

HP SiteScope

For the Windows, Solaris, and Linux operating systems

Software Version: 11.21

Monitor Reference

Document Release Date: December 2012

Software Release Date: December 2012



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.

Copyright Notice

© Copyright 2005 - 2012 Hewlett-Packard Development Company, L.P.

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.

iPod is a trademark of Apple Computer, Inc.

Java is a registered trademark of Oracle and/or its affiliates.

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

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes software developed by the JDOM Project (<http://www.jdom.org/>).

Documentation Updates

The title page of this document 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>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

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

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

This document was last updated: Monday, November 12, 2012

Support

Visit the HP Software Support Online web site at:

<http://www.hp.com/go/hpsoftwaresupport>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web 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 register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

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

Contents

Monitor Reference	1
Contents	5
Welcome to the SiteScope Monitor Reference	9
SiteScope Monitor Reference Overview	10
Monitor Categories List	14
SiteScope Monitors (A-Z)	19
Active Directory Replication Monitor	20
Amazon Web Services Monitor	24
Apache Server Monitor	30
BroadVision Application Server Monitor	35
Browsable Windows Performance Monitor	40
Check Point Monitor	44
Cisco Works Monitor	47
Citrix Monitor	54
ColdFusion Server Monitor	61
COM+ Server Monitor	67
Composite Monitor	73
CPU Monitor	79
Custom Monitor	86
Custom Database Monitor	98
Custom Log File Monitor	117
Custom WMI Monitor	141
Database Counter Monitor	157
Database Query Monitor	167
DB2 8.x and 9.x Monitor	182
DHCP Monitor	188
Directory Monitor	192

Disk Space Monitor (Deprecated)	198
DNS Monitor	205
Dynamic Disk Space Monitor	210
e-Business Transaction Monitor	223
F5 Big-IP Monitor	228
File Monitor	235
Formula Composite Monitor	241
FTP Monitor	247
Generic Hypervisor Monitor	253
HAProxy Monitor	261
HP iLO (Integrated Lights-Out) Monitor	266
HP NonStop Event Log Monitor	272
HP NonStop Resources Monitor	280
IPMI Monitor	284
KVM Monitor	287
JMX Monitor	296
LDAP Monitor	309
Link Check Monitor	315
Log File Monitor	320
Mail Monitor	334
MAPI Monitor	340
Memcached Statistics Monitor	347
Memory Monitor	351
Microsoft ASP Server Monitor	358
Microsoft Exchange 2007/2010 Monitor	364
Microsoft Exchange 2003 Mailbox Monitor	372
Microsoft Exchange 5.5 Message Traffic Monitor	377
Microsoft Exchange 2000/2003/2007 Message Traffic Monitor	380
Microsoft Exchange 2003 Public Folder Monitor	384
Microsoft Hyper-V Monitor	388
Microsoft IIS Server Monitor	394
Microsoft Lync Server 2010 Monitors	401

Microsoft SQL Server Monitor	411
Microsoft Windows Dial-up Monitor	418
Microsoft Windows Event Log Monitor	423
Microsoft Windows Media Player Monitor	434
Microsoft Windows Media Server Monitor	439
Microsoft Windows Performance Counter Monitor	445
Microsoft Windows Resources Monitor	452
Microsoft Windows Services State Monitor	461
Network Bandwidth Monitor	467
News Monitor	474
Oracle 10g Application Server Monitor	478
Oracle 9i Application Server Monitor	483
Oracle Database Monitor	487
Ping Monitor	495
Port Monitor	500
Radius Monitor	505
Real Media Player Monitor	510
Real Media Server Monitor	514
SAP CCMS Monitor	520
SAP CCMS Alerts Monitor	530
SAP Java Web Application Server Monitor	537
SAP Performance Monitor	543
SAP Work Processes Monitor	549
Script Monitor	556
Service Monitor	567
Siebel Application Server Monitor	574
Siebel Log File Monitor	583
Siebel Web Server Monitor	589
SNMP Monitor	596
SNMP by MIB Monitor	604
SNMP Trap Monitor	611
Solaris Zones Monitor	617

SunONE Web Server Monitor	625
Sybase Monitor	631
Syslog Monitor	636
Tuxedo Monitor	645
UDDI Monitor	650
UNIX Resources Monitor	653
URL Monitor	659
URL Content Monitor	673
URL List Monitor	686
URL Sequence Monitor	695
VMware Datastore Monitor	718
VMware Host Monitors	732
VMware Performance Monitor	753
Web Script Monitor	771
Web Server Monitor	784
Web Service Monitor	789
WebLogic Application Server Monitor	798
WebSphere Application Server Monitor	805
WebSphere MQ Status Monitor	828
WebSphere Performance Servlet Monitor	836
XML Metrics Monitor	842
Integration Monitors (A-Z)	848
HP OM Event Monitor	849
HP Service Manager Monitor	861
NetScout Event Monitor	869
Technology Database Integration Monitor	874
Technology Log File Integration Monitor	889
Technology SNMP Trap Integration Monitor	903
Technology Web Service Integration Monitor	915

Welcome to the SiteScope Monitor Reference

This guide describes how to set up the monitoring environment and configure SiteScope and integration monitors to monitor the enterprise IT infrastructure. It contains information for configuring the specific monitor only. For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

How This Guide Is Organized

This guide covers the following topics:

- ["SiteScope Monitors \(A-Z\)" on page 19](#)

Describes how to set up the monitoring environment and configure each type of SiteScope monitor. It includes information on supported versions, setup requirements, user permissions, and troubleshooting issues.

- ["Integration Monitors \(A-Z\)" on page 848](#)

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

Note: For details on setting panels in the monitor Properties tab that are common to all monitors, see Common Monitor Settings in Using SiteScope.

Who Should Read This Guide

This guide is intended for the following users of HP SiteScope and HP Business Service Management (BSM):

- SiteScope/BSM administrators
- SiteScope/BSM application administrators
- SiteScope/BSM data collector administrators
- SiteScope/BSM 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 BSM should be familiar with BSM and enterprise monitoring and management concepts.

SiteScope Monitor Reference Overview

SiteScope monitors 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.

Monitor Categories

This section describes the monitor classes and the category listing formats.

This section contains the following topics:

- ["Standard Monitors" below](#)
- ["Customizable Monitors" on the next page](#)
- ["Integration Monitors" on the next page](#)
- ["Solution Template Monitors" on the next page](#)

To see the list of monitors contained in each monitor category, see [Monitor Categories List](#).

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.

- **Application Monitors.** Monitors in this category monitor third-party applications. These monitors enable SiteScope to access and retrieve data from the monitored applications.
- **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.
- **Generic Monitors.** Monitors in this category monitor different types of environment. These monitors can monitor networks, applications, and databases depending on how they are configured.
- **Media Monitors.** Monitors in this category monitor applications that play media files and stream data.
- **Network Monitors.** Monitors in this category monitor network health and availability.
- **Server Monitors.** Monitors in this category monitor server health and availability.
- **Virtualization and Cloud Monitors.** Monitors in this category monitor virtualized environments and cloud infrastructures.
- **Web Transaction Monitors.** Monitors in this category monitor web-based applications.

Customizable Monitors

Custom monitors broaden the capabilities of regular SiteScope monitors for tracking the availability and performance of your infrastructure systems and applications. Using custom monitors, you can develop your own solutions for environments that are not supported by predefined SiteScope monitors.

You can create your own monitor that collects data, and define a script that processes the collected data and creates metrics. Each time the custom monitor runs, it updates the metrics and returns a status for the metrics defined in the script.

Custom monitors can be published to the HP Live Network for sharing with other SiteScope users. For more details on using Custom monitors, see [Using Custom Monitors](#).

Integration Monitors

This group of optional monitor types are used to integrate HP products with other commonly used Enterprise Management systems and applications.

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 [Integration Monitors](#).

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. After they have been deployed, you can edit or delete them using the same steps as with other monitor types. For more information, see [Solution Templates](#).

The monitor types using solution templates include:

- Active Directory (with and without Global Catalog)
- HP Service Manager
- Microsoft Exchange
- Microsoft IIS Server
- Microsoft Lync Server
- Microsoft SQL Server
- Microsoft Windows Resources
- Oracle Database
- SAP Application Server
- Siebel Application/Gateway/Web Server (for UNIX and Windows)
- UNIX Resources
- VMware Host CPU/Memory/Network/State/Storage

Monitor Reference

SiteScope Monitor Reference Overview

- WebLogic Application Server
- WebSphere Application Server

Monitor Categories List

This section displays the SiteScope monitors in each monitor category.

- "Application Monitors" below
- "Customizable Monitors" on the next page
- "Database Monitors" on the next page
- "Generic Monitors" on page 16
- "Integration Monitors" on page 16
- "Media Monitors" on page 16
- "Network Monitors" on page 16
- "Server Monitors" on page 17
- "Virtualization and Cloud Monitors" on page 17
- "Web Transaction Monitors" on page 18

Application Monitors

- "Active Directory Replication Monitor" on page 20
- "Apache Server Monitor" on page 30
- "BroadVision Application Server Monitor" on page 35
- "Check Point Monitor" on page 44
- "Cisco Works Monitor" on page 47
- "Citrix Monitor" on page 54
- "ColdFusion Server Monitor" on page 61
- "COM+ Server Monitor" on page 67
- "F5 Big-IP Monitor" on page 228
- "HAProxy Monitor" on page 261
- "Memcached Statistics Monitor" on page 347
- "Microsoft ASP Server Monitor" on page 358
- "Microsoft Exchange 2007/2010 Monitor" on page 364
- "Microsoft Exchange 2003 Mailbox Monitor" on page 372
- "Microsoft Exchange 5.5 Message Traffic Monitor" on page 377
- "Microsoft Exchange 2000/2003/2007 Message Traffic Monitor" on page 380

Monitor Reference

Monitor Categories List

- "Microsoft Exchange 2003 Public Folder Monitor" on page 384
- "Microsoft IIS Server Monitor" on page 394
- "News Monitor" on page 474
- "Oracle 9i Application Server Monitor" on page 483
- "Oracle 10g Application Server Monitor" on page 478
- "Radius Monitor" on page 505
- "SAP CCMS Monitor" on page 520
- "SAP CCMS Alerts Monitor" on page 530
- "SAP Java Web Application Server Monitor" on page 537
- "SAP Performance Monitor" on page 543
- "SAP Work Processes Monitor" on page 549
- "Siebel Application Server Monitor" on page 574
- "Siebel Log File Monitor" on page 583
- "Siebel Web Server Monitor" on page 589
- "SunONE Web Server Monitor" on page 625
- "Tuxedo Monitor" on page 645
- "UDDI Monitor" on page 650
- "WebLogic Application Server Monitor" on page 798
- "WebSphere Application Server Monitor" on page 805
- "WebSphere MQ Status Monitor" on page 828
- "WebSphere Performance Servlet Monitor" on page 836

Customizable Monitors

- "Custom Monitor" on page 86
- "Custom Database Monitor" on page 98
- "Custom Log File Monitor" on page 117
- "Custom WMI Monitor" on page 141

Database Monitors

- "DB2 8.x and 9.x Monitor" on page 182
- "Database Counter Monitor" on page 157
- "Database Query Monitor" on page 167
- "LDAP Monitor" on page 309
- "Microsoft SQL Server Monitor" on page 411

- "Oracle Database Monitor" on page 487
- "Sybase Monitor" on page 631

Generic Monitors

- "Composite Monitor" on page 73
- "Directory Monitor" on page 192
- "File Monitor" on page 235
- "JMX Monitor" on page 296
- "Log File Monitor" on page 320
- "Script Monitor" on page 556
- "Sybase Monitor" on page 631
- "Web Service Monitor" on page 789
- "XML Metrics Monitor" on page 842

Integration Monitors

- "HP OM Event Monitor" on page 849
- "HP Service Manager Monitor" on page 861
- "NetScout Event Monitor" on page 869
- "Technology Database Integration Monitor" on page 874
- "Technology Log File Integration Monitor" on page 889
- "Technology SNMP Trap Integration Monitor" on page 903
- "Technology Web Service Integration Monitor" on page 915

Media Monitors

- "Microsoft Lync Server 2010 Monitors" on page 401 (Microsoft A/V Conferencing Server, Microsoft Archiving Server, Microsoft Director Server, Microsoft Edge Server, Microsoft Front End Server, Microsoft Mediation Server, Microsoft Monitoring and CDR Server, and Microsoft Registrar Server)
- "Microsoft Windows Media Player Monitor" on page 434
- "Microsoft Windows Media Server Monitor" on page 439
- "Real Media Player Monitor" on page 510
- "Real Media Server Monitor" on page 514

Network Monitors

- "DHCP Monitor" on page 188
- "DNS Monitor" on page 205
- "FTP Monitor" on page 247

- "Formula Composite Monitor" on page 241
- "Mail Monitor" on page 334
- "MAPI Monitor" on page 340
- "Microsoft Windows Dial-up Monitor" on page 418
- "Network Bandwidth Monitor" on page 467
- "Ping Monitor" on page 495
- "Port Monitor" on page 500
- "SNMP Monitor" on page 596
- "SNMP Trap Monitor" on page 611
- "SNMP by MIB Monitor" on page 604

Server Monitors

- "Browsable Windows Performance Monitor" on page 40
- "CPU Monitor" on page 79
- "Disk Space Monitor (Deprecated)" on page 198
- "Dynamic Disk Space Monitor" on page 210
- "HP iLO (Integrated Lights-Out) Monitor" on page 266
- "HP NonStop Event Log Monitor" on page 272
- "HP NonStop Resources Monitor" on page 280
- "IPMI Monitor" on page 284
- "Memory Monitor" on page 351
- "Microsoft Windows Event Log Monitor" on page 423
- "Microsoft Windows Performance Counter Monitor" on page 445
- "Microsoft Windows Resources Monitor" on page 452
- "Microsoft Windows Services State Monitor" on page 461
- "Service Monitor" on page 567
- "UNIX Resources Monitor" on page 653
- "Web Server Monitor" on page 784

Virtualization and Cloud Monitors

- "Amazon Web Services Monitor" on page 24
- "Generic Hypervisor Monitor" on page 253
- "KVM Monitor" on page 287
- "Microsoft Hyper-V Monitor" on page 388

Monitor Reference

Monitor Categories List

- "Solaris Zones Monitor" on page 617
- "VMware Host Monitors" on page 732 (VMware Host CPU, VMware Host Memory, VMware Host Network, VMware Host State, and VMware Host Storage)
- "VMware Performance Monitor" on page 753

Web Transaction Monitors

- "e-Business Transaction Monitor" on page 223
- "Link Check Monitor" on page 315
- "URL Monitor" on page 659
- "URL Content Monitor" on page 673
- "URL List Monitor" on page 686
- "URL Sequence Monitor" on page 695
- "Web Script Monitor" on page 771

Part 1

SiteScope Monitors (A-Z)

Chapter 1

Active Directory Replication Monitor

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.

Note:

- The Active Directory Replication monitor is an optional SiteScope monitor that requires additional licensing to enable it 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 in the Using SiteScope Guide.

To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click the **Active Directory** solution template that you require, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

Learn More

This section includes:

- ["Active Directory Replication Monitor Overview" below](#)
- ["Supported Versions" below](#)

Active Directory Replication Monitor Overview

The Active Directory Replication monitor enables 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. The error and warning thresholds for the monitor can be set on each of the monitored Domain Controllers.

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 calculated.

Supported Versions

This monitor supports monitoring remote servers running on Windows Server 2000, 2003, 2008, and 2008 R2.

Tasks

How to Configure the Active Directory Replication Monitor

1. Prerequisites

- The VMware Datastore monitor requires additional licensing to enable the monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- The **LDAP Authentication Tool** is available when configuring this monitor to authenticate a user on an LDAP server (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Link Check Tool in the Using SiteScope Guide.

2. Deploy the Active Directory Solution template

This monitor can only be added by deploying an Active Directory Solution template. For information about using templates to deploy monitors, see SiteScope Templates in the Using SiteScope Guide.

3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors.

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

"How to Deploy a Monitor" in the Using SiteScope Guide

UI Descriptions

Active Directory Replication Monitor Settings

User interface elements are described below:

UI Element	Description
Domain controller	Domain controller that contains the replicated data.
Replicating domain controllers	Comma separated list of domain controllers that replicate data from the domain controller entered above.
User name	<p>User name or the entire Security Principal of a Domain Admin account.</p> <p>If a user name is given, the default security principal is created from the root context of the Domain Controller.</p> <p>Example: If you enter <code>Administrator</code> for a domain controller in the domain <code>yourcompany.com</code>, then the entire Security Principal would be <code>CN=Administrator, CN=Users, DC=yourcompany, DC=com</code>.</p>
Password	Password for the Domain Admin account.
Maximum replication time (seconds)	<p>Maximum amount of time for replication to occur. The monitor goes into error if any of the Replicating Domain Controllers exceed this replication time.</p> <p>Default value: 600 seconds</p>
Polling interval (seconds)	<p>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.</p> <p>Default value: 10 seconds</p>
Directory path	<p>Path to a directory in the Active Directory that you want to monitor. This is in the form of an LDAP query.</p> <p>Default value: Based on the default Directory for this server. For example, the default for a Domain Controller for <code>sub.yourcompany.com</code> is <code>DC=sub, DC=yourcompany, DC=com</code>.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 2

Amazon Web Services Monitor

The Amazon Web Services monitor enables monitoring of Amazon Web Services (AWS) cloud resources.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Amazon Web Services monitor.

Learn More

Amazon Web Services Monitor Overview

The Amazon Web Services monitor enables monitoring of Amazon Web Services (AWS) cloud resources, starting with Amazon Elastic Compute Cloud service (EC2). It provides data on resource utilization, operational performance, and overall network demand patterns.

Data collected from AWS-hosted applications can also be reported to Amazon CloudWatch using the Amazon CloudWatch integration. This data can then be used for AWS AutoScaling, reporting and alerting. For details on enabling the Amazon CloudWatch integration, see Amazon CloudWatch Integration Preferences.

The Amazon Web Services monitor enables monitoring of Amazon Web service cloud resources, starting with Amazon Elastic Compute Cloud service (EC2). It provides data on resource utilization, operational performance, and overall network demand patterns.

Tasks

How to Configure the Amazon Web Services Monitor

1. Prerequisites

The Amazon CloudWatch Service is required to monitor Amazon Web Services.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Amazon Web Services Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
AWS Access Key ID	An alphanumeric token that uniquely identifies a request sender. This ID is associated with your AWS Secret Access Key.
AWS Secret Key	The key assigned to you by AWS when you sign up for an AWS account. Used for request authentication.
Socket timeout (milliseconds)	Amount of time, in milliseconds, to wait for data from a server during a single data request. After the socket timeout period elapses, the monitor logs an error and reports the error status. A value of zero means there is no timeout used. Default value: 120 milliseconds
Region	The Amazon EC2 region that is used to get or store measurements. Default value: US East (Northern Virginia) Note: When configuring the monitor in template mode, enter the Amazon region ID in the Region ID box as follows: <ul style="list-style-type: none"> • us-east-1 for US East (Northern Virginia) • us-west-2 for US West (Oregon) • us-west-1 for US West (Northern California) • eu-west-1 for EU (Ireland) • ap-southeast-1 for Asia Pacific (Singapore) • ap-northeast-1 for Asia Pacific (Tokyo) • sa-east-1 for South America (Sao Paulo) • us-gov-west-1 for AWS GovCloud
Get Regions	Opens the Get Regions dialog box, enabling you to select the Amazon EC2 region that is used to get or store measurements. Amazon EC2 is currently available in the following regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), South America (Sao Paulo), and AWS GovCloud. Note: This button is not available when configuring the monitor in template mode; you must manually enter the region ID using one of the IDs listed in Region above.

