication 621
- WebSphere MQ Status Monitor Settings 716
- WebSphere Performance Monitor Settings
 - 718
- WebSphere solution template
 - deploying 1379
 - settings 1380
 - system requirements 1379
- Windows Remote Preferences
 - configuring to monitor on remote server 236
- Windows Resources Monitor
 - about 903
- Windows servers
 - monitoring remote 219, 285
 - perfex for troubleshooting
 - connections 337
 - technical notes on monitoring 335
 - troubleshooting event log access 334

X

- XML documents
 - example match content syntax 1520
 - monitoring as URLs 1520
 - using content match values 1522
- xml template deployment 1253
- XSL Transform tool 1634