UI Element	Description
Counter Settings	
Counters	Server performance counters to check with this monitor. The list displays the available counters and those currently selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor.
Proxy Settings	
NTLM V2 Proxy	Select if the proxy requires authentication using NTLM version 2.
Address	Domain name and port of an HTTP Proxy Server if a proxy server can be used to access the AWS cloud resources to be monitored.
User name	Proxy server user name if required to access the AWS cloud resources. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Password	Proxy server password if required to access the AWS cloud resources. Note: Your proxy server must support Proxy-Authentication for these options to function.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

- The Amazon Web Services Monitor only gets data from instances that have detailed monitoring enabled in the AWS Management Console (it does not get data from instances with basic monitoring enabled).
- Amazon does not store data sent from SiteScope via the Amazon integration or from Amazon instances for more than two weeks (old data is automatically removed). As a result, the Amazon Web Services monitor does not return data older than two weeks.
- By default, SiteScope gets data from AWS-hosted applications at a 2-minutes interval. You can customize the period for receiving data from Amazon by adding the `_amazonCloudWebServiceMonitorPeriod` property (and a value in minutes) to the `<SiteScope root directory>\groups\master.config` file. For example, `_amazonCloudWebServiceMonitorPeriod=10` means that SiteScope gets the average values of metrics for the last 10 minutes.

Chapter 3

Apache Server Monitor

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 enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Apache server you are running.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Apache Server monitor.

Learn More

Supported Platforms/Versions

This monitor supports monitoring remote servers running on Apache 1.3.9, 1.3.12, 2.0 and 2.2 servers.

Tasks

How to Configure the Apache Server Monitor

1. Prerequisites

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.
- Know the user name and password for accessing the counters of the Apache server you want to monitor, if required.
- If using a proxy server to access the server, get the domain name and port of an HTTP Proxy Server from your network administrator.
- 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.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Apache Server Monitor Settings

User interface elements are described below:

UI Element	Description
Server Settings	
Administration URL	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> .
Operating System	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
Counter Settings	
Counters	Server performance counters to check with this monitor. The list displays the available counters and those currently selected for this monitor.
Connection Settings	
Authorization user name	User name if the server you want to monitor requires a name and password for access.
Authorization password	Password if the server you want to monitor requires a name and password for access.
HTTP Proxy	Domain name and port of an HTTP Proxy Server if required by the proxy server is to access the server.
Proxy user name	Proxy server user name if required to access the server. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Proxy password	Proxy server password if required to access the server. Note: your proxy server must support Proxy-Authenticate for these options to function.
Timeout (seconds)	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. Default value: 60 seconds

For information on configuring setting panels that are common to all monitors, see Common

Monitor Settings in the Using SiteScope Guide.

Chapter 4

BroadVision Application Server Monitor

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 enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each BroadVision server in your environment. The error and warning thresholds for the monitor can be set on one or more BroadVision server performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the BroadVision Application monitor.

Learn More

Supported Versions

This monitor supports monitoring remote servers running on BroadVision 4.1, 5.x, and 6.0 servers.

Tasks

How to Configure the BroadVision Application Server Monitor

1. Prerequisites

- 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.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

BroadVision Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Server	BroadVision root server name of the BroadVision server you want to monitor. For example, 199.123.45.678.
Port	ORB port number to the BroadVision server you want to monitor. Example: 1221
Counter Settings	
Counters	Server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 5

Browsable Windows Performance Monitor

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.

To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click the required Microsoft Exchange Solution Template, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

Tasks

How to Configure the Browsable Windows Performance Counter monitor

1. Prerequisites

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.

2. Deploy the monitor using the Microsoft Exchange Solution Template

This monitor can be added only by deploying a Microsoft Exchange Solution Template. For information about using templates to deploy monitors, see Solution Templates Overview in the Using SiteScope Guide.

3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors.

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Browsable Windows Performance Counter Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the performance counters you want to monitor are found.</p> <p>Note: After deployment, you can use the drop-down list to select a server from the list of Microsoft Windows remote servers that are available to SiteScope.</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p>
Counter file	<p>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.</p> <p>The files in this list all reside in the <SiteScope root directory>\templates.perfmon\browsable directory under SiteScope. There are a number of default files in the standard SiteScope distribution.</p>
Counters	<p>Server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p> <p>Note when working in template mode: To update counters in template browsable monitors that need a target server, click the Select measurement from button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.</p>
Get Counters	<p>Opens the Select Counters dialog box, enabling you to select the counters you want to monitor.</p> <p>Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 6

Check Point Monitor

Use the Check Point monitor to monitor the content of event logs and other data from Check Point Firewall-1 4.1 NG servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate Check Point monitor instance for each Check Point Firewall-1 server in your environment. The error and warning thresholds for the monitor can be set on one or more firewall statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Check Point monitor.

Tasks

How to Configure the Check Point monitor

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Check Point Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Index	Index of the SNMP object you want to check with this monitor. Non-table object IDs have an index of 0 (zero). Default value: 0
Community	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	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 (161), enter the port number as part of the server address.
Retry delay (seconds)	Number of seconds that the monitor should wait for a response from the server before retrying the request. Default value: 1 second
Timeout (seconds)	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. Default value: 5 seconds
Counter Settings	
<List of counters>	Displays the available server performance counters and those currently selected for this monitor.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 7

Cisco Works Monitor

Use the Cisco Works monitor to monitor the content of event logs and other data from Cisco Works 2000 servers. You can monitor multiple parameters or counters with a single monitor instance. This enables 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. The error and warning thresholds for the monitor can be set on one or more Cisco Works server statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Cisco Works monitor.

Learn More

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Cisco Works Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **SNMP Browser Tool** is available when configuring this monitor to verify the connection properties of an SNMP agent and to gain more information about the MIBs which that agent implements (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Browser Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Cisco Works Monitor Settings

User interface elements are described below:

UI Element	Description
SNMP Settings	
Server	Name of the server you want to monitor.
Port	Port to use when requesting data from the SNMP agent. Default value: 161
MIB file	MIB file display option. <ul style="list-style-type: none">• CISCOWORKS-MIB file causes only those objects that are described within that MIB file to be displayed.• 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. Default value: All MIBs
Counter calculation mode	Performs a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are: <ul style="list-style-type: none">• Calculate delta. Calculates a simple delta of the current value from the previous value.• Calculate rate. Calculates a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements.• Do not calculate. No calculation is performed. 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.

UI Element	Description
Starting OID	<p>Use 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 here.</p> <p>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 enter a different value.</p> <p>Default value: 1</p> <p>Note: This field is available in template mode only.</p>
SNMP Connection Settings	
Timeout (seconds)	<p>Amount of time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.</p> <p>Default value: 5</p>
Number of retries	<p>Number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.</p> <p>Default value: 1</p>
Community	<p>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.</p> <p>Default value: public</p>
SNMP version	<p>Version of SNMP to use when connecting. Supports SNMP version 1, 2, and 3. Selecting V3 enables you to enter V3 settings in the SNMP V3 setting fields below.</p> <p>Default value: V1</p>
Authentication algorithm	<p>Authentication algorithm to use for version 3 connections.</p> <p>Default value: MD5</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
User name	<p>User name for version 3 connections.</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
Password	<p>Authentication password to use for version 3 connections.</p> <p>Note: This field is available only if SNMP V3 is selected.</p>

UI Element	Description
Privacy algorithm	The privacy algorithm used for authentication for SNMP version 3 (DES, 128-Bit AES, 192-Bit AES, 256-Bit AES). Default value: DES Note: This field is available only if SNMP V3 is selected.
Privacy password	Privacy password for version 3 connections. Leave blank if you do not want privacy. Note: This field is available only if SNMP V3 is selected.
Context name	Context Name to use for this connection. This is applicable for SNMP V3 only. Note: This field is available only if SNMP V3 is selected.
Context engine ID	Hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only. Note: This field is available only if SNMP V3 is selected.
SNMP Counters	
Counters	Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note: <ul style="list-style-type: none"> The counters displayed are those received during the timeout period, and may not include all the counters available on the server. Specifying a longer timeout in the Timeout (seconds) field in the SNMP Connection Settings panel may result in receiving more counters. The total time for receiving the counters may be longer than the timeout specified, due to additional processing time not part of the request/response period. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 8

Citrix Monitor

Use the Citrix monitor to monitor the server performance statistics from Citrix servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning.

Create a separate Citrix monitor instance for each Citrix server in your environment. The error and warning thresholds for the monitor can be set on one or more Citrix server performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Citrix monitor.

Learn More

This section includes:

- "What to Monitor" below
- "Supported Versions/Platforms" below
- "IPv6 Addressing Supported Protocols" below

What to Monitor

The Citrix monitor makes use of performance objects and counters to measure application server performance. The Citrix 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) (<http://support.citrix.com/article/CTX106319>), and about the Terminal Services Session Object at <http://msdn.microsoft.com/en-us/library/ms804500.aspx>.

Supported Versions/Platforms

This monitor supports monitoring remote servers running on:

- Citrix MetaFrame 1.8 Service Pack 3
- Citrix MetaFrame XP(s,a,e) Feature Release 1/Service Pack 1
- Citrix MetaFrame XP(s,a,e) Feature Release 2/Service Pack 2
- Citrix Presentation Server 3.5, 4.x
- Citrix XenApp 4.6, 5.0, 6.0
- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Citrix Monitor

1. Prerequisites

The following are important requirements for using the Citrix monitor:

- SiteScopes running on Windows platforms need 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 Servers option in the remote server view. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.
- The Remote Registry service must be running on the machine where the Citrix 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 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 Monitor to Run on Windows 2003 as a Non-Administrator User](#)" on page 454 in the Using SiteScope Guide.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Citrix Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the Citrix server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none">• Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.• When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none">• Browse servers. Select a server from the drop-down list of servers visible in the local domain.• Enter server name. If the server you want to monitor does not appear in the Serverslist because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Counters	<p>The server performance counters selected for 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).</p> <p>Note when working in template mode: To update counters in template browsable monitors that need a target server, click the Select measurement from button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 9

ColdFusion Server Monitor

Use the ColdFusion Server monitor to monitor the server performance statistics from ColdFusion 4.5.x and 9 servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate ColdFusion Server monitor instance for each ColdFusion server in your environment. The error and warning thresholds for the monitor can be set on one or more ColdFusion server performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the ColdFusion Server monitor.

Learn More

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the ColdFusion Server Monitor

1. Prerequisites

- SiteScopes running on Windows platforms need 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 Servers option in the remote server view. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.
- If ColdFusion is running on Windows 2000, the Remote Registry service must be running on the machine where the ColdFusion server is running.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

ColdFusion Server Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the ColdFusion Server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Counters	Server performance counters selected for this monitor. Use the Get Counters button to select counters. Note when working in template mode: To update counters in template browsable monitors that need a target server, click the Select measurement from button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 10

COM+ Server Monitor

Use the COM+ Server monitor to monitor the performance of COM+ software components registered and running on Microsoft Windows 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 monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. Contact your HP sales representative for more information.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the COM+ monitor.

Learn More

Supported Versions

This monitor supports monitoring COM+ software components running on Microsoft Windows Server 2000, 2003, 2008, and 2008 R2 servers.

Tasks

How to Configure the COM+ Monitor

1. Prerequisites

- An Option license for the COM+ Server monitor must be obtained and input into SiteScope. Contact your HP sales representative for more information.
- There must be HTTP connectivity between the SiteScope server and the server running the COM+ probe.

2. Install the COM+ probe

A COM+ probe component must be installed and running on the target COM+ server you want to monitor.

- Go to the [HP Software Support](http://www.hp.com/go/hpssoftwaresupport) site (<http://www.hp.com/go/hpssoftwaresupport>) and click the **Downloads** tab. Then click **Software patches**, and enter your HP user name and password to access the Software Patches page.
- In the **Product** section, select **SiteScope**.
- In the optional search box, enter **COM+** and click **Search**.
- Download the COM+ probe from the results.
- After downloading, follow the instructions for installing the probe on the COM+ server to be monitored.

Note: You cannot have multiple SiteScope instances share one probe instance. You can have multiple COM+ Server 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.

3. Start the COM+ probe

After successfully installing the probe, you must start it prior to running or defining a COM+ Server 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**.

4. Configure the monitor properties

Create a COM+ Server monitor, and specify the COM+ probe for the target COM+ server. The COM+ probe is queried for a list of available functions to monitor, and a browse tree is displayed. Select the COM+ functions or counters that you want to measure.

Configure the other COM+ Server monitor fields as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

COM+ Monitor Settings

User interface elements are described below:

UI Element	Description
COM+ probe host name	Host name of the COM+ probe.
COM+ probe port number	Port number of the COM+ probe. Default value: 8008
Credentials	Option for providing the user name and password authorization to the COM+ probe: <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
HTTP proxy	Domain name and port of an HTTP proxy server if a proxy server is used to access the probe.
Proxy server user name	Proxy user name if the proxy server requires a name and password to access the probe. Your proxy server must support Proxy-Authenticate for these options to function.
Proxy server password	Proxy password if the proxy server requires a name and password to access the probe.
Timeout (seconds)	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. Default value: 60 seconds 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.

UI Element	Description
Counters	Server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 11

Composite Monitor

This monitor enables you to monitor complex network environments by checking the status readings of a set of other SiteScope monitors, groups, or both. Each time the Composite monitor runs, it returns a status based on the number and percentage of items in the specified monitors, groups, or both, currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Composite monitor.

Learn More

What to Monitor

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 permit, you can use the Composite monitor to create customized alert behavior.

Tasks

How to Configure the Composite Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Composite Monitor Settings

User interface elements are described below:

UI Element	Description
Items	<p>Click the Add  button to open the Add Items dialog box, and select the groups, monitors, or both, that you want in the Composite monitor. For details on the Add Items dialog box, see "Add Items Dialog Box" on the next page. The Add Items dialog box displays all the monitors that are part of the same SiteScope.</p> <p>To remove items from the list, select the groups, monitors, or both, you want to remove (you can select multiple items using the CTRL or SHIFT keys), and click the Delete  button.</p> <p>Note when working in template mode:</p> <ul style="list-style-type: none"> • The monitors that you add to the Composite monitor are placeholders. They become real monitors when you deploy the Composite monitor. • If you add the Composite monitor to a template, group, or subgroup, when you click the Add Items button, the Add Items dialog box displays only the monitors that are part of the same template as the new Composite monitor.
Run monitors	<p>The Composite monitor controls 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 Frequency 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> <p>Default value: Not selected</p>
Monitor delay (seconds)	<p>Amount of time, in seconds, to wait between running each monitor (if Run monitors is selected).</p> <p>This setting is useful if you need to wait for processing to occur on your systems before running the next monitor.</p> <p>Default value: 0 seconds</p>
Check all monitors in group (s)	<p>All monitors in the selected groups (and their subgroups) are checked and counted.</p> <p>Default value: Not selected (each group is checked and counted as a single item when checking status readings).</p>

Add Items Dialog Box

This dialog box enables you to select the monitors, groups, or both, that you want in the Composite monitor.

User interface elements are described below:

UI Element	Description
Add Selected Items	Click to add the selected groups, monitors, or both, to the Composite monitor.
 SiteScope	Represents the SiteScope root directory.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors). If a group alert has been set up for the monitor group or subgroup, the alert  symbol is displayed next to the group icon.
	Represents a SiteScope monitor (enabled/disabled). If an alert has been set up for the monitor, the alert  symbol is displayed next to the monitor icon.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

- When using this monitor to monitor a URL monitor in which at least one of the steps uses a session cookie to send to the server instead of logging in each time, the Composite monitor saves the context including the cookie. This means that the login information does not need to be entered again, as the login credentials are sent in a cookie.
- This monitor cannot be copied to a template. It must be created directly in a template.

Chapter 12

CPU Monitor

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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the CPU monitor.

Learn More

This section includes:

- "Supported Platforms/Versions" below
- "Status" below
- "IPv6 Addressing Supported Protocols" below
- "Scheduling the Monitor" on the next page

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

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 Windows, 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.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Scheduling the 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.

Tasks

How to Configure the CPU Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Performance Counters Tool** is available when configuring this monitor to check performance counters on a specific machine in a Windows network (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Performance Counters Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

CPU Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the CPU you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none">• Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.• When configuring this monitor on SiteScopes running on UNIX versions, only remote servers that have been configured with an SSH connection method are displayed.• When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none">• Browse servers. Select a server from the drop-down list of servers in the local domain.• Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

Monitor Specific Tips/Limitations

- Unable to monitor CPU usage on a clean installation of Red Hat Linux 4.

Cause: The `mpstat` command that SiteScope runs on the monitored server as depicted in **<SiteScope root directory>\Templates.os** folder (`/usr/bin/mpstat`), is not deployed by default on a Linux machine. Linux installations come with a `sysstat` package.

Solution: In a terminal window, type `up2date sysstat` to deploy the `mpstat` package.

- Getting invalid CPU value error message in **<SiteScope root directory>\logs\RunMonitor.log** file when using `perfmon` monitors on VMware host servers.

Solution: Use the VMWare Performance monitor to measure CPU on VMWare host servers.

Chapter 13

Custom Monitor

The Custom monitor broadens the capabilities of regular SiteScope monitors for tracking the availability and performance of monitored environments. The Custom monitor enables you to create your own monitor by developing a script that collects data from an application or a remote machine using custom Java or JavaScript code. The script then processes the data and creates metrics in names determined by you. You can use Java code developed by yourself or by a third-party to process the data.

You can share custom monitors by publishing them to the HP Live Network community, enabling other SiteScope users to import the monitor template for their own use.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **Custom** monitor.

Learn More

Custom Monitor Overview

The Custom monitor enables you to develop your own monitor on top of the SiteScope infrastructure.

Custom monitors enable you to do the following:

- **Create monitors that provide additional metrics not available in existing monitors, and then process the collected data**

You can create your own monitor by developing a script that collects data using custom Java or JavaScript code, and then processes the data and creates metrics. Each time the Custom monitor runs, it updates the metrics and returns a status for the metrics defined in the script.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**).

- **Customize how results are displayed**

You can determine how results are displayed. For example, whether result data is displayed in megabytes or kilobytes.

After developing the monitor, you can:

- **Define thresholds for new metrics**

After the first monitor run, you can define thresholds for metrics that were defined in the script, since these custom metrics did not exist before the first run. This provides more advanced data processing options than regular monitors. Note that metrics can change between script runs, for example, where variables are used in metric names. Thresholds using a metric that does not exist after the monitor run are removed automatically.

- **Share the monitor with other SiteScope users**

After developing the monitor, you can export the monitor to a template, add external jars and/or classes if the monitor depends on them, and create a content package. The content package can then be sent to specific users, or shared with other SiteScope users by publishing it to the SiteScope community on [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>).

By sharing knowledge with other SiteScope users, you can benefit from extended SiteScope monitor coverage and the development of new monitors outside the SiteScope release cycle.

Tasks

This section includes:

- "How to Develop a Custom Monitor" below
- "How to Access the Monitor Configuration Parameters Exposed in the Script" on page 92
- "How to Import and Use a Customizable Monitor" on page 93

How to Develop a Custom Monitor

1. Prerequisites

- You should be an advanced user SiteScope with knowledge of JavaScript.
- You should have knowledge of the application being monitored.

2. Create a Custom monitor

Create a group into which you want to add the custom monitor. Right-click the group, select **New > Monitor**, and select the **Custom** monitor. In the General Settings panel, enter a name and description for the monitor.

3. Create the data processing script

In the **Data Processing Script** area of Custom Monitor Settings, create the script that parses the results and creates new metrics according to the name that you determined.

For details on the monitor configuration properties, including how to access them, and the monitor storage and metrics names, see "How to Access the Monitor Configuration Parameters Exposed in the Script" on page 92.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**). A sample jar file showing the custom monitor's capability to access Java code is provided in the **<SiteScope root directory>\examples\monitors\custom\lib** folder.

For details on scripting in Java, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

Tip:

- A sample Custom monitor script is provided in the **Data Processing Script** box. To use it, you need to uncomment the script.
- Sample scripts for all the custom monitors are available from the sample content package located in the **<SiteScope installation directory>\examples\monitors\custom** folder. **CustomMonitorSamplePackage.zip** contains examples for SiteScope 11.20, and **CustomMonitorsExamples_11_21.zip** contains updated examples including a Custom Database monitor with a dynamic query, a manifest file created using the Export Content Package Wizard, and template mail and template mail subject files. To use these scripts, you need to import the custom monitor content package and then deploy the custom monitor template. For

task details, see steps 3 and 4 of ["How to Import and Use a Customizable Monitor"](#) on page 93.

Note:

- If your monitor needs to open a network connection to another server from the data processing script or the Java code that is called from the script, you must enable the **Allow network access** setting in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- Access for the data processing script is restricted to the following folders/files on the SiteScope server:
 - The `\conf` folder which is located inside each content package (`<SiteScope root directory>\packages\imported` or `<SiteScope root directory>\packages\workspace`) (requires *Read* permissions).
 - `<SiteScope root directory>\logs\custom_monitors*` (all permissions)
- You can use the `custom_monitor.log` file for any info, warning, error, and debug messages that you want to write during the execution of the script. The log is located in `<SiteScope root directory>\logs\custom_monitors`. For details on changing the log to DEBUG mode, see ["Custom Monitor Logs"](#) on page 97.
- By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the **Maximum number of counters** value in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- When working in template mode, you can use template variables in a data processing script.

4. [Generate a path for storing the files used for creating the Custom monitor](#)

Click the **Create Path** button to create a folder where the relevant jars, classes, configuration, and template files required for running the monitor can be saved. A folder with a relative path is created under `<SiteScope root directory>\packages\workspace\package_<Package ID>`. The path is displayed as read only.

The folder contains the following (empty) subfolders:

- `packages\workspace\package_<>\lib`. Used for storing external jar files used by the monitor script.
- `packages\workspace\package_<>\classes`. Used for storing compiled Java classes; note that they should be copied with the entire package folder structure.
- `packages\workspace\package_<>\conf`. Used for storing configuration files, documentation, and XML files.
- `packages\workspace\package_<>\template`. Used for storing the template files that contain the custom monitor (you perform this in ["Create a monitor template - optional"](#) on the next page).

You can copy the required files to these folders at this stage, or when performing "Create a content package - optional" below.

Note: If you add or modify jars/classes after the first monitor run, you must either:

- Restart SiteScope for the changes to take effect, or
- To avoid having to restart SiteScope, you must enable the **Reload classes and jars on each monitor run** option in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.

5. **Configure topology reporting - optional**

To report monitor and related CI topology data to BSM's RTSM, configure the required topology reporting settings as described in How to Configure Topology Reporting for a Custom Monitor in the Using SiteScope Guide.

6. **Configure other settings for the monitor - optional**

Configure other settings for the monitor as required. For details, see Common Monitor Settings in the Using SiteScope Guide.

7. **Save the monitor and wait for the first monitor run**

Save the monitor. SiteScope verifies the correctness of the monitor configuration both locally and on the remote server to be monitored, before saving the settings, regardless of whether you clicked **Verify & Save** or **Save**.

The monitor collects data and filters it based on the script you supplied.

8. **Define thresholds for the metrics - optional**

After the monitor has run, you can:

- Make changes to the script and define thresholds for metrics that were created or updated in the run. For details, see Threshold Settings in the Using SiteScope Guide.
- Check status and values of the metrics in the SiteScope Dashboard.
- Set up alerts on the monitor. For details, see How to Configure an Alert in the Using SiteScope Guide.

9. **Create a monitor template - optional**

- a. To copy the monitor to a template, right-click the monitor, select **Copy to Template**, and select the template group to which you want to add the copied configuration. For details, see How to Create a Template by Copying Existing Configurations in the Using SiteScope Guide.
- b. Make any necessary changes such as adding template variables to the template. For details on template variables, see New Variable Dialog Box.

10. **Create a content package - optional**

- a. Copy the files used for creating the monitor to the predefined content package subfolders:

- **<SiteScope>\packages\workspace\package_<Package ID>\lib.** (Optional) Copy any external jars used by the custom monitor script to this folder. Java classes from the jar files can be accessed from the data processing script. Note that you can use this monitor without external jars.

Note: In the data processing script, to import a package from a jar that does not start with `com.`, `org.`, or `java.`, you must add the package's prefix:

```
importPackage (Packages.<packageName>)
```

For example, `importPackage (Packages.it.companyname.test);`

For details on importing Java classes and packages, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

- **<SiteScope>\packages\workspace\package_<>\classes.** (Optional) Copy the compiled Java classes with the entire package folder structure to this folder; this is not required if the class files were packaged in a jar that was copied to the **\lib** folder. The class files can be accessed from the data processing script.
 - **<SiteScope>\packages\workspace\package_<>\conf.** (Optional) Copy the configuration files, documentation, and XML files to this folder.
 - **<SiteScope>\packages\workspace\package_<>\template.** (Optional) The folder should contain the template files exported from SiteScope (performed in "[Create a monitor template - optional](#)" on the previous page). Each template can contain various types of monitors; custom and regular.
- b. Copy extension files - optional

If the monitor references script or alert extension files in the SiteScope file system, copy them to the relevant folders in **<SiteScope root directory>\packages\workspace\extensions>**:

- **\scripts.** Used for storing script files that are used to run shell commands or other scripts on the machine where SiteScope is running.
- **\scripts.remote.** Used for storing script files that are used for running a script that is stored on a remote machine.
- **\templates.mail.** Used for storing the file containing the format and content of alert messages sent by email.
- **\templates.mail.subject.** Used for storing the file containing the subject line of alert messages sent by email.
- **\templates.mib.** Used for storing the MIB files that are used to create a browsable tree that contains names and descriptions of the objects found during a traversal.
- **\templates.os.** Used for storing the shell commands to be run when monitoring remote UNIX servers.

Note:

- On exporting the files to a content package, the unique package ID is added to the script and template files as a suffix (before the file extension) in the **<SiteScope root directory>\packages\imported** directory, and under the relevant folder in the SiteScope root directory.
- As part of the import process, the **template.os** and **templates.mib** files are edited and the unique package ID is added to some properties inside the files.

c. Export the content package to a zip file

Select the **Templates** context. In the template tree, right-click the template or template container that you want to export to a content package, and select **Export > Content Package**.

In the Export Content Package Wizard, enter details of the content package (manifest), and select the templates and files associated with these templates to include. For Wizard details, see Export Content Package Wizard.

Note: The Select Files page of the Wizard displays files from the **<SiteScope root directory>\packages\workspace\package_<Package ID>** and **<SiteScope root directory>\packages\workspace\extensions>** folders listed above, except for the **\META-INF** and **\templates** folders which are not displayed.

11. Share the custom monitor with other SiteScope users - optional

You can distribute a content package zip file by:

- Sending it to individual SiteScope users.
- Sharing it with other SiteScope users by uploading it to the Community Content for SiteScope page on [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>). HP Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HP Software portfolio.

For task details, see How to publish content to the HP Live Network community.

How to Access the Monitor Configuration Parameters Exposed in the Script

Data Processing Script:

- You can access the configuration parameters for custom monitors in the data processing script using:

```
myContext.getInputData().getConfigurationParameter("<configuration parameter name>");
```

Example:

```
var monitorName = myContext.getInputData().getConfigurationParameter("monitorName");
```

The following monitor properties are exposed to the script (for all custom monitors):

- `monitorName`. The name of the monitor.
- `monitorDescription`. A description of the monitor.

The following monitor properties are exposed to the script for the Custom Database monitor only:

- `dbConnectionUrl`. The connection URL of the database to which you want to connect.
- No additional properties are exposed for the Custom Monitor.
- You can set the summary string which is used as the monitor status in the SiteScope Dashboard using:

```
myContext.getScriptResult().setSummary("<text summary>");
```

The default value is: `summary = <a set of metrics and their values>`

- You can set monitor availability which is displayed in the SiteScope Dashboard using:

```
myContext.getScriptResult().setAvailability(<true/false>)
```

The default value is: `availability = true`

Topology Script:

You can access the configuration parameters for custom monitors in the topology script using:

```
Framework.getDestinationAttributeAsObject("configuration").get("<configuration parameter name>")
```

To access data saved in the monitor storage (this is a place where you can save script data for use in future executions):

```
Framework.getDestinationAttributeAsObject("monitorStorage").get("<configuration parameter name>")
```

To access the list of metric names used in the script:

```
Framework.getDestinationAttributeAsObject("metrics")
```

How to Import and Use a Customizable Monitor

After developing a custom monitor and creating a content package zip file, the content package can then be sent to specific users, or be published to the [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>) community enabling other users to import the monitor for their own use.

For details on using the Wizard, see [Export Content Package Wizard](#).

1. Prerequisites

Only a SiteScope administrator user, or a user granted the **Add, edit or delete templates** permissions can import monitor templates from a content package. For details, see [Permissions in the Using SiteScope Guide](#).

2. Access the custom monitor content package

- If a content package zip file was sent to you, skip to the next step.
- If a content package was made available to the Community Content for SiteScope page on [HP Live Network](#), download the content package to your SiteScope machine. [HP Live](#)

Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HP Software portfolio.

For task details, see How to download a template or content package from the HP Live Network in the Using SiteScope Guide.

3. Import the custom monitor content package

- a. In SiteScope, select the **Templates** context. In the template tree, right-click the template container into which you want to import the content package, and click **Import**.
- b. In the Content Import dialog box, select **Content package**, and click the **Browse** button. Navigate to the folder containing the package you want to import (packages are distributed in zip format). Click **Open**, and then click **OK**.

For details on the Content Import dialog box, see Content Import Dialog Box in the Using SiteScope Guide.

4. Verify the template was imported successfully by checking it was added to the template tree

The content package is copied to the **<SiteScope root directory>\packages\imported** folder, and a new folder is created with the name: **<Package/Zip Name>.zip_<Package ID>**.

The folder contains:

- **\META-INF**. Contains the manifest file where information about the content package is stored.
- **\templates**. Contains files from which templates in this content package were imported into SiteScope.
- **<Package/Zip Name>**. Uncompressed package that contains the above-mentioned folders, the **\extensions** folder which contains script and alert template files referenced by monitors in the imported templates, and the folders used for Custom monitors:
 - **\classes**. Used for storing compiled Java classes.
 - **\conf** Used for storing configuration files, documentation, and XML files.
 - **\lib** Used for storing external jar files used by the monitor script. Note that the **\lib** folder is shared between all monitors imported in the same template.
- **<Package/Zip Name>.zip.properties**. This is the descriptor (manifest) file for content packages created in SiteScope 11.20, that is used in case of rollback, uninstall, or upgrade. The file contains the ID of the SiteScope template that was deployed, the location of the files in SiteScope, and other information about the content package.

The imported templates and dependency files can be used directly or modified as required.

Where script or alert templates are referenced in the user interface, the unique package ID is added as a suffix.

Example: ShortMail alert action template referenced in the Template field.

Action Type Settings	
Action name:	EMail
* Recipients:	Default
Addresses:	
* Subject:	Typical
* Template:	ShortMail_06b62f60-807c-4102-adea-9a7ebdd80e8b

5. Deploy the custom monitor template

After importing the custom monitor template, you can deploy the template to a group.

- a. In the template tree, right-click the custom monitor template you want to deploy, and select **Deploy Template**.
- b. In the Select Group dialog box, select a group into which you want to deploy the template. Alternatively, you can click the **New Group** button and create a new group to which you can deploy the template. For user interface details, see Select Group Dialog Box in the Using SiteScope Guide.
- c. In the Deployment Values dialog box, enter the required variable values in the entry boxes displayed, and click **OK**. The entry boxes displayed correspond to the template variables used in the template objects. For user interface details, see Deployment Values Dialog Box in the Using SiteScope Guide.

Note: When deploying the template or publishing changes in the template to deployed groups, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, since the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.

- d. Verify that the template was deployed successfully (the template objects should be added to the specified group in the monitor tree).

For task details, see How to Deploy Templates Using the User Interface in the Using SiteScope Guide.

6. Configure monitor status thresholds

After the monitor run, you can define thresholds for metrics that were resolved in the run. In the **Threshold Settings** panel of the custom monitor, select metrics for which you want to define thresholds in the **Condition** column by using variables or free text, or selecting default metrics from the drop-down list, and enter the value applicable to the metric parameter.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Custom Monitor Settings

User interface elements are described below:

UI Element	Description
Data Processing Script	
<Script>	<p>The input data for the data processing script is displayed in this box.</p> <p>Define the script that parses the results and creates new metrics. For details on the monitor configuration properties in the script, including how to access them, and the monitor storage and metrics names, see "How to Access the Monitor Configuration Parameters Exposed in the Script" on page 92.</p> <p>Note: By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the Maximum number of counters value in Preferences > Infrastructure Preferences > Custom Monitor Settings.</p>
Package path	<p>Path generated by SiteScope where the files used for developing the monitor can be saved. This enables you to add the jars on which the monitor depends (if applicable), classes, configuration, and templates files to the monitor. The path is displayed as read only.</p> <p>Click the Create Path button to create a folder with a relative path in the SiteScope root directory (<code>packages\workspace\package_<unique ID></code>). The path is displayed as read only.</p> <p>The folder contains the following subfolders into which you copy the files used to create the monitor:</p> <ul style="list-style-type: none">• lib. (Optional) Used for storing external jar files used by the monitor script. Note that you can use this monitor without external jars.• classes. (Optional) Used for storing Java compiled classes; note that they should be copied with the entire package folder structure.• conf. (Optional) Used for storing configuration files, documentation, and XML files.• template. (Mandatory) Used for storing the template files that contain the custom monitor. It must contain at least one template. Each template can contain various types of monitors; custom and regular. <p>Note: This field is displayed when working in monitor mode only. When working in template mode and the monitor is deployed, the content pack is imported into the path.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section describes troubleshooting and limitations for the Custom monitor.

- "General Tips/Limitations" below
- "Custom Monitor Logs" below

General Tips/Limitations

- If a user-defined or imported Java package has the same name as an existing SiteScope or standard Java package, SiteScope ignores the user-defined/imported Java package.
- When setting custom monitor metrics with a string (non-numeric) value, the maximum and average values in the Measurement Summary table of the Management Report are shown as 'n/a'. This also occurs if you change the metric value type, for example, if you set the metric with a numeric value, and later change it to a string value or vice versa.
- When deploying a custom monitor using a template, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, since the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.
- When publishing changes to a template that contains a custom monitor, we recommend using the **Disable custom monitors while publishing changes** option (selected by default) in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. The monitor is temporarily disabled before changes are published and is restored to the enabled state after changes have been made.
- Setting status thresholds using a baseline is not supported on user-defined metrics.

Custom Monitor Logs

- Errors in the monitor (including errors in the script) are written to the SiteScope logs in the same way as for any other monitor. Check the **error.log** and **RunMonitor.log** files.
- Error messages from the script are displayed in the **custom_monitor.log** file located in **<SiteScope root directory>\logs\custom_monitors**. This log can be used for info, warning, error, and debug messages from running the script.

To change the log level to **DEBUG** mode, in **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties**, change **#{loglevel}** to **DEBUG** in the following paragraph:

```
# Custom monitors category
log4j.category.CustomMonitor=#{loglevel},custom.monitor.appender
log4j.additivity.CustomMonitor=false change
```

Chapter 14

Custom Database Monitor

The Custom Database monitor broadens the capabilities of database monitors which are used to monitor the availability and performance of your systems and applications, whose data is accessible through database queries. Using the Custom Database monitor, you can create your own database monitor by developing queries that collect data, and a script that processes the collected data and creates metrics. You can use Java code developed by yourself or by a third-party to process the data.

You can share custom monitors by publishing them to the HP Live Network community, enabling other SiteScope users to import the monitor template for their own use.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **Custom Database** monitor.

Learn More

This section includes:

- "Custom Database Monitor Overview" below
- "IPv6 Addressing Supported Protocols" on the next page

Custom Database Monitor Overview

The Custom Database monitor enables you to develop your own database monitor on top of the SiteScope infrastructure. This provides you with greater flexibility not available in existing monitors.

You can use the Custom Database monitor to:

- **Collect any (database) data you like**

You can create a series of SQL queries for the database tables you want to monitor. SiteScope runs the queries and returns the results to the monitor in an object that contains a set of results for each query. Each time the monitor runs, it re-runs your queries and collects fresh data.

- **Process the collected data**

You can create a script in the monitor that can extract and process the results of the collected data. For example, you can define metrics based on collected data from the database and perform mathematical operations on it as in the sample script provided.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**).

- **Collect data dynamically**

You can include dynamically-defined queries in the data processing script. These queries are executed while the script is running, in contrast to predefined queries, which are executed before the script is run. Dynamically-executed queries provide the added benefit of enabling you to create queries based on values that are not in the monitored entity data store (for example, timestamp), create queries based on previous query results or calculations, and include variables in queries. For details, see Data Processing Script with Dynamic Queries in the Using SiteScope Guide.

After developing the monitor, you can:

- **Define thresholds for new metrics**

After the first monitor run, you can define thresholds for metrics that were defined in the script, since these custom metrics did not exist before the first run. This provides more advanced data processing options than regular monitors. Note that metrics can change between script runs, for example, where variables are used in metric names. Thresholds using a metric that does not exist after the monitor run are removed automatically.

- **Share the monitor with other SiteScope users**

After developing the monitor, you can export the monitor to a template, add external jars and/or classes if the monitor depends on them, and create a content package. The content package can then be sent to specific users, or shared with other SiteScope users by publishing it to the SiteScope community on [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>).

By sharing knowledge with other SiteScope users, you can benefit from extended SiteScope monitor coverage and the development of new monitors outside the SiteScope release cycle.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports IPv6 addresses in the TCP (JDBC) protocol. Support for IPv6 might also depend on the JDBC driver being used.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

This section includes:

- "How to Develop a Custom Database Monitor" below
- "How to Access the Monitor Configuration Parameters Exposed in the Script" on page 106
- "How to Import and Use a Custom Database Monitor" on page 107

How to Develop a Custom Database Monitor

1. Prerequisites

- You should be an advanced SiteScope user with knowledge of JavaScript.
- You should have knowledge of SQL and the database systems being monitored.
- The database monitoring environment must be configured as described in "How to Configure the Database Query Monitoring Environment" on page 171. (Ignore the last step in this task.)

2. Create a Custom Database monitor with the relevant database queries

- a. Create a group into which you want to add the custom monitor. Right-click the group, select **New > Monitor**, and select the **Custom Database** monitor.
- b. Configure the monitor properties:
 - In the **General Settings** panel, enter a name and description for the monitor.
 - In the **Main Settings** area of Custom Database Monitor Settings, configure the monitor properties as described in the UI Descriptions section below.
 - In the **Queries** table, enter a separate query for each database instance and table in the database you want to monitor.

Tip: By default, you can enter up to 10 queries in the table. You can modify the number of queries that can be added to the table in **Preferences > Infrastructure Preferences > Custom Monitor Settings** by configuring the **Maximum number of queries** value.

3. Create the data processing script

In the **Data Processing Script** area of Custom Database Monitor Settings, create the script that parses the results and creates new metrics in the names that you determined.

In addition, you can include any number of queries in the script. The queries are executed as the script is run, which means that the monitor collects fresh data from the database being monitored. After the data is retrieved, it becomes available for the script to use. A query in a script has the same syntax as a query defined in the queries table, but it can be structured using variables which makes it dynamic within the monitor run context. For details on dynamic queries, see Data Processing Script with Dynamic Queries in the Using SiteScope Guide.

For details on the monitor configuration properties, including how to access them, and the monitor storage and metrics names, see "[How to Access the Monitor Configuration Parameters Exposed in the Script](#)" on page 106.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**). A sample jar file showing the custom monitor's capability to access Java code is provided in the **<SiteScope root directory>\examples\monitors\custom\lib** folder.

For details on scripting in Java, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

Tip:

- A sample Custom Database monitor script is provided in the **Data Processing Script** box. To use it, you need to uncomment the script.
- Sample scripts for all the custom monitors are available from the sample content package located in the **<SiteScope installation directory>\examples\monitors\custom** folder. **CustomMonitorSamplePackage.zip** contains examples for SiteScope 11.20, and **CustomMonitorsExamples_11_21.zip** contains updated examples including a Custom Database monitor with a dynamic query, a manifest file created using the Export Content Package Wizard, and template mail and template mail subject files. To use these scripts, you need to import the custom monitor content package and then deploy the custom monitor template. For task details, see steps 3 and 4 of "[How to Import and Use a Custom Database Monitor](#)" on page 107.

Note:

- If your monitor needs to open a network connection to another server from the data processing script or the Java code that is called from the script, you must enable the **Allow network access** setting in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- Access for the data processing script is restricted to the following folders/files on the SiteScope server:
 - The **\conf** folder which is located inside each content package (**<SiteScope root directory>\packages\imported** or **<SiteScope root directory>\packages\workspace**) (requires *Read* permissions).
 - **<SiteScope root directory>\logs\custom_monitors*** (all permissions)
- You can use the **custom_monitor.log** file for any info, warning, error, and debug messages that you want to write during the execution of the script. The log is located in **<SiteScope root directory>\logs\custom_monitors**. For details on changing the log to DEBUG mode, see "[Custom Monitor Logs](#)" on page 115.
- By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the **Maximum number of counters** value in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.

- When working in template mode, you can use template variables in a data processing script.

4. **Generate a path for storing the files used for creating the Custom Database monitor**

Click the **Create Path** button to create a folder where the relevant jars, classes, configuration, and template files required for running the monitor can be saved. A folder with a relative path is created under **<SiteScope root directory>\packages\workspace\package_<Package ID>**. The path is displayed as read only.

The folder contains the following (empty) subfolders:

- **packages\workspace\package_<>\lib**. Used for storing external jar files used by the monitor script.
- **packages\workspace\package_<>\classes**. Used for storing compiled Java classes; note that they should be copied with the entire package folder structure.
- **packages\workspace\package_<>\conf**. Used for storing configuration files, documentation, and XML files.
- **packages\workspace\package_<>\template**. Used for storing the template files that contain the custom monitor (you perform this in "Create a monitor template - optional" on the next page).

You can copy the required files to these folders at this stage, or when performing "Create a content package - optional" on the next page.

Note: If you add or modify jars/classes after the first monitor run, you must either:

- Restart SiteScope for the changes to take effect, or
- To avoid having to restart SiteScope, you must enable the **Reload classes and jars on each monitor run** option in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.

5. **Configure topology reporting - optional**

To report monitor and related CI topology data to BSM's RTSM, configure the required topology reporting settings as described in How to Configure Topology Reporting for a Custom Monitor in the Using SiteScope Guide.

6. **Configure other settings for the monitor - optional**

Configure other settings for the monitor as required. For details, see Common Monitor Settings in the Using SiteScope Guide.

7. **Save the monitor and wait for the first monitor run**

Save the monitor. SiteScope verifies the correctness of the monitor configuration both locally and on the remote server to be monitored, before saving the settings, regardless of whether you clicked **Verify & Save** or **Save**.

The monitor collects data from the database instances, and filters the data based on the script you supplied.

8. Define thresholds for the metrics - optional

After the monitor has run, you can:

- Make changes to the script and define thresholds for metrics that were created or updated in the run. For details, see *Threshold Settings* in the *Using SiteScope Guide*.
- Check status and values of the metrics in the SiteScope Dashboard.
- Set up alerts on the monitor. For details, see *How to Configure an Alert* in the *Using SiteScope Guide*.

9. Create a monitor template - optional

- a. To copy the monitor to a template, right-click the monitor, select **Copy to Template**, and select the template group to which you want to add the copied configuration. For details, see *How to Create a Template by Copying Existing Configurations* in the *Using SiteScope Guide*.
- b. Make any necessary changes such as adding template variables to the template. For details on template variables, see *New Variable Dialog Box*.

10. Create a content package - optional

- a. Copy the files used for creating the monitor to the predefined content package subfolders:
 - **<SiteScope>\packages\workspace\package_<Package ID>\lib**. (Optional) Copy any external jars used by the custom monitor script to this folder. Java classes from the jar files can be accessed from the data processing script. Note that you can use this monitor without external jars.

Note: In the data processing script, to import a package from a jar that does not start with `com.`, `org.`, or `java.`, you must add the package's prefix:

```
importPackage (Packages.<packageName>)
```

For example, `importPackage (Packages.it.companyname.test);`

For details on importing Java classes and packages, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

- **<SiteScope>\packages\workspace\package_<>\classes**. (Optional) Copy the compiled Java classes with the entire package folder structure to this folder; this is not required if the class files were packaged in a jar that was copied to the **lib** folder. The class files can be accessed from the data processing script.
- **<SiteScope>\packages\workspace\package_<>\conf**. (Optional) Copy the configuration files, documentation, and XML files to this folder.
- **<SiteScope>\packages\workspace\package_<>\template**. (Optional) The folder should contain the template files exported from SiteScope (performed in "[Create a monitor template - optional](#)" above). Each template can contain various types of monitors; custom and regular.

b. Copy extension files - optional

If the monitor references script or alert extension files in the SiteScope file system, copy them to the relevant folders in **<SiteScope root directory>\packages\workspace\extensions>**:

- **\scripts**. Used for storing script files that are used to run shell commands or other scripts on the machine where SiteScope is running.
- **\scripts.remote**. Used for storing script files that are used for running a script that is stored on a remote machine.
- **\templates.mail**. Used for storing the file containing the format and content of alert messages sent by email.
- **\templates.mail.subject**. Used for storing the file containing the subject line of alert messages sent by email.
- **\templates.mib**. Used for storing the MIB files that are used to create a browsable tree that contains names and descriptions of the objects found during a traversal.
- **\templates.os**. Used for storing the shell commands to be run when monitoring remote UNIX servers.

Note:

- On exporting the files to a content package, the unique package ID is added to the script and template files as a suffix (before the file extension) in the **<SiteScope root directory>\packages\imported** directory, and under the relevant folder in the SiteScope root directory.
- As part of the import process, the **template.os** and **templates.mib** files are edited and the unique package ID is added to some properties inside the files.

c. Export the content package to a zip file

Select the **Templates** context. In the template tree, right-click the template or template container that you want to export to a content package, and select **Export > Content Package**.

In the Export Content Package Wizard, enter details of the content package (manifest), and select the templates and files associated with these templates to include. For Wizard details, see Export Content Package Wizard.

Note: The Select Files page of the Wizard displays files from the **<SiteScope root directory>\packages\workspace\package_<Package ID>** and **<SiteScope root directory>\packages\workspace\extensions>** folders listed above, except for the **\META-INF** and **\templates** folders which are not displayed.

11. Share the custom monitor with other SiteScope users - optional

You can distribute a content package zip file by:

- Sending it to individual SiteScope users.

- Sharing it with other SiteScope users by uploading it to the Community Content for SiteScope page on [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>). HP Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HP Software portfolio.

For task details, see [How to publish content to the HP Live Network community](#).

How to Access the Monitor Configuration Parameters Exposed in the Script

Data Processing Script:

- You can access the configuration parameters for custom monitors in the data processing script using:

```
myContext.getInputData().getConfigurationParameter("<configuration parameter name>");
```

Example:

```
var monitorName = myContext.getInputData().getConfigurationParameter("monitorName");
```

The following monitor properties are exposed to the script (for all custom monitors):

- `monitorName`. The name of the monitor.
- `monitorDescription`. A description of the monitor.

The following monitor properties are exposed to the script for the Custom Database monitor only:

- `dbConnectionUrl`. The connection URL of the database to which you want to connect.
- You can set the summary string which is used as the monitor status in the SiteScope Dashboard using:

```
myContext.getScriptResult().setSummary("<text summary>");
```

The default value is: `summary = <a set of metrics and their values>`

- You can set monitor availability which is displayed in the SiteScope Dashboard using:

```
myContext.getScriptResult().setAvailability(<true/false>)
```

The default value is: `availability = true`

Topology Script:

You can access the configuration parameters for custom monitors in the topology script using:

```
Framework.getDestinationAttributeAsObject("configuration").get("<configuration parameter name>")
```

To access data saved in the monitor storage (this is a place where you can save script data for use in future executions):

```
Framework.getDestinationAttributeAsObject("monitorStorage").get("<configuration parameter name>")
```

To access the list of metric names used in the script:

```
Framework.getDestinationAttributeAsObject("metrics")
```

How to Import and Use a Custom Database Monitor

After developing a custom monitor and creating a content package zip file, the content package can then be sent to specific users, or be published to the [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>) community enabling other users to import the monitor for their own use.

For details on using the Wizard, see [Export Content Package Wizard](#).

1. Prerequisites

Only a SiteScope administrator user, or a user granted the **Add, edit or delete templates** permissions can import monitor templates from a content package. For details, see [Permissions in the Using SiteScope Guide](#).

2. Access the custom monitor content package zip file

- If a content package zip file was sent to you, skip to the next step.
- If a content package was made available to the Community Content for SiteScope page on [HP Live Network](#), download the content package to your SiteScope machine. HP Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HP Software portfolio.

For task details, see [How to download a template or content package from the HP Live Network in the Using SiteScope Guide](#).

3. Import the custom monitor content package

- a. In SiteScope, select the **Templates** context. In the template tree, right-click the template container into which you want to import the content package, and click **Import**.
- b. In the Content Import dialog box, select **Content package**, and click the **Browse** button. Navigate to the folder containing the package you want to import (packages are distributed in zip format). Click **Open**, and then click **OK**.

For details on the Content Import dialog box, see [Content Import Dialog Box in the Using SiteScope Guide](#).

4. Verify the template was imported successfully by checking it was added to the template tree

The content package is copied to the **<SiteScope root directory>\packages\imported** folder, and a new folder is created with the name: **<Package/Zip Name>.zip_<Package ID>**.

The folder contains:

- **\META-INF**. Contains the manifest file where information about the content package is stored.
- **\templates**. Contains files from which templates in this content package were imported into SiteScope.
- **<Package/Zip Name>**. Uncompressed package that contains the above-mentioned folders, the **\extensions** folder which contains script and alert template files referenced by monitors in the imported templates, and the folders used for Custom monitors:

- **\classes**. Used for storing compiled Java classes.
- **\conf** Used for storing configuration files, documentation, and XML files.
- **\lib** Used for storing external jar files used by the monitor script. Note that the **\lib** folder is shared between all monitors imported in the same template.
- **<Package/Zip Name>.zip.properties**. This is the descriptor (manifest) file for content packages created in SiteScope 11.20, that is used in case of rollback, uninstall, or upgrade. The file contains the ID of the SiteScope template that was deployed, the location of the files in SiteScope, and other information about the content package.

The imported templates and dependency files can be used directly or modified as required.

Where script or alert templates are referenced in the user interface, the unique package ID is added as a suffix.

Example: ShortMail alert action template referenced in the Template field.

Action Type Settings	
Action name:	E Mail
* Recipients:	Default
Addresses:	
* Subject:	Typical
* Template:	ShortMail_06b62f60-807c-4102-adea-9a7ebdd80e8b

5. Deploy the custom monitor template

After importing the custom monitor template, you can deploy the template to a group.

- a. In the template tree, right-click the custom monitor template you want to deploy, and select **Deploy Template**.
- b. In the Select Group dialog box, select a group into which you want to deploy the template. Alternatively, you can click the **New Group** button and create a new group to which you can deploy the template. For user interface details, see Select Group Dialog Box in the Using SiteScope Guide.
- c. In the Deployment Values dialog box, enter the required variable values in the entry boxes displayed, and click **OK**. The entry boxes displayed correspond to the template variables used in the template objects. For user interface details, see Deployment Values Dialog Box in the Using SiteScope Guide.

Note: When deploying the template or publishing changes in the template to deployed groups, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, since the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.

- d. Verify that the template was deployed successfully (the template objects should be added to the specified group in the monitor tree).

For task details, see [How to Deploy Templates Using the User Interface](#) in the [Using SiteScope Guide](#).

6. **Configure monitor status thresholds**

When deploying the template, only the default metrics included with the monitor are displayed (custom metrics defined in the script do not exist until after the monitor has run). For example, when configuring a Custom Log File monitor, the following metrics are default: `line`, `lines/min`, `matches`, `matches/min`.

After the monitor run, you can define thresholds for metrics that were resolved in the run. In the **Threshold Settings** panel of the custom monitor, select metrics for which you want to define thresholds in the **Condition** column by using variables or free text, or selecting default metrics from the drop-down list, and enter the value applicable to the metric parameter.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Custom Database Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Database connection URL	<p>Connection URL of the database to which you want to connect. The syntax should be in the format:</p> <pre>jdbc:<sub protocol>:<subname> or <IP address>:<database server port>:<sid>.</pre> <p>Example: To connect to the Oracle database on a machine using port 1521 use: <code>jdbc:oracle:thin:@206.168.191.19:1521:ORCL.</code> The colon (:) and the (@) symbols must be included as shown.</p>
Database driver	<p>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 <SiteScope root directory>\WEB-INF\lib\ directory.</p> <p>Default value: <code>sun.jdbc.odbc.JdbcOdbcDriver</code></p> <p>Tip: You can specify database drivers that have timeout problems (where database queries processed with these drivers exceed the timeout specified in the monitor's Query timeout field) in the Timeout proxied query drivers list field (in Preferences > Infrastructure Preferences > General Settings). These drivers are queried separately with a monitor-based timeout.</p>
Database user name	<p>User name used to log on to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystem JDBC-ODBC bridge driver, <code>sun.jdbc.odbc.JdbcOdbcDriver</code>), you can leave this blank and choose Windows Authentication when you setup the ODBC connection.</p> <p>With Windows 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>

UI Element	Description
Database password	<p>Password used to log on 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 Windows Authentication when you create the ODBC connection.</p> <p>With Windows Authentication, SiteScope connects using the login account of the SiteScope service.</p>
Max rows	<p>Maximum number of rows the monitor retrieves from the database for each monitor run. 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. The same rows in the amount limited by this property value are retrieved from the beginning of the table on each monitor run if Enumerating field, Enumerating field type and Initial enumerating value fields are not populated.</p> <p>The value should be sufficient to keep up with database table growth, yet small enough to avoid java.lang.OutOfMemoryException 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> <p>Default value: 5000 rows</p>
Physically close if idle connection count exceeds	<p>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>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>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>
Use connection pool	<p>Enables SQL connection sharing. 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>
Database queries table	

UI Element	Description	
	New query. Adds a new line to the Database queries table, enabling you to enter a new query.	
	Edit query. Opens the Query Editor, in which the selected SQL query is displayed and can be edited.	
	Delete query. Deletes the selected query.	
No	<p>The query number. By default, you can add up to 10 queries to the table. The queries are run in the order in which they appear in the table.</p> <p>Note: You can modify the number of queries that can be added to the table by changing the Maximum number of queries value in Preferences > Infrastructure Preferences > Custom Monitor Settings.</p>	
Queries	Enter a query for each database instance and table in the database you want to monitor. You can create or edit a query in the table (in line mode), or in the Query Editor. To open the Query Editor, click the Edit query button. It is recommended to use the Query Editor when adding or viewing long queries.	
Enumerating field	<p>Enumeration means the monitor retrieves the rows that were added to the queried table since its last execution. Enumerating field is the column name for the database field that the monitor uses for retrieving these rows.</p> <p>Note: The column used as enumerating field must be included in the SELECT clause.</p>	
Enumerating field 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. The following table maps SQL types to the required enumerating field type.	
	SQL Type	Enumerating Field Type
	SMALLINT	INTEGER
	INTEGER	INTEGER / LONG
	BIGINT	LONG
	NUMERIC	LONG
	DOUBLE	DOUBLE
	DECIMAL	DOUBLE
	FLOAT	DOUBLE
	TIMESTAMP	TIMESTAMP
	DATE	TIMESTAMP

UI Element	Description
Initial enumerating value	<p>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 <code>DATE</code> and you enter a value of <code>2000-01-31 12:00:00</code> 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>
Data Processing Script	
<Script>	<p>The input data for the data processing script is displayed in this box.</p> <p>Define the script that parses the results and creates new metrics. For details on the monitor configuration properties in the script, including how to access them, and the monitor storage and metrics names, see "How to Access the Monitor Configuration Parameters Exposed in the Script" on page 106.</p> <p>Note: By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the Maximum number of counters value in Preferences > Infrastructure Preferences > Custom Monitor Settings.</p>
Package path	<p>Path generated by SiteScope where the files used for developing the monitor can be saved. This enables you to add the jars on which the monitor depends (if applicable), classes, configuration, and templates files to the monitor. The path is displayed as read only.</p> <p>Click the Create Path button to create a folder with a relative path in the SiteScope root directory (<code>packages\workspace\package_<unique ID></code>). The path is displayed as read only.</p> <p>The folder contains the following subfolders into which you copy the files used to create the monitor:</p> <ul style="list-style-type: none"> • lib. (Optional) Used for storing external jar files used by the monitor script. Note that you can use this monitor without external jars. • classes. (Optional) Used for storing Java compiled classes; note that they should be copied with the entire package folder structure. • conf. (Optional) Used for storing configuration files, documentation, and XML files. • template. (Mandatory) Used for storing the template files that contain the custom monitor. It must contain at least one template. Each template can contain various types of monitors; custom and regular. <p>Note: This field is displayed when working in monitor mode only. When working in template mode and the monitor is deployed, the content pack is imported into the path.</p>

UI Element	Description
Use Tool (Lower left side of the New Custom Database Monitor dialog box)	Click the Use Tool button to open the Database Connection tool when configuring or editing a monitor. This enables you to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database (provided you are an administrator in SiteScope, or a user granted Use monitor tools permissions). For details on the tool, see Database Connection Tool in the Using SiteScope Guide.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section describes troubleshooting and limitations for the Custom Database monitor.

- "General Tips/Limitations" below
- "Custom Monitor Logs" below

General Tips/Limitations

- If a user-defined or imported Java package has the same name as an existing SiteScope or standard Java package, SiteScope ignores the user-defined/imported Java package.
- When setting custom monitor metrics with a string (non-numeric) value, the maximum and average values in the Measurement Summary table of the Management Report are shown as 'n/a'. This also occurs if you change the metric value type, for example, if you set the metric with a numeric value, and later change it to a string value or vice versa.
- When deploying a custom monitor using a template, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, since the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.
- When publishing changes to a template that contains a custom monitor, we recommend using the **Disable custom monitors while publishing changes** option (selected by default) in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. The monitor is temporarily disabled before changes are published and is restored to the enabled state after changes have been made.
- Setting status thresholds using a baseline is not supported on user-defined metrics.
- If running a dynamic query from within a data processing script fails, an exception is thrown.

Custom Monitor Logs

- Errors in the monitor (including errors in the script) are written to the SiteScope logs in the same way as for any other monitor. Check the **error.log** and **RunMonitor.log** files.
- Error messages from the script are displayed in the **custom_monitor.log** file located in **<SiteScope root directory>\logs\custom_monitors**. This log can be used for info, warning, error, and debug messages from running the script.

To change the log level to **DEBUG** mode, in **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties**, change **#{loglevel}** to **DEBUG** in the following paragraph:

```
# Custom monitors category
log4j.category.CustomMonitor=#{loglevel},custom.monitor.appender
log4j.additivity.CustomMonitor=false change
```

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, 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 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 Database driver.
- **error, connect error, No suitable driver:** check for syntax errors in Database connection URL, such as dots instead of colons.

Possible Errors Using the MySQL Driver

If, after enabling SiteScope to monitor a MySQL database, you get an authorization error in the Database Query monitor, 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.

Possible Errors with Sybase Database Monitoring

- Verify you are using the correct driver for the version of Sybase you are monitoring. Enter `com.sybase.jdbc.SybDriver` for Sybase version 4.x. and `com.sybase.jdbc2.jdbc.SybDriver` for Sybase version 5.x.
- **error, driver connect error, com/sybase/jdbc/SybDriver.** Verify there are no spaces at the end of the driver name. Save the changes and try the monitor again.
- **connect error, JZ006: Caught IOException: java.net.UnknownHostException: dbservername.** Verify the name of the database server in **Database connection URL** is correct.

Chapter 15

Custom Log File Monitor

The Custom Log File monitor broadens the capabilities of Log File monitors which are used to automatically scan log files for error information, thereby eliminating the need to manually scan the logs. You can create your own Log File monitor that scans for matches in the form of a text phrase or regular expression, and a script that processes the collected data and creates metrics. You can use Java code developed by yourself or by a third-party to process the data.

You can share custom monitors by publishing them to the HP Live Network community, enabling other SiteScope users to import the monitor template for their own use.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **Custom Log File** monitor.

Learn More

This section includes:

- "Custom Log File Monitor Overview" below
- "Scheduling the Monitor" on the next page
- "Customizing Custom Log File Content Matches and Monitor Alerts" on the next page
- "Support for IPv6 Addresses" on the next page

Custom Log File Monitor Overview

The Custom Log File monitor enables you to develop your own Log File monitor on top of the SiteScope infrastructure.

Custom monitors enable you to do the following:

- **Create monitors that provide additional metrics not available in existing monitors**

You can define a text phrase or regular expression that watches for log file entries, and create new metrics from the collected data. Each time the monitor runs, it updates the metrics and returns a status for the metrics defined in the script.

- **Process the collected data**

The returned data can be extracted and processed in the script. For example, you can create a monitor that scans a log file for content match of **system time** and **idle time** values, and develop a script that creates a metric named **sum of overall CPU usage**, which is the sum of these values.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**).

- **Customize how results are displayed**

You can determine how results are displayed. For example, whether result data is displayed in megabytes or kilobytes.

After developing the monitor, you can:

- **Define thresholds for new metrics**

After the first monitor run, you can define thresholds for metrics that were defined in the script, since these custom metrics did not exist before the first run. This provides more advanced data processing options than regular monitors. Note that metrics can change between script runs, for example, where variables are used in metric names. Thresholds using a metric that does not exist after the monitor run are removed automatically.

- **Share the monitor with other SiteScope users**

After developing the monitor, you can export the monitor to a template, add external jars and/or classes if the monitor depends on them, and create a content package. The content package can then be sent to specific users, or shared with other SiteScope users by publishing it to the SiteScope community on [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>).

By sharing knowledge with other SiteScope users, you can benefit from extended SiteScope monitor coverage and the development of new monitors outside the SiteScope release cycle.

Scheduling the Monitor

You can schedule Custom 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.

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 the "Check from beginning" on page 135 property.

Customizing Custom Log File Content Matches and Monitor Alerts

You can create a Custom Log File monitor that triggers customized alerts for content matches according to the threshold status of the monitor.

To configure the Custom Log File monitor with custom matches and alerts:

1. In the Custom Log File Monitor Settings, configure the following settings:
 - **Run alerts:** Select the **For each log entry matched** option.
 - **Content match:** Enter the text to look for in the log entries. For example, to find `text` entries `redflag` and `disaster` in the log file, enter `/(redflag|disaster)/`.
 - **Match value label:.** Enter a label name for the matched values found in the target log file. For example, type `matchedValue`.
2. In the Threshold Settings, set the error and warning threshold. For example, set `Error if matchedValue == disaster` and set `Warning if matchedValue == redflag`.
3. Configure error, warning, and good alerts for the Custom 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 *How to Configure an Alert* in the *Using SiteScope Guide*.

Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the following protocols are supported:

- NetBIOS (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

This section includes:

- "How to Develop the Custom Log File Monitor" below
- "How to Access the Monitor Configuration Parameters Exposed in the Script" on page 128
- "How to Import and Use a Custom Log File Monitor" on page 129

How to Develop the Custom Log File Monitor

1. Prerequisites

- You should be an advanced SiteScope user with knowledge of writing scripts in JavaScript, and have knowledge of the content of the log file of the application being monitored.
- The following configuration requirements must be performed or verified before the Custom Log File monitor can be used:
 - The log file to be monitored must exist, and be accessible under credentials used for connecting to the remote server, or under which SiteScope is running (if monitoring a local file).
 - The remote server should be created with credentials that grant read access on the monitored file.

2. Create a Custom Log File monitor with the relevant regular expressions to match lines in the log file

- a. Create a group into which you want to add the custom monitor. Right-click the group, select **New > Monitor**, and select the **Custom Log File** monitor.
- b. In the **General Settings** panel, enter a name and description for the monitor.
- c. In the **Custom Log File Monitor Settings** panel, configure the monitor properties as described in the UI Descriptions section below.

In the **Content match** box, enter a regular expression depending on whether:

- You want to process matched rows only (in which case, the regular expression should not contain groupings). For sample configuration details and results, see "[Example A - Configuring a Custom Log File monitor without grouping](#)" on the next page.
- You want to process the matched rows and custom matching values (in which case, the regular expression should contain groupings). For sample configuration details and results, see "[Example B - Configuring a Custom Log File monitor with matching custom values \(grouping\)](#)" on page 123.
- You are running the monitor on a remote UNIX machine. For sample configuration details and results, see "[Example C - Configuring a Custom Log File monitor to run on a remote UNIX server](#)" on page 124.

All matched lines of the log file are processed as input data for the data processing script.

Example A - Configuring a Custom Log File monitor without grouping

- Configure the following properties in Custom Log File Monitor Settings:

Content match: /ERROR/

- For logs:

```
2012-05-01 13:40:17, ERROR - request failed
2012-05-01 13:41:55, INFO - system check complete
2012-05-01 13:43:08, INFO - new record created
2012-05-01 13:47:12, INFO - Starting service: Event Integration Startup Task
2012-05-01 13:47:12, INFO - Starting service: Statistics Task
2012-05-01 13:47:12, INFO - Starting service: SQL Connection Management Service
2011-09-07 16:50:43, ERROR - Standard directory handler failed with exception
2011-09-07 16:58:01, INFO - The Heartbeat Scheduler was started
```

The result is the following two lines:

```
2012-05-01 13:40:17, ERROR - request failed
2011-09-07 16:50:43, ERROR - Standard directory handler failed with exception
```

Example B - Configuring a Custom Log File monitor with matching custom values (grouping)

- Configure the following properties in Custom Log File Monitor Settings:

Content match: /Used Memory=([0-9]*)MB Available Memory=([0-9]*)MB/

Match value label: used,available

- For logs:

```
2011-09-12 16:46:23,390 [StatisticsLogger]
INFO - Used Memory=56MB Available Memory=439MB Total Memory=496MB
Max Memory=496MB

2011-09-12 16:46:23,390 [StatisticsLogger]
INFO - PoolName=ProcessPool::perfex utilization=0.0%
avgWaitInQueueTime=0 poolMaxSize=200 execTime=0

2011-09-12 16:46:23,390 [StatisticsLogger]
INFO - PoolName=ProcessPool::perfex_dispatcher utilization=0.0%
avgWaitInQueueTime=0 poolMaxSize=200 execTime=0

2011-09-12 16:46:23,390 [StatisticsLogger]
INFO - executionCount=0 averageTime=?ms driftAverageTime=?ms

2011-09-12 16:47:23,382 [StatisticsLogger]
INFO - Used Memory=51MB Available Memory=444MB Total Memory=496MB
Max Memory=496MB
```

The result is the following two lines and values in bold (for the used and available labels):

```
2011-09-12 16:46:23,390 [StatisticsLogger]
INFO - Used Memory=56MB Available Memory=439MB Total Memory=496MB
Max Memory=496MB

2011-09-12 16:47:23,382 [StatisticsLogger]
INFO - Used Memory=51MB Available Memory=444MB Total Memory=496MB
Max Memory=496MB
```

Example C - Configuring a Custom Log File monitor to run on a remote UNIX server

- Configure the following properties in Custom Log File Monitor Settings:

Content match: /Used Memory=([0-9]*)MB Available Memory=([0-9]*)MB/

Match value label: used,available

Server-side processing: Selected

Return matching raw data from server-side: Not selected

- For logs:

```
2011-09-12 16:46:23,390 [StatisticsLogger] INFO - Used Memory=56MB
Available Memory=439MB Total Memory=496MB Max Memory=496MB

2011-09-12 16:46:23,390 [StatisticsLogger] INFO - PoolName=ProcessPool::
perfex utilization=0.0% avgWaitInQueueTime=0 poolMaxSize=200 execTime=0

2011-09-12 16:46:23,390 [StatisticsLogger] INFO - PoolName=ProcessPool::
perfex_dispatcher utilization=0.0% avgWaitInQueueTime=0 poolMaxSize=200 execTime=0

2011-09-12 16:46:23,390 [StatisticsLogger] INFO - executionCount=0
averageTime=?ms driftAverageTime=?ms
```

```
2011-09-12 16:47:23,382 [StatisticsLogger] INFO - Used Memory=51MB
Available Memory=444MB Total Memory=496MB Max Memory=496MB
```

The result is the following two lines and values in bold (for the used and available labels):

```
2011-09-12 16:46:23,390 [StatisticsLogger] INFO - Used Memory=56MB
Available Memory=439MB Total Memory=496MB Max Memory=496MB

2011-09-12 16:47:23,382 [StatisticsLogger] INFO - Used Memory=51MB
Available Memory=444MB Total Memory=496MB Max Memory=496MB
```

3. Create the data processing script

In the **Data Processing Script** area, create the script that parses raw data and log match values and creates new metrics according to the name that you determined.

For example, you could write a script that calculates sum of the **system time** and **idle time** that are transferred as a result of log file scanning. The new metric will be displayed in the SiteScope Dashboard as **sum of overall CPU usage**.

For details on the monitor configuration properties, including how to access them, and the monitor storage and metrics names, see "[How to Access the Monitor Configuration Parameters Exposed in the Script](#)" on page 128.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**). A sample jar file showing the custom monitor's capability to access Java code is provided in the **<SiteScope root directory>\examples\monitors\custom\lib** folder.

For details on scripting in Java, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

Tip:

- A sample Custom Log File monitor script is provided in the **Data Processing Script** box. To use it, you need to uncomment the script.
- Sample scripts for all the custom monitors are available from the sample content package located in the **<SiteScope installation directory>\examples\monitors\custom** folder. **CustomMonitorSamplePackage.zip** contains examples for SiteScope 11.20, and **CustomMonitorsExamples_11_21.zip** contains updated examples including a Custom Database monitor with a dynamic query, a manifest file created using the Export Content Package Wizard, and template mail and template mail subject files. To use these scripts, you need to import the custom monitor content package and then deploy the custom monitor template. For task details, see steps 3 and 4 of "[How to Import and Use a Custom Log File Monitor](#)" on page 129.

Note:

- If your monitor needs to open a network connection to another server from the data processing script or the Java code that is called from the script, you must enable the **Allow network access** setting in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- Access for the data processing script is restricted to the following folders/files on the SiteScope server:
 - The **\conf** folder which is located inside each content package (**<SiteScope root directory>\packages\imported** or **<SiteScope root directory>\packages\workspace**) (requires *Read* permissions).
 - **<SiteScope root directory>\logs\custom_monitors*** (all permissions)
- You can use the **custom_monitor.log** file for any info, warning, error, and debug messages that you want to write during the execution of the script. The log is located in **<SiteScope root directory>\logs\custom_monitors**. For details on changing the log to DEBUG mode, see "[Custom Monitor Logs](#)" on page 139.
- By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the **Maximum number of counters** value in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- When working in template mode, you can use template variables in a data processing script.

4. **Generate a path for storing the files used for creating the Custom Log File monitor**

Click the **Create Path** button to create a folder where the relevant jars, classes, configuration, and template files required for running the monitor can be saved. A folder with a relative path is created under **<SiteScope root directory>\packages\workspace\package_<Package ID>**. The path is displayed as read only.

The folder contains the following (empty) subfolders:

- `packages\workspace\package_<>\lib`. Used for storing external jar files used by the monitor script.
- `packages\workspace\package_<>\classes`. Used for storing compiled Java classes; note that they should be copied with the entire package folder structure.
- `packages\workspace\package_<>\conf`. Used for storing configuration files, documentation, and XML files.
- `packages\workspace\package_<>\template`. Used for storing the template files that contain the custom monitor (you perform this in "Create a monitor template - optional" below).

You can copy the required files to these folders at this stage, or when performing "Custom Log File Monitor" on page 117.

Note: If you add or modify jars/classes after the first monitor run, you must either:

- Restart SiteScope for the changes to take effect, or
- To avoid having to restart SiteScope, you must enable the **Reload classes and jars on each monitor run** option in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.

5. **Configure topology reporting - optional**

To report monitor and related CI topology data to BSM's RTSM, configure the required topology reporting settings as described in How to Configure Topology Reporting for a Custom Monitor in the Using SiteScope Guide.

6. **Configure other settings for the monitor - optional**

Configure other settings for the monitor as required. For details, see Common Monitor Settings in the Using SiteScope Guide.

7. **Save the monitor and wait for the first monitor run**

Save the monitor. SiteScope verifies the correctness of the monitor configuration both locally and on the remote server to be monitored, before saving the settings (this is regardless of whether you clicked **Verify & Save** or **Save**).

The monitor collects data from the log files, and filters the data based on the script you supplied.

8. **Define thresholds for the metrics - optional**

After the monitor has run, you can:

- Make changes to the script and define thresholds for metrics that were created or updated in the run. For details, see Threshold Settings in the Using SiteScope Guide.
- Check status and values of the metrics in the SiteScope Dashboard.
- Set up alerts on the monitor. For details, see How to Configure an Alert in the Using SiteScope Guide.

9. **Create a monitor template - optional**

- a. To copy the monitor to a template, right-click the monitor, select **Copy to Template**, and select the template group to which you want to add the copied configuration. For details, see *How to Create a Template by Copying Existing Configurations* in the *Using SiteScope Guide*.
- b. Make any necessary changes such as adding template variables to the template. For details on template variables, see *New Variable Dialog Box*.

10. Create a content package - optional

- a. Copy the files used for creating the monitor to the predefined content package subfolders:
 - o **<SiteScope>\packages\workspace\package_<Package ID>\lib**. (Optional) Copy any external jars used by the custom monitor script to this folder. Java classes from the jar files can be accessed from the data processing script. Note that you can use this monitor without external jars.

Note: In the data processing script, to import a package from a jar that does not start with `com.`, `org.`, or `java.`, you must add the package's prefix:

```
importPackage (Packages.<packageName>)
```

For example, `importPackage (Packages.it.companyname.test);`

For details on importing Java classes and packages, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

- o **<SiteScope>\packages\workspace\package_<>\classes**. (Optional) Copy the compiled Java classes with the entire package folder structure to this folder; this is not required if the class files were packaged in a jar that was copied to the **lib** folder. The class files can be accessed from the data processing script.
 - o **<SiteScope>\packages\workspace\package_<>\conf**. (Optional) Copy the configuration files, documentation, and XML files to this folder.
 - o **<SiteScope>\packages\workspace\package_<>\template**. (Optional) The folder should contain the template files exported from SiteScope (performed in "[Create a monitor template - optional](#)" on the previous page). Each template can contain various types of monitors; custom and regular.
- b. Copy extension files - optional

If the monitor references script or alert extension files in the SiteScope file system, copy them to the relevant folders in **<SiteScope root directory>\packages\workspace\extensions**:

- o **\scripts**. Used for storing script files that are used to run shell commands or other scripts on the machine where SiteScope is running.
- o **\scripts.remote**. Used for storing script files that are used for running a script that is stored on a remote machine.
- o **\templates.mail**. Used for storing the file containing the format and content of alert messages sent by email.
- o **\templates.mail.subject**. Used for storing the file containing the subject line of alert messages sent by email.

- **\templates.mib**. Used for storing the MIB files that are used to create a browsable tree that contains names and descriptions of the objects found during a traversal.
- **\templates.os**. Used for storing the shell commands to be run when monitoring remote UNIX servers.

Note:

- On exporting the files to a content package, the unique package ID is added to the script and template files as a suffix (before the file extension) in the **<SiteScope root directory>\packages\imported** directory, and under the relevant folder in the SiteScope root directory.
- As part of the import process, the **template.os** and **templates.mib** files are edited and the unique package ID is added to some properties inside the files.

- c. Export the content package to a zip file

Select the **Templates** context. In the template tree, right-click the template or template container that you want to export to a content package, and select **Export > Content Package**.

In the Export Content Package Wizard, enter details of the content package (manifest), and select the templates and files associated with these templates to include. For Wizard details, see Export Content Package Wizard.

Note: The Select Files page of the Wizard displays files from the **<SiteScope root directory>\packages\workspace\package_<Package ID>** and **<SiteScope root directory>\packages\workspace\extensions** folders listed above, except for the **\META-INF** and **\templates** folders which are not displayed.

11. Share the custom monitor with other SiteScope users - optional

You can distribute a content package zip file by:

- Sending it to individual SiteScope users.
- Sharing it with other SiteScope users by uploading it to the Community Content for SiteScope page on [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>). HP Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HP Software portfolio.

For task details, see How to publish content to the HP Live Network community.

How to Access the Monitor Configuration Parameters Exposed in the Script

Data Script:

- You can access the configuration parameters for custom monitors in the data script using:

```
myContext.getInputData().getConfigurationParameter(<config param name>);
```

Example:

```
var monitorName = myContext.getInputData().getConfigurationParameter("monitorName");
```

The following monitor properties are exposed to the script (for all custom monitors):

- `monitorName`. The name of the monitor.
- `monitorDescription`. A description of the monitor.

The following monitor properties are exposed to the script for the Custom Log File monitor only:

- `server`. The name of the server where the log file you want to monitor is located.
- `logFilePath`. The path of the monitor's log file.
- You can set the summary string which is used as the monitor status in the SiteScope Dashboard using:

```
myContext.getScriptResult().setSummary(<user's text summary>);
```

The default value is: `summary = <a set of metrics and their values>`

- You can set monitor availability which is displayed in the SiteScope Dashboard using:

```
myContext.getScriptResult().setAvailability(<true/false>)
```

The default value is: `availability = true`

Topology Script:

You can access the configuration parameters for custom monitors in the topology script using:

```
Framework.getDestinationAttributeAsObject("configuration").get("<configuration parameter name>")
```

To access data saved in the monitor storage (this is a place where you can save script data for use in future executions):

```
Framework.getDestinationAttributeAsObject("monitorStorage").get("<configuration parameter name>")
```

To access the list of metric names used in the script:

```
Framework.getDestinationAttributeAsObject("metrics")
```

How to Import and Use a Custom Log File Monitor

After developing a custom monitor and creating a content package zip file, the content package can then be sent to specific users, or be published to the [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>) community enabling other users to import the monitor for their own use.

For details on using the Wizard, see [Export Content Package Wizard](#).

1. Prerequisites

Only a SiteScope administrator user, or a user granted the **Add, edit or delete templates** permissions can import monitor templates from a content package. For details, see [Permissions](#) in the [Using SiteScope Guide](#).

2. Access the content package zip file

- If a content package zip file was sent to you, skip to the next step.
- If a content package was made available to the Community Content for SiteScope page on [HP Live Network](#), download the content package to your SiteScope machine. HP Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HP Software portfolio.

For task details, see How to download a template or content package from the HP Live Network in the Using SiteScope Guide.

3. Import the custom monitor content package

- a. In SiteScope, select the **Templates** context. In the template tree, right-click the template container into which you want to import the content package, and click **Import**.
- b. In the Content Import dialog box, select **Content package**, and click the **Browse** button. Navigate to the folder containing the package you want to import (packages are distributed in zip format). Click **Open**, and then click **OK**.

For details on the Content Import dialog box, see Content Import Dialog Box in the Using SiteScope Guide.

4. Verify the template was imported successfully by checking it was added to the template tree

The content package is copied to the **<SiteScope root directory>\packages\imported** folder, and a new folder is created with the name: **<Package/Zip Name>.zip_<Package ID>**.

The folder contains:

- **\META-INF**. Contains the manifest file where information about the content package is stored.
- **\templates**. Contains files from which templates in this content package were imported into SiteScope.
- **<Package/Zip Name>**. Uncompressed package that contains the above-mentioned folders, the **\extensions** folder which contains script and alert template files referenced by monitors in the imported templates, and the folders used for Custom monitors:
 - **\classes**. Used for storing compiled Java classes.
 - **\conf** Used for storing configuration files, documentation, and XML files.
 - **\lib** Used for storing external jar files used by the monitor script. Note that the **\lib** folder is shared between all monitors imported in the same template.
- **<Package/Zip Name>.zip.properties**. This is the descriptor (manifest) file for content packages created in SiteScope 11.20, that is used in case of rollback, uninstall, or upgrade. The file contains the ID of the SiteScope template that was deployed, the location of the files in SiteScope, and other information about the content package.

The imported templates and dependency files can be used directly or modified as required.

Where script or alert templates are referenced in the user interface, the unique package ID is added as a suffix.

Example: ShortMail alert action template referenced in the Template field.

Action Type Settings	
Action name:	EMail
* Recipients:	Default
Addresses:	
* Subject:	Typical
* Template:	ShortMail_06b62f60-807c-4102-adea-9a7ebdd80e8b

5. Deploy the custom monitor template

After importing the custom monitor template, you can deploy the template to a group.

- In the template tree, right-click the custom monitor template you want to deploy, and select **Deploy Template**.
- In the Select Group dialog box, select a group into which you want to deploy the template. Alternatively, you can click the **New Group** button and create a new group to which you can deploy the template. For user interface details, see Select Group Dialog Box in the Using SiteScope Guide.
- In the Deployment Values dialog box, enter the required variable values in the entry boxes displayed, and click **OK**. The entry boxes displayed correspond to the template variables used in the template objects. For user interface details, see Deployment Values Dialog Box in the Using SiteScope Guide.

Note: When deploying the template or publishing changes in the template to deployed groups, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, since the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.

- Verify that the template was deployed successfully (the template objects should be added to the specified group in the monitor tree).

For task details, see How to Deploy Templates Using the User Interface in the Using SiteScope Guide.

6. Configure monitor status thresholds

When deploying the template, only the default metrics included with the monitor are displayed (custom metrics defined in the script do not exist until after the monitor has run).

After the monitor run, you can define thresholds for metrics that were resolved in the run. In the **Threshold Settings** panel of the custom monitor, select metrics for which you want to define thresholds in the **Condition** column by using variables or free text, or selecting default metrics from the drop-down list, and enter the value applicable to the metric parameter.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Custom Log File Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Server	<p>Server where the file you want to monitor is located. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note: If using NetBIOS to connect to other servers in an Windows domain, use the UNC format to specify the path to the remote log file. For example, \\lab_machine\users\SiteScopes\Version_11.2\Build_2000\SiteScope.</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> • Browse servers. Select a server from the drop-down list of servers visible in the local domain. • Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Log file path	<p>Path to the log file you want to monitor.</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 the UNIX user account being used to log on to the remote machine.• Remote Windows through NetBIOS. For reading log files on remote Windows servers using the NetBIOS method, use UNC to specify the path to the remote log file. Example: <code>\\remoteserver\sharedfolder\filename.log</code>• Remote Windows through SSH. For reading log files on remote Windows servers using the SSH method, specify the local path of the remote log file on the remote machine. Example: <code>C:\Windows\System32\filename.log</code> 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 <i>How to Configure SiteScope to Monitor a Remote Microsoft Windows Server</i> in the <i>Using SiteScope Guide</i>. <p>You can also monitor files local to the server where SiteScope is running. Example: <code>C:\application\appLogs\access.log</code></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 <i>SiteScope Date Variables</i> in the <i>Using SiteScope Guide</i>.</p>

UI Element	Description
Run alerts	<p>Method for running alerts for this monitor.</p> <ul style="list-style-type: none"> • For each log entry matched. The monitor triggers alerts according to thresholds applied to each matching entry found. Since status can change according to thresholds for each matched entry, each alert action could be triggered many times within a monitor run. <p>Example: If you want to send a warning alert on matched text value "power off" and an error alert if more than one server is turned off, set the following thresholds:</p> <ul style="list-style-type: none"> ▪ <code>Error if matchCount > 1</code> ▪ <code>Warning if value == 'power off'</code> <p>To send an error alert if only one threshold is matched, set <code>Error if value == 'power off'</code>.</p> <p>For details on how to create a Custom Log File monitor that triggers customized alerts for content matches, see "Customizing Custom Log File Content Matches and Monitor Alerts" on page 119.</p> <ul style="list-style-type: none"> • Once, after all log entries have been checked. 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 metric, an alert is not triggered.</p>
Check from beginning	<p>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>
Content match	<p>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 Custom 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 Regular Expressions Overview in the Using SiteScope Guide.</p>

UI Element	Description
Open Tool	Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.
Advanced Settings	
Log file encoding	<p>If the log file content to be monitored uses an encoding that is different than the encoding used on the server where SiteScope is running, select 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>Default value: windows-1252</p>
Rules file path	<p>Enter the full path to your rules file. In special cases, it may be necessary to create a custom rules file to specify different alerts for different log entry matches. You can also set a parameter in the rules file to run script alerts. You can use any of the properties in the SiteScope Alert Template and Event Properties Directory.</p> <p>An example rules file is located in <SiteScope root directory>\examples\log_monitor\sample.rules. For instructions on how to use the file and example rules, see "How to Use the Rules File" on page 323, or read the instructions in the file itself.</p>
Match value labels	<p>Use to enter 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 Data Processing Script. Separate multiple labels with a comma (,).</p> <p>Note: If match value labels are not used, the matched values are named <code>value1</code>, <code>value2</code>, and so forth.</p>
Multi-line match	<p>Runs a regular expression match on multiple lines of text.</p> <p>Default value: Not selected</p>

UI Element	Description
Server-side processing	<p>Processes log file data on the server-side. Benefits include low memory usage and low CPU utilization on the SiteScope server, and faster monitor run. Server-side processing does however cause high CPU utilization on the remote server when processing the file.</p> <p>Default value: Not selected (we recommend using this option only if SiteScope performance is affected by large amounts of data being appended to the target log file between monitor runs, and the Log File monitor is performing badly in regular mode).</p> <p>Note:</p> <ul style="list-style-type: none"> • Server-side processing is available for remote Linux, Red Hat Enterprise Linux, and Oracle Solaris servers only. Windows SSH is not supported. • Rule files are not supported in this mode. • The encoding for the remote server must be Unicode, or match the encoding of the log file (if the remote file is in Unicode charset).
Return matching raw data from server-side	<p>Returns the whole row of raw data with matching patterns from the server-side when a match is found.</p> <p>Default value: Not selected</p> <p>Note: This setting is only available when Server-side processing is selected.</p>
No error if file not found	<p>Monitor remains in Good status if the file is not found. The monitor status remains Good regardless of the monitor threshold configuration.</p> <p>Default value: Not selected</p>
Timeout Settings	
Enable timeout	<p>The monitor stops its run after the specified timeout period has been exceeded.</p> <p>Default value: Not selected</p>
After timeout, resume reading from end of file	<p>If selected, the monitor resumes reading from the end of the log file during the next run, instead of from the current location.</p> <p>Default value: Not selected</p> <p>Note: This setting is only available when Enable timeout is selected.</p>
Status after timeout	<p>The status condition that the monitor goes into if the monitor times out.</p> <p>The status categories include: Error, Warning, Good</p> <p>Default value: Warning</p> <p>Note: This setting is only available when Enable timeout is selected.</p>

UI Element	Description
Timeout (seconds)	<p>Amount of time, in seconds, that SiteScope should wait before the monitor times out.</p> <p>Default value: 60 seconds</p> <p>Note: This setting is only available when Enable timeout is selected.</p>
Data Processing Script	
<Script>	<p>The input data for the data processing script is displayed in this box.</p> <p>Define the script that parses the results and creates new metrics. For details on the monitor configuration properties in the script, including how to access them, and the monitor storage and metrics names, see "How to Access the Monitor Configuration Parameters Exposed in the Script" on page 128.</p> <p>Note: By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the Maximum number of counters value in Preferences > Infrastructure Preferences > Custom Monitor Settings.</p>
Package path	<p>Path generated by SiteScope where the files used for developing the monitor can be saved. This enables you to add the jars on which the monitor depends (if applicable), classes, configuration, and templates files to the monitor. The path is displayed as read only.</p> <p>Click the Create Path button to create a folder with a relative path in the SiteScope root directory (<code>packages\workspace\package_<unique ID></code>). The path is displayed as read only.</p> <p>The folder contains the following subfolders into which you copy the files used to create the monitor:</p> <ul style="list-style-type: none"> • lib. (Optional) Used for storing external jar files used by the monitor script. Note that you can use this monitor without external jars. • classes. (Optional) Used for storing Java compiled classes; note that they should be copied with the entire package folder structure. • conf. (Optional) Used for storing configuration files, documentation, and XML files. • template. (Mandatory) Used for storing the template files that contain the custom monitor. It must contain at least one template. Each template can contain various types of monitors; custom and regular. <p>Note: This field is displayed when working in monitor mode only. When working in template mode and the monitor is deployed, the content pack is imported into the path.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section describes troubleshooting and limitations for the Custom Log File monitor.

- "General Tips/Limitations" below
- "Custom Monitor Logs" below

General Tips/Limitations

- If a user-defined or imported Java package has the same name as an existing SiteScope or standard Java package, SiteScope ignores the user-defined/imported Java package.
- When setting custom monitor metrics with a string (non-numeric) value, the maximum and average values in the Measurement Summary table of the Management Report are shown as 'n/a'. This also occurs if you change the metric value type, for example, if you set the metric with a numeric value, and later change it to a string value or vice versa.
- When deploying a custom monitor using a template, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, since the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.
- When publishing changes to a template that contains a custom monitor, we recommend using the **Disable custom monitors while publishing changes** option (selected by default) in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. The monitor is temporarily disabled before changes are published and is restored to the enabled state after changes have been made.
- Setting status thresholds using a baseline is not supported on user-defined metrics.
- This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see "[How to Configure the HP NonStop Resources Monitor](#)" on page 282.
- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When monitoring a log file on a FreeBSD remote server, make sure the correct path to the "cat" command is used in **<SiteScope root directory>\templates.os\FreeBSD.config**, since the command was moved in the latest FreeBSD versions.

Custom Monitor Logs

- Errors in the monitor (including errors in the script) are written to the SiteScope logs in the same way as for any other monitor. Check the **error.log** and **RunMonitor.log** files.
- Error messages from the script are displayed in the **custom_monitor.log** file located in **<SiteScope root directory>\logs\custom_monitors**. This log can be used for info, warning, error, and debug messages from running the script.

To change the log level to **DEBUG** mode, in **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties**, change **\${loglevel}** to **DEBUG** in the following paragraph:

Monitor Reference

Chapter 15: Custom Log File Monitor

```
# Custom monitors category
log4j.category.CustomMonitor=${loglevel},custom.monitor.appender
log4j.additivity.CustomMonitor=false change
```

Chapter 16

Custom WMI Monitor

The Custom WMI monitor broadens the capabilities of monitors that support the Windows Management Instrumentation (WMI) method for collecting data by checking the availability and performance of management data on Windows-based operating systems. You can create your own WMI monitor by developing WMI Query Language (WQL) queries that collect data, and a script that processes the collected data and creates metrics. You can use Java code developed by yourself or by a third-party to process the data.

You can share custom monitors by publishing them to the HP Live Network community, enabling other SiteScope users to import the monitor template for their own use.

Tip: You can view guided and narrated demonstrations for using the WMI Custom monitor on the HP Videos channel on YouTube:

- Custom WMI Monitor Creation Process and Packaging - <http://youtu.be/bB6NITGdd88>
- Custom WMI Monitor Data Processing Script - <http://youtu.be/Glw3JVnunWE>

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **Custom WMI** monitor.

Learn More

Custom WMI Monitor Overview

The Custom WMI monitor enables you to develop your own monitors on top of the SiteScope infrastructure. This provides you with greater flexibility not available in existing monitors.

You can use the Custom WMI monitor to:

- **Collect any (WMI) data you like**

You can create a series of pre-defined WQL queries for the Windows operating systems you want to monitor. SiteScope runs the queries and returns the results to the monitor in an object that contains a set of results for each query. Each time the monitor runs, it re-runs your queries and collects fresh data.

- **Process the collected data**

You can create a script in the monitor that can extract and process the results of the collected data. For example, you can define metrics based on collected data from the Windows operating system or perform mathematical operations on it as in the sample script provided.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**).

- **Collect data dynamically**

You can include dynamically-defined queries in the data processing script. These queries are executed while the script is running, in contrast to predefined queries, which are executed before the script is run. Dynamically-executed queries provide the added benefit of enabling you to create queries based on values that are not in the monitored entity data store (for example, timestamp), create queries based on previous query results or calculations, and include variables in queries. For details, see Data Processing Script with Dynamic Queries in the Using SiteScope Guide.

After developing the monitor, you can:

- **Define thresholds for new metrics**

After the first monitor run, you can define thresholds for metrics that were defined in the script, since these custom metrics did not exist before the first run. This provides more advanced data processing options than regular monitors. Note that metrics can change between script runs, for example, where variables are used in metric names. Thresholds using a metric that does not exist after the monitor run are removed automatically.

- **Share the monitor with other SiteScope users**

After developing the monitor, you can export the monitor to a template, add external jars and/or classes if the monitor depends on them, and create a content package. The content package can then be sent to specific users, or shared with other SiteScope users by publishing it to the SiteScope community on [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>).

By sharing knowledge with other SiteScope users, you can benefit from extended SiteScope monitor coverage and the development of new monitors outside the SiteScope release cycle.

Tasks

This section includes:

- "How to Develop the Custom WMI Monitor" below
- "How to Access the Monitor Configuration Parameters Exposed in the Script" on page 148
- "How to Import and Use a Custom WMI Monitor" on page 149

How to Develop the Custom WMI Monitor

1. Prerequisites

- You should be an advanced SiteScope user with knowledge of writing scripts in JavaScript, and have knowledge of WMI and WQL.
- The following are requirements for using SiteScope to collect performance measurements on a remote machine using WMI:
 - The WMI service must be running on the remote machine. For details, refer to the Windows Management Instrumentation documentation ([http://msdn.microsoft.com/en-us/library/aa826517\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa826517(VS.85).aspx)).
 - The user defined for the WMI remote server must have permissions to read statistics remotely from any name space that they use in the queries. For details, refer to <http://support.microsoft.com/kb/295292>.

For information about troubleshooting WMI service problems, see "Tips/Troubleshooting" on page 155.

2. Create a Custom WMI monitor with the relevant queries

- a. Create a group into which you want to add the custom monitor. Right-click the group, select **New > Monitor**, and select the **Custom WMI** monitor.
- b. In the **General Settings** panel, enter a name and description for the monitor.
- c. In the **Custom WMI Monitor Settings** panel, select the server that you want to monitor (only those Windows remote servers configured with a WMI connection are available).
- d. In the WMI queries table, enter the WQL queries and the WMI namespace on which you want to perform the queries.

Tip: By default, you can enter up to 10 queries in the table. You can modify the number of queries that can be added to the table in **Preferences > Infrastructure Preferences > Custom Monitor Settings** by configuring the **Maximum number of queries** value.

For user interface details, see the UI Descriptions section below.

Example

These queries collect processor performance and memory data from the monitored server.

No.	Queries	Namespace
0	Select PercentProcessorTime,Timestamp_Sys100NS From Win32_PerfRawData_PerfOS_Processor	root\cimv2
1	Select PercentProcessorTime,Timestamp_Sys100NS From Win32_PerfRawData_PerfOS_Processor	root\cimv2

3. Create the data processing script

In the **Data Processing Script** area of Custom WMI Monitor Settings, create the script that parses the results and creates new metrics according to the name that you determined.

In addition, you can include any number of queries in the script. The queries are executed as the script is run, which means that the monitor collects fresh data from the Windows operating system being monitored. After the data is retrieved, it becomes available for the script to use. A query in a script has the same syntax as a query defined in the queries table, but it can be structured using variables which makes it dynamic within the monitor run context. For details on dynamic queries, see Data Processing Script with Dynamic Queries in the Using SiteScope Guide.

For details on the monitor configuration properties, including how to access them, and the monitor storage and metrics names, see "[How to Access the Monitor Configuration Parameters Exposed in the Script](#)" on page 148.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**). A sample jar file showing the custom monitor's capability to access Java code is provided in the **<SiteScope root directory>\examples\monitors\custom\lib** folder.

For details on scripting in Java, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

Tip:

- A sample Custom WMI monitor script is provided in the **Data Processing Script** box. To use it, you need to uncomment the script.
- Sample scripts for all the custom monitors are available from the sample content package located in the **<SiteScope installation directory>\examples\monitors\custom** folder. **CustomMonitorSamplePackage.zip** contains examples for SiteScope 11.20, and **CustomMonitorsExamples_11_21.zip** contains updated examples including a Custom Database monitor with a dynamic query, a manifest file created using the Export Content Package Wizard, and template mail and template mail subject files. To use these scripts, you need to import the custom monitor content package and then deploy the custom monitor template. For task details, see steps 3 and 4 of "[How to Import and Use a Custom WMI Monitor](#)" on page 149.

Note:

- If your monitor needs to open a network connection to another server from the data processing script or the Java code that is called from the script, you must enable the **Allow network access** setting in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- Access for the data processing script is restricted to the following folders/files on the SiteScope server:
 - The `\conf` folder which is located inside each content package (`<SiteScope root directory>\packages\imported` or `<SiteScope root directory>\packages\workspace`) (requires *Read* permissions).
 - `<SiteScope root directory>\logs\custom_monitors*` (all permissions)
- You can use the `custom_monitor.log` file for any info, warning, error, and debug messages that you want to write during the execution of the script. The log is located in `<SiteScope root directory>\logs\custom_monitors`. For details on changing the log to DEBUG mode, see "Custom Monitor Logs" on page 155.
- By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the **Maximum number of counters** value in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- When working in template mode, you can use template variables in a data processing script.

4. **Generate a path for storing the files used for creating the Custom WMI monitor**

Click the **Create Path** button to create a folder where the relevant jars, classes, configuration, and template files required for running the monitor can be saved. A folder with a relative path is created under `<SiteScope root directory>\packages\workspace\package_<Package ID>`. The path is displayed as read only.

The folder contains the following (empty) subfolders:

- `packages\workspace\package_<>\lib`. Used for storing external jar files used by the monitor script.
- `packages\workspace\package_<>\classes`. Used for storing compiled Java classes; note that they should be copied with the entire package folder structure.
- `packages\workspace\package_<>\conf`. Used for storing configuration files, documentation, and XML files.
- `packages\workspace\package_<>\template`. Used for storing the template files that contain the custom monitor (you perform this in "Custom WMI Monitor" on page 141).

You can copy the required files to these folders at this stage, or when performing "Custom WMI Monitor" on page 141.

Note: If you add or modify jars/classes after the first monitor run, you must either:

- Restart SiteScope for the changes to take effect, or
- To avoid having to restart SiteScope, you must enable the **Reload classes and jars on each monitor run** option in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.

5. **Configure topology reporting - optional**

To report monitor and related CI topology data to BSM's RTSM, configure the required topology reporting settings as described in How to Configure Topology Reporting for a Custom Monitor in the Using SiteScope Guide.

6. **Configure other settings for the monitor - optional**

Configure other settings for the monitor as required. For details, see Common Monitor Settings in the Using SiteScope Guide.

7. **Save the monitor and wait for the first monitor run**

Save the monitor. SiteScope verifies the correctness of the monitor configuration locally and on the remote server to be monitored, before saving the settings, regardless of whether you click the **Verify & Save** or **Save** button.

The monitor collects data from the Windows operating system, and filters the data based on the script you supplied.

8. **Define thresholds for the metrics - optional**

After the monitor has run, you can:

- Make changes to the script and define thresholds for metrics that were created or updated in the run. For details, see Threshold Settings in the Using SiteScope Guide.
- Check status and values of the metrics in the SiteScope Dashboard.
- Set up alerts on the monitor. For details, see How to Configure an Alert in the Using SiteScope Guide.

9. **Create a monitor template - optional**

- a. To copy the monitor to a template, right-click the monitor, select **Copy to Template**, and select the template group to which you want to add the copied configuration. For details, see How to Create a Template by Copying Existing Configurations in the Using SiteScope Guide.
- b. Make any necessary changes such as adding template variables to the template. For details on template variables, see New Variable Dialog Box.

10. **Create a content package - optional**

- a. Copy the files used for creating the monitor to the predefined content package subfolders:
 - **<SiteScope>\packages\workspace\package_<Package ID>\lib**. (Optional) Copy any external jars used by the custom monitor script to this folder. Java classes from the jar files can be accessed from the data processing script. Note that you can use this monitor without external jars.

Note: In the data processing script, to import a package from a jar that does not start with `com.`, `org.`, or `java.`, you must add the package's prefix:

```
importPackage (Packages.<packageName>)
```

For example, `importPackage (Packages.it.companyname.test);`

For details on importing Java classes and packages, see

<http://www.mozilla.org/rhino/ScriptingJava.html>.

- **<SiteScope>\packages\workspace\package_<>\classes.** (Optional) Copy the compiled Java classes with the entire package folder structure to this folder; this is not required if the class files were packaged in a jar that was copied to the `\lib` folder. The class files can be accessed from the data processing script.
 - **<SiteScope>\packages\workspace\package_<>\conf.** (Optional) Copy the configuration files, documentation, and XML files to this folder.
 - **<SiteScope>\packages\workspace\package_<>\template.** (Optional) The folder should contain the template files exported from SiteScope (performed in "Custom WMI Monitor" on page 141). Each template can contain various types of monitors; custom and regular.
- b. Copy extension files - optional

If the monitor references script or alert extension files in the SiteScope file system, copy them to the relevant folders in **<SiteScope root directory>\packages\workspace\extensions>**:

- **\scripts.** Used for storing script files that are used to run shell commands or other scripts on the machine where SiteScope is running.
- **\scripts.remote.** Used for storing script files that are used for running a script that is stored on a remote machine.
- **\templates.mail.** Used for storing the file containing the format and content of alert messages sent by email.
- **\templates.mail.subject.** Used for storing the file containing the subject line of alert messages sent by email.
- **\templates.mib.** Used for storing the MIB files that are used to create a browsable tree that contains names and descriptions of the objects found during a traversal.
- **\templates.os.** Used for storing the shell commands to be run when monitoring remote UNIX servers.

Note:

- On exporting the files to a content package, the unique package ID is added to the script and template files as a suffix (before the file extension) in the **<SiteScope root directory>\packages\imported** directory, and under the relevant folder in the SiteScope root directory.

- As part of the import process, the **template.os** and **templates.mib** files are edited and the unique package ID is added to some properties inside the files.

- c. Export the content package to a zip file

Select the **Templates** context. In the template tree, right-click the template or template container that you want to export to a content package, and select **Export > Content Package**.

In the Export Content Package Wizard, enter details of the content package (manifest), and select the templates and files associated with these templates to include. For Wizard details, see Export Content Package Wizard.

Note: The Select Files page of the Wizard displays files from the **<SiteScope root directory>\packages\workspace\package_<Package ID>** and **<SiteScope root directory>\packages\workspace\extensions>** folders listed above, except for the **\META-INF** and **\templates** folders which are not displayed.

11. Share the custom monitor with other SiteScope users - optional

You can distribute a content package zip file by:

- Sending it to individual SiteScope users.
- Sharing it with other SiteScope users by uploading it to the Community Content for SiteScope page on [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>). HP Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HP Software portfolio.

For task details, see How to publish content to the HP Live Network community.

How to Access the Monitor Configuration Parameters Exposed in the Script

Data Script:

- You can access the configuration parameters for custom monitors in the data script using:

```
myContext.getInputData().getConfigurationParameter("<configuration parameter name>");
```

Example:

```
var monitorName = myContext.getInputData().getConfigurationParameter("monitorName");
```

The following monitor properties are exposed to the script (for all custom monitors):

- `monitorName`. The name of the monitor.
- `monitorDescription`. A description of the monitor.

The following monitor properties are exposed to the script for the Custom WMI monitor only:

- `server`. The name of the server from which you want to collect the data.

- You can set the summary string which is used as the monitor status in the SiteScope Dashboard using:

```
myContext.getScriptResult().setSummary(<user's text summary>);
```

The default value is: `summary = <a set of metrics and their values>`

- You can set monitor availability which is displayed in the SiteScope Dashboard using:

```
myContext.getScriptResult().setAvailability(<true/false>)
```

The default value is: `availability = true`

Topology Script:

You can access the configuration parameters for custom monitors in the topology script using:

```
Framework.getDestinationAttributeAsObject("configuration").get("<configuration parameter name>")
```

To access data saved in the monitor storage (this is a place where you can save script data for use in future executions):

```
Framework.getDestinationAttributeAsObject("monitorStorage").get("<configuration parameter name>")
```

To access the list of metric names used in the script:

```
Framework.getDestinationAttributeAsObject("metrics")
```

How to Import and Use a Custom WMI Monitor

After developing a custom monitor and creating a content package zip file, the content package can then be sent to specific users, or be published to the [HP Live Network](https://hpln.hp.com/group/sitescope) (<https://hpln.hp.com/group/sitescope>) community enabling other users to import the monitor for their own use.

For details on using the Wizard, see [Export Content Package Wizard](#).

1. Prerequisites

Only a SiteScope administrator user, or a user granted the **Add, edit or delete templates** permissions can import monitor templates from a content package. For details, see [Permissions](#) in the [Using SiteScope Guide](#).

2. Access the custom monitor content package zip file

- If a content package zip file was sent to you, skip to the next step.
- If a content package was made available to the Community Content for SiteScope page on [HP Live Network](#), download the content package to your SiteScope machine. HP Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HP Software portfolio.

For task details, see [How to download a template or content package from the HP Live Network](#) in the [Using SiteScope Guide](#).

3. Import the custom monitor content package

- a. In SiteScope, select the **Templates** context. In the template tree, right-click the template

container into which you want to import the content package, and click **Import**.

- b. In the Content Import dialog box, select **Content package**, and click the **Browse** button. Navigate to the folder containing the package you want to import (packages are distributed in zip format). Click **Open**, and then click **OK**.

For details on the Content Import dialog box, see Content Import Dialog Box in the Using SiteScope Guide.

4. **Verify the template was imported successfully by checking it was added to the template tree**

The content package is copied to the **<SiteScope root directory>\packages\imported** folder, and a new folder is created with the name: **<Package/Zip Name>.zip_<Package ID>**.

The folder contains:

- **\META-INF**. Contains the manifest file where information about the content package is stored.
- **\templates**. Contains files from which templates in this content package were imported into SiteScope.
- **<Package/Zip Name>**. Uncompressed package that contains the above-mentioned folders, the **\extensions** folder which contains script and alert template files referenced by monitors in the imported templates, and the folders used for Custom monitors:
 - **\classes**. Used for storing compiled Java classes.
 - **\conf** Used for storing configuration files, documentation, and XML files.
 - **\lib** Used for storing external jar files used by the monitor script. Note that the **\lib** folder is shared between all monitors imported in the same template.
- **<Package/Zip Name>.zip.properties**. This is the descriptor (manifest) file for content packages created in SiteScope 11.20, that is used in case of rollback, uninstall, or upgrade. The file contains the ID of the SiteScope template that was deployed, the location of the files in SiteScope, and other information about the content package.

The imported templates and dependency files can be used directly or modified as required.

Where script or alert templates are referenced in the user interface, the unique package ID is added as a suffix.

Example: ShortMail alert action template referenced in the Template field.

Action Type Settings	
Action name:	EMail
* Recipients:	Default
Addresses:	
* Subject:	Typical
* Template:	ShortMail_06b62f60-807c-4102-adea-9a7ebdd80e8b

5. Deploy the custom monitor template

After importing the custom monitor template, you can deploy the template to a group.

- a. In the template tree, right-click the custom monitor template you want to deploy, and select **Deploy Template**.
- b. In the Select Group dialog box, select a group into which you want to deploy the template. Alternatively, you can click the **New Group** button and create a new group to which you can deploy the template. For user interface details, see Select Group Dialog Box in the Using SiteScope Guide.
- c. In the Deployment Values dialog box, enter the required variable values in the entry boxes displayed, and click **OK**. The entry boxes displayed correspond to the template variables used in the template objects. For user interface details, see Deployment Values Dialog Box in the Using SiteScope Guide.

Note: When deploying the template or publishing changes in the template to deployed groups, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, since the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.

- d. Verify that the template was deployed successfully (the template objects should be added to the specified group in the monitor tree).

For task details, see How to Deploy Templates Using the User Interface in the Using SiteScope Guide.

6. Configure monitor status thresholds

When deploying the template, only the default metrics included with the monitor are displayed (custom metrics defined in the script do not exist until after the monitor has run).

After the monitor run, you can define thresholds for metrics that were resolved in the run. In the **Threshold Settings** panel of the custom monitor, select metrics for which you want to define thresholds in the **Condition** column by using variables or free text, or selecting default metrics from the drop-down list, and enter the value applicable to the metric parameter.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Custom WMI Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Server	<p>Name of the server that you want to monitor. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope with a WMI connection are displayed). Alternatively, click the Add Remote Server button to add a new server.</p> <p>Note: When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p>
Add Remote Server	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see "New/Edit Microsoft Windows Remote Server Dialog Box" in the Using SiteScope Guide.</p> <p>Note: In the Add Microsoft Windows Remote Server dialog box, the Method field is automatically set to WMI (and cannot be changed), since this monitor can only use a Windows remote server configured with a WMI connection.</p>
WMI queries table	
	New query. Adds a new line to the WMI queries table, enabling you to enter a new query.
	Edit query. Opens the Query Editor, in which the selected WMI query is displayed and can be edited.
	Delete query. Enables you to delete the selected query.
No	<p>The query number. By default, you can add up to 10 queries to the table. The queries are run in the order in which they appear in the table.</p> <p>Note: You can modify the number of queries that can be added to the table by changing the Maximum number of queries value in Preferences > Infrastructure Preferences > Custom Monitor Settings.</p>
Queries	<p>Enter the WMI query you want to use. You can create or edit a query in the table (in line mode), or in the Query Editor. To open the Query Editor, click the Edit query button. It is recommended to use the Query Editor when adding or viewing long queries.</p>

UI Element	Description
Namespace	<p>Enter the WMI namespace on which you want to perform the WQL query. Each namespace holds classes that expose different types of information.</p> <p>Example: root\cimv2</p>
Data Processing Script	
<Script>	<p>The input data for the data processing script is displayed in this box.</p> <p>Define the script that parses the results and creates new metrics. For details on the monitor configuration properties in the script, including how to access them, and the monitor storage and metrics names, see "How to Access the Monitor Configuration Parameters Exposed in the Script" on page 148.</p> <p>Note: By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the Maximum number of counters value in Preferences > Infrastructure Preferences > Custom Monitor Settings.</p>
Package path	<p>Path generated by SiteScope where the files used for developing the monitor can be saved. This enables you to add the jars on which the monitor depends (if applicable), classes, configuration, and templates files to the monitor. The path is displayed as read only.</p> <p>Click the Create Path button to create a folder with a relative path in the SiteScope root directory (<code>packages\workspace\package_<unique ID></code>). The path is displayed as read only.</p> <p>The folder contains the following subfolders into which you copy the files used to create the monitor:</p> <ul style="list-style-type: none"> • lib. (Optional) Used for storing external jar files used by the monitor script. Note that you can use this monitor without external jars. • classes. (Optional) Used for storing Java compiled classes; note that they should be copied with the entire package folder structure. • conf. (Optional) Used for storing configuration files, documentation, and XML files. • template. (Mandatory) Used for storing the template files that contain the custom monitor. It must contain at least one template. Each template can contain various types of monitors; custom and regular. <p>Note: This field is displayed when working in monitor mode only. When working in template mode and the monitor is deployed, the content pack is imported into the path.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section describes troubleshooting and limitations for the Custom WMI monitor.

- "General Tips/Limitations" below
- "Monitor Specific Tips/Limitations" below
- "Custom Monitor Logs" below

General Tips/Limitations

- If a user-defined or imported Java package has the same name as an existing SiteScope or standard Java package, SiteScope ignores the user-defined/imported Java package.
- When setting custom monitor metrics with a string (non-numeric) value, the maximum and average values in the Measurement Summary table of the Management Report are shown as 'n/a'. This also occurs if you change the metric value type, for example, if you set the metric with a numeric value, and later change it to a string value or vice versa.
- When deploying a custom monitor using a template, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, since the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.
- When publishing changes to a template that contains a custom monitor, we recommend using the **Disable custom monitors while publishing changes** option (selected by default) in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. The monitor is temporarily disabled before changes are published and is restored to the enabled state after changes have been made.
- Setting status thresholds using a baseline is not supported on user-defined metrics.

Monitor Specific Tips/Limitations

- SiteScope does not support WMI event handling or WMI method execution.
- It is not recommended to have more than 4000 monitors using WMI.
- When a metric or object is shared between resources, SiteScope is unable to receive data for the metrics and the query fails. If other metrics are referenced in the same query, they also fail to receive data. For details and troubleshooting information, refer to <http://support.microsoft.com/kb/836802>.
- If running a dynamic query from within a data processing script fails, an exception is thrown.
- Due to a WMI Interface problem on Microsoft Windows Server 2003, the Custom WMI monitor is unable to get the correct values for **CurrentClockSpeed** and **MaxClockSpeed** from WMI namespace when SiteScope is running on a Windows Server 2003 platform.

Custom Monitor Logs

- Errors in the monitor (including errors in the script) are written to the SiteScope logs in the same way as for any other monitor. Check the **error.log** and **RunMonitor.log** files.
- Error messages from the script are displayed in the **custom_monitor.log** file located in **<SiteScope root directory>\logs\custom_monitors**. This log can be used for info, warning,

error, and debug messages from running the script.

To change the log level to **DEBUG** mode, in **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties**, change **\${loglevel}** to **DEBUG** in the following paragraph:

```
# Custom monitors category
```

```
log4j.category.CustomMonitor=${loglevel},custom.monitor.appender
```

```
log4j.additivity.CustomMonitor=false change
```

Chapter 17

Database Counter Monitor

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 enables you to watch server loading for performance, availability, and capacity planning. The error and warning thresholds for the monitor can be set on one or more database server performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Database Counter monitor.

Learn More

This section includes:

- "Supported Versions" below
- "Setup Requirements and User Permissions" below
- "IPv6 Addressing Supported Protocols" on page 160
- "Database Counter Topology" on page 160

Supported Versions

This monitor supports monitoring on any database with a valid JDBC driver that supports SQL queries.

Setup Requirements and User Permissions

The following are several key requirements for using the Database Counter 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. If the file is in zip format, unzip the contents to a temporary directory. 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.mercury.jdbc.sqlserver.SQLServerDriver**. DataDirect driver from DataDirect Technologies. It is a driver for those Microsoft SQL databases that use Windows authentication. For details on installing the driver, see the note below.

Note: To install the MSSQL JDBC driver:

- 1). Download the MSSQL JDBC driver from the [Microsoft Download Center](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2505) (<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2505>), and unzip the contents to a temporary directory.
- 2). Copy the **sqljdbc4.jar** file to the **<SiteScope root directory>\WEB-INF\lib** subdirectory.
- 3). Restart the SiteScope service.
- 4). Use the Database Connection Tool for connection tuning:
Database Connection URL: `jdbc:sqlserver://<IP Address>:<port>;InstanceName=<name>;DatabaseName=<name>`
Database Driver: `com.microsoft.sqlserver.jdbc.SQLServerDriver`
- 5). Create the desired database monitor type.

- **com.mercury.jdbc.oracle.OracleDriver**. A driver for Oracle databases. This driver is deployed with SiteScope. When using the driver, the database connection URL has the form of: `jdbc:mercury:oracle://<server name or IP address>:<database server port>;sid=<sid>`

- **oracle.jdbc.driver.OracleDriver.** SiteScope supports the following categories of JDBC driver that are supplied by Oracle:
 - JDBC thin driver for Oracle 7 and 8 databases.
 - JDBC OCI (thick) driver. For details on accessing Oracle databases using OCI driver, see ["How to access Oracle databases using OCI driver"](#) on page 161.
- **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: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.
- Database drivers that have timeout problems (where database queries processed with these drivers exceed the timeout specified in the monitor's **Query timeout** field) can be specified in the **Timeout proxied query drivers list** field (in **Preferences > Infrastructure Preferences > General Settings**). These drivers are queried separately with a monitor-based timeout.
- 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.

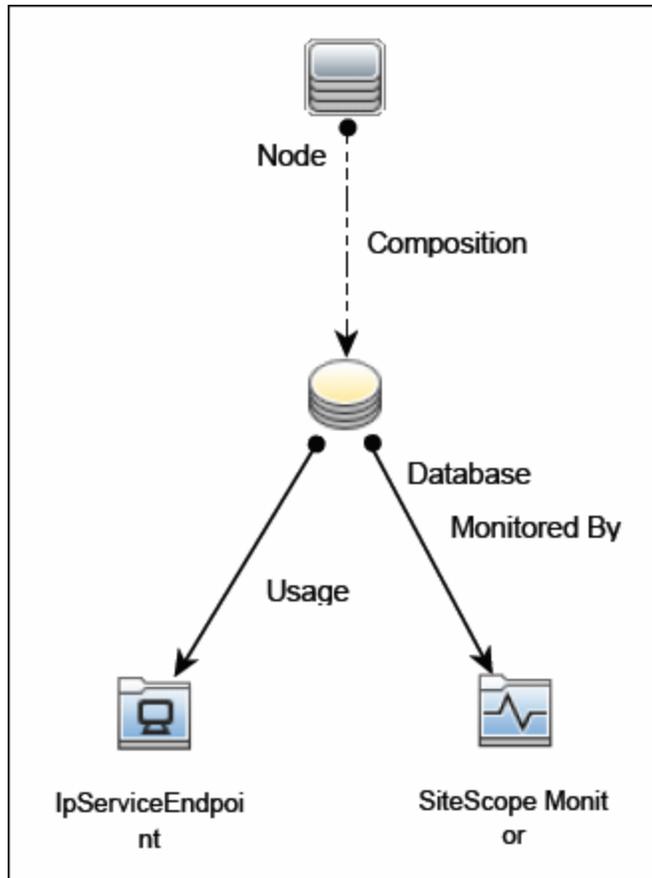
IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the TCP (JDBC) protocol. Support for IPv6 might also depend on the JDBC driver being used.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Database Counter Topology

The Database Counter monitor can identify the topology of the database system being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

Tasks

This section includes:

- "How to Configure the Database Counter Monitor" below
- "How to access Oracle databases using OCI driver" below

How to Configure the Database Counter Monitor

1. Prerequisites

Before configuring the monitor, make sure you have the necessary "Setup Requirements and User Permissions" on page 158.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Database Connection Tool** is available when configuring this monitor to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Database Connection Tool in the Using SiteScope Guide.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "Database Counter Topology" on the previous page.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

How to access Oracle databases using OCI driver

You can monitor an Oracle database using an OCI driver. If the port or SID are changed, you only need to make the change in the **tnsnames.ora** file (the SiteScope Oracle monitors remain unchanged).

1. On the SiteScope server, install the version of Oracle client that you are using.
2. Connect to the Oracle database using the Oracle OCI driver.
 - Set **ORACLE_HOME** environment variable (**ORACLE_HOME** is the folder where the Oracle client or database has been installed).
 - Add **ORACLE_HOME\lib** to System PATH (on Windows platforms), or **LD_LIBRARY_PATH** env variable (on UNIX platforms).
 - Set **CLASSPATH** environment variable to use Oracle JDBC driver from **ORACLE_HOME\jdbc\lib**.
3. In the `\oracle\oraX\network\admin\tnsnames.ora` file, configure the service name. You can test this using a SQL+ tool or the SiteScope Database Connection tool (see Database

Connection Tool in the Using SiteScope Guide).

4. Add a database monitor within SiteScope, and configure the following settings in the Monitor Settings panel:
 - **Database connection URL:** `jdbc:oracle:oci8:@<service name>`
 - **Database driver:** `oracle.jdbc.driver.OracleDriver`
 - Enter the database user credentials in the **Database user name** and **Database password** boxes

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Database Counter Monitor Settings

User interface elements are described below:

UI Element	Description
Database connection URL	<p>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 the (@) symbols must be included as shown.</p> <p>Note for using Windows Authentication: If you want to access the database using Windows authentication, enter <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>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 driver	<p>Driver used to connect to the database.</p> <p>Example: <code>org.postgresql.Driver</code></p> <p>Tip: You can specify database drivers that have timeout problems (where database queries processed with these drivers exceed the timeout specified in the monitor's Query timeout field) in the Timeout proxied query drivers list field (in Preferences > Infrastructure Preferences > General Settings). These drivers are queried separately with a monitor-based timeout.</p>
Database machine name	<p>Identifier for the target database server, as it should be reported to BSM.</p> <p>Note: This field is used only for topology reporting.</p>
Database port	<p>Port number, for the target database server, as it should be reported to BSM. You can specify the port manually. If none is specified, the monitor attempts to detect the port from the database connection URL. If it fails, topology is still reported, just without <code>IpServiceEndpoint</code>.</p> <p>Note: This field is used only for topology reporting.</p>

UI Element	Description
Database instance name	<p>Name of the database instance, as it should be reported to BSM.</p> <p>For SQL servers, the monitor automatically detects and populates this field from the database connection URL.</p> <p>For Oracle, the monitor automatically detects the instance name from the database connection URL without populating the field.</p> <p>If the field is empty and auto detection fails, no topology is reported and the default CI type Node is displayed in the HP Integration Settings panel.</p> <p>Note: This field is used only for topology reporting.</p>
Divisor query	<p>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>
No cumulative counters	<p>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).</p>
Credentials	<p>Option for providing the user name and password to be used to access the database server:</p> <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
No divide counters	<p>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.</p> <p>The divisor is either taken from the Divisor Query, or it is the elapsed time in seconds since the previous monitor run.</p>
Counters	<p>Server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p>Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

UI Element	Description
<p>Database Connection Settings</p> <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 enter. 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 and 9.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>	
<p>Use connection pool</p>	<p>Enables SQL connection sharing. 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>
<p>Physically close if idle connection count exceeds</p>	<p>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>
<p>Idle connection timeout</p>	<p>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>
<p>Query timeout</p>	<p>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>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- 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. For details, see JDBC Global Options in the Using SiteScope Guide.

Chapter 18

Database Query Monitor

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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Database Query monitor.

Learn More

This section includes:

- "Supported Versions" below
- "What to Monitor" below
- "Setup Requirements and User Permissions" below
- "IPv6 Addressing Supported Protocols" on page 170

Supported Versions

This monitor supports monitoring on any database with a valid JDBC driver that supports SQL queries.

What to Monitor

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 and User Permissions

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. If the file is in zip format, unzip the contents to a temporary directory. 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.mercury.jdbc.sqlserver.SQLServerDriver**. DataDirect driver from DataDirect Technologies. It is a driver for those Microsoft SQL databases that use Windows authentication. For details on installing the driver, see the note below.

Note: To install the MSSQL JDBC driver:

- 1). Download the MSSQL JDBC driver from the [Microsoft Download Center](#)

(<http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=11774>), and unzip the contents to a temporary directory.

2). Copy the **sqljdbc4.jar** file to the **<SiteScope root directory>\WEB-INF\lib** subdirectory.

3). Restart the SiteScope service.

4). Use the Database Connection Tool for connection tuning:

Database Connection URL: `jdbc:sqlserver://<IP Address>:<port>;InstanceName=<name>;DatabaseName=<name>`

Database Driver: `com.microsoft.sqlserver.jdbc.SQLServerDriver`

5). Create the desired database monitor type.

- **com.mercury.jdbc.oracle.OracleDriver.** A driver for Oracle databases. This driver is deployed with SiteScope. When using the driver, the database connection URL has the form of: `jdbc:mercury:oracle://<server name or IP address>:<database server port>;sid=<sid>`
 - **oracle.jdbc.driver.OracleDriver.** SiteScope supports the following categories of JDBC driver that are supplied by Oracle:
 - JDBC thin driver for Oracle 7 and 8 databases.
 - JDBC OCI (thick) driver. For details on accessing Oracle databases using OCI driver, see "[How to Access Oracle Databases Using OCI Driver](#)" on page 172.
 - **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: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 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.
 - Database drivers that have timeout problems (where database queries processed with these drivers exceed the timeout specified in the monitor's **Query timeout** field) can be specified in

the **Timeout proxied query drivers list** field (in **Preferences > Infrastructure Preferences > General Settings**). These drivers are queried separately with a monitor-based timeout.

- 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.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports IPv6 addresses in the TCP (JDBC) protocol. Support for IPv6 might also depend on the JDBC driver being used.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

This section includes:

- ["How to Configure the Database Query Monitoring Environment"](#) below
- ["How to Access Oracle Databases Using OCI Driver"](#) on the next page
- ["How to Access Oracle Databases Without Using ODBC"](#) on the next page
- ["How to Enable SiteScope to Monitor an Informix Database"](#) on page 173
- ["How to Enable SiteScope to Monitor a MySQL Database"](#) on page 173
- ["How to Enable SiteScope to Monitor a Sybase Database"](#) on page 174

How to Configure the Database Query Monitoring Environment

1. Prerequisites

There are several key requirements for using this monitor. For details, see ["Setup Requirements and User Permissions"](#).

2. Configure the database driver

- You can monitor an Oracle database using an OCI driver. For details, see ["How to Access Oracle Databases Using OCI Driver"](#) on the next page.
- You can monitor an Oracle database using the Oracle Thin JDBC Driver. For details, see ["How to Access Oracle Databases Without Using ODBC"](#) on the next page.

3. Enable SiteScope to monitor the database

- For details on enabling SiteScope to monitor an Informix database, see ["How to Enable SiteScope to Monitor an Informix Database"](#) on page 173.
- For details on enabling SiteScope to monitor a MySQL database, see ["How to Enable SiteScope to Monitor a MySQL Database"](#) on page 173.
- For details on enabling SiteScope to monitor a Sybase database, see ["How to Enable SiteScope to Monitor a Sybase Database"](#) on page 174.

4. Troubleshoot driver or database errors

To troubleshoot possible errors using the Oracle Thin Driver, MySQL Driver, or Sybase database, see ["Tips/Troubleshooting"](#) on page 180.

5. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip:

- The Database Connection Tool is available when configuring this monitor to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Database Connection Tool in the

Using SiteScope Guide.

- 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 minute.
- You can also modify the default number of columns, rows, and characters that are displayed for the Database Query monitor in the SiteScope Dashboard by changing the **DB maximum columns**, **DB maximum rows**, and **DB maximum value length** settings in **Preferences > Infrastructure Preferences > Monitor Settings**.

How to Access Oracle Databases Using OCI Driver

You can monitor an Oracle database using an OCI driver. If the port or SID are changed, you only need to make the change in the **tnsnames.ora** file (the SiteScope Oracle monitors remain unchanged).

1. On the SiteScope server, install the version of Oracle client that you are using.
2. Connect to the Oracle database using the Oracle OCI driver.
 - Set **ORACLE_HOME** environment variable (**ORACLE_HOME** is the folder where the Oracle client or database has been installed).
 - Add **ORACLE_HOME\lib** to System PATH (on Windows platforms), or **LD_LIBRARY_PATH** env variable (on UNIX platforms).
 - Set **CLASSPATH** environment variable to use Oracle JDBC driver from **ORACLE_HOME\jdbc\lib**.
3. In the `\oracle\oraX\network\admin\tnsnames.ora` file, configure the service name. You can test this using a SQL+ tool or the SiteScope Database Connection tool (see Database Connection Tool in the Using SiteScope Guide).
4. Add a database monitor within SiteScope, and configure the following settings in the Monitor Settings panel:
 - **Database connection URL:** `jdbc:oracle:oci8:@<service name>`
 - **Database driver:** `oracle.jdbc.driver.OracleDriver`
 - Enter the database user credentials in the **Database user name** and **Database password** boxes

How to Access Oracle Databases Without Using ODBC

If you want to monitor an Oracle database without using ODBC, you can use the Oracle Thin JDBC Drivers.

1. To set up SiteScope to use the JDBC Thin Drivers, 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, and configure the following settings in the Monitor Settings panel:

- **Database connection URL.** The 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.

- **Database driver.** Enter the following string: `oracle.jdbc.driver.OracleDriver`.

How to Enable SiteScope to Monitor an Informix Database

Monitoring an Informix database requires the use of a JDBC driver.

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. Add a Database Query monitor within SiteScope, and configure the following settings in the Monitor Settings panel:

- **Database connection URL.** The format for the Informix JDBC driver is:

```
jdbc:informix-sqli://<database hostname>:<tcp port><database server>:INFORMIXSERVER=<database>
```

- If you require a **Database user name** and **Database 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;
```

- **Database driver.** Enter the Informix JDBC driver `com.informix.jdbc.IfxDriver`

How to Enable SiteScope to Monitor a MySQL Database

Monitoring a MySQL database requires the use of a JDBC driver.

1. Download the MySQL JDBC driver from the MySQL web site (<http://www.mysql.com>).
2. Uncompress the distribution file.
3. Copy the .jar file into the **<SiteScope root directory>\WEB-INF\lib** directory.
4. Stop and restart SiteScope.
5. Add a Database Query monitor within SiteScope, and configure the following settings in the Monitor Settings panel:

- **Database connection URL.** The 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.

- **Database driver.** Enter the specification for the MySQL JDBC driver:

```
org.gjt.mm.mysql.Driver
```

How to Enable SiteScope to Monitor a Sybase Database

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. Do not extract the zip file.
3. Stop and restart the SiteScope service.
4. Add a Database Query monitor within SiteScope, and configure the following settings in the Monitor Settings panel:

- **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 enter:

```
jdbc:sybase:Tds:bgsu97:2408
```

- 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 enter:

```
jdbc:sybase:Tds:bgsu97:2408/quincy
```

- **Database driver.** Enter `com.sybase.jdbc.SybDriver` (for Sybase version 4.x) or `com.sybase.jdbc2.jdbc.SybDriver` (for Sybase version 5.x).

- Enter the **Database user name** and **Database password**.
- Enter 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
```

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Database Query Monitor Settings

User interface elements are described below:

UI Element	Description
Database connection URL	<p>URL to a database connection (no spaces are allowed in the URL). 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, enter <code>jdbc:odbc:test</code> as the connection URL.</p> <p>Note for using Windows Authentication: If you want to access the database using Windows authentication, enter <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>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 <SiteScope root directory>\WEB-INF\lib\ directory.</p> <p>Default value: <code>sun.jdbc.odbc.JdbcOdbcDriver</code></p> <p>Tip: You can specify database drivers that have timeout problems (where database queries processed with these drivers exceed the timeout specified in the monitor's Query timeout field) in the Timeout proxied query drivers list field (in Preferences > Infrastructure Preferences > General Settings). These drivers are queried separately with a monitor-based timeout.</p>

UI Element	Description
Database user name	<p>User name used to log on to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystems JDBC-ODBC bridge driver, <code>sun.jdbc.odbc.JdbcOdbcDriver</code>), you can leave this blank and choose Windows Authentication when you setup the ODBC connection.</p> <p>With Windows 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>Password used to log on to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystems JDBC ODBC bridge driver (<code>sun.jdbc.odbc.JdbcOdbcDriver</code>), you can leave this blank and choose Windows Authentication when you create the ODBC connection.</p> <p>With Windows Authentication, SiteScope connects using the login account of the SiteScope service.</p>
Query	<p>SQL query to test.</p> <p>Example:<code>select * from sysobjects</code></p>
Match content	<p>Text string 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 <code>i</code> 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>

UI Element	Description
Open Tool	Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.
File path	<p>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 for complex queries or queries that change and are updated by an external application.</p>
Column labels	<p>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>
Database machine name	Text identifier describing the database server that this monitor is monitoring if you are reporting monitor data to an installation of HP Business Service Management. This text descriptor is used to identify the database server when the monitor data is viewed in an HP Business Service Management report.
<p>Database Connection Settings</p> <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 and 9.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>	
Use connection pool	<p>Enables SQL connection sharing. 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>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>

UI Element	Description
Idle connection timeout	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. Default value: 5 minutes
Query timeout	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. Default value: 1 minute

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section describes troubleshooting and limitations for the Database Query monitor.

General Tips

- If you require multiple columns in the monitor output, you can use the **_databaseMaxColumns** property in the **<SiteScope root directory>\groups\master.config** file or the **DB maximum columns** setting in **Preferences > Infrastructure Preferences > Monitor Settings**) to adjust the maximum number of columns displayed in the SiteScope Dashboard (the default is 10 columns). You can also change the maximum number of rows processed by DB monitors (**DB maximum rows**) and the maximum length, in characters, of the data processed by DB monitors (**DB maximum value length**). The default maximum number of rows is 1, and the default maximum value length is 200 characters.
- When using the Database Connection Tool to apply properties to the monitor, you must enter the credential data manually (if you select a credential profile the credential data is lost).
- You can set additional database options that affect all resources that connect to the database in the JDBC Global Options in **Preferences > General Preferences**. For details, see JDBC Global Options in the Using SiteScope Guide.

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, 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 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 Database driver.
- **error, connect error, No suitable driver**: check for syntax errors in Database connection

URL, such as dots instead of colons.

Possible Errors Using the MySQL Driver

If, after enabling SiteScope to monitor a MySQL database, you get an authorization error in the Database Query monitor, 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.

Possible Errors with Sybase Database Monitoring

- Verify you are using the correct driver for the version of Sybase you are monitoring. Enter `com.sybase.jdbc.SybDriver` for Sybase version 4.x. and `com.sybase.jdbc2.jdbc.SybDriver` for Sybase version 5.x.
- **error, driver connect error, com/sybase/jdbc/SybDriver.** Verify 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** field is correct.

Chapter 19

DB2 8.x and 9.x Monitor

Use the DB2 8.x and 9.x monitor to monitor DB2 8.x and 9.x servers for availability and proper functioning. You can monitor multiple parameters or counters with a single monitor instance. This enables 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. The error and warning thresholds for the monitor can be set on up to ten DB2 server performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the DB2 8.x and 9.x monitor.

Learn More

This section includes:

- "IPv6 Addressing Supported Protocols" below
- "DB2 8.x and 9.x Topology" below

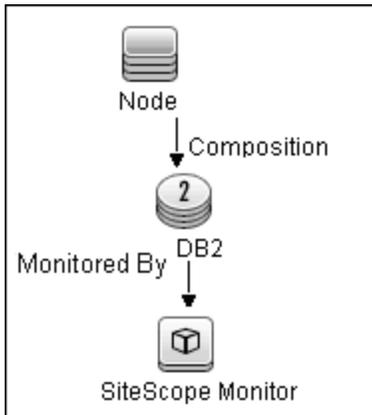
IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the TCP (JDBC) protocol. Support for IPv6 might also depend on the JDBC driver being used.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

DB2 8.x and 9.x Topology

The DB2 8.x and 9.x monitor can identify the topology of the DB2 system being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

Tasks

How to Configure the DB2 8.x and 9.x Monitor

1. Prerequisites

- JDBC drivers for connecting to the DB2 Database server. These can be found in your DB2 server installation directories. Copy the **db2jcc.jar** file to the **<SiteScope root directory>\WEB-INF\lib** folder.
- This monitor uses the Snapshot mirroring functionality supported by DB2. You must enable the Snapshot Mirror on your DB2 instance to retrieve counters. For details, refer to the relevant IBM DB2 documentation.

Note: Since DB2 8.x and 9.x monitors are based on JDBC connections, there is no binding with any specific operation systems.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Database Connection Tool** is available when configuring this monitor to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Database Connection Tool in the Using SiteScope Guide.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["DB2 8.x and 9.x Topology" on the previous page](#).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

DB2 8.x and 9.x Monitor Settings

User interface elements are described below:

UI Element	Description
DB2 server	Address or name of the server where the DB2 database is running.
Port	Port on which the DB2 database accepts connections. Default value: 50000
Database	DB2 database node name that you want to monitor. Default value: sample Example: DB2 is the default node name created by DB2 installation.
Credentials	Option for providing the user name and password to be used to access the DB2 database server: <ul style="list-style-type: none">• Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box.• Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (selected by default). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Partition	Partition to monitor. -1 is the current partition; -2 is all partitions. Default value: -1
Calculate rate	Calculates 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 on to the database, the counter keeps growing. Selecting this option, the monitor displays the value 2, which means 2 user logins per second.
Counters	Server performance counters to check with this monitor. Use the Get Counters button to select counters.

UI Element	Description
<p>Get Counters</p>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p>Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>
<p>Database Connection Settings</p> <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 and 9.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>	
<p>Use connection pool</p>	<p>Enables SQL connection sharing. 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>
<p>Physically close if idle connection count exceeds</p>	<p>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>
<p>Idle connection timeout</p>	<p>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>
<p>Query timeout</p>	<p>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>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- 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. For details, see JDBC Global Options in the Using SiteScope Guide.

Chapter 20

DHCP Monitor

This monitor enables you to monitor 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the DHCP monitor.

Learn More

DHCP Monitor Overview

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.

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 about every 10 minutes.

Tasks

How to Configure the DHCP Monitor

1. Prerequisites

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.

- a. Download the jDHCP library (either in .zip or in .tar.gz format).
- b. Extract the file named **JDHCP.jar** and copy it to the **<SiteScope root directory>\WEB-INF\lib** directory.
- c. After installing the **JDHCP.jar** file, restart the SiteScope service.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

DHCP Monitor Settings

User interface elements are described below:

UI Element	Description
Timeout	Amount of time, in seconds, to wait for an IP address. Default value: 10 seconds
Requested client address	IP address to request from the DHCP server.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 21

Directory Monitor

The Directory monitor enables you to monitor an entire directory and report 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Directory monitor.

Learn More

This section includes:

- ["Directory Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)

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.

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see [SiteScope Monitoring Using Secure Shell \(SSH\)](#) in the [Using SiteScope Guide](#).
- This monitor supports monitoring remote servers running on Windows and HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see ["How to Configure the HP NonStop Resources Monitor" on page 282](#).

Tasks

How to Configure the Directory Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Directory Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the directory you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</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> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none">• Browse servers. Select a server from the drop-down list of servers visible in the local domain.• Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Directory path	<p>Directory that you want to monitor.</p> <ul style="list-style-type: none"> • To monitor directories on a remote Windows 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 on 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 on 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 Remote Servers Overview in the Using SiteScope Guide. <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 in the Using SiteScope Guide.</p>
No subdirectories	Subdirectories are not included in the match count.
File name match	Text or an expression to match against. Only file names which match are counted in the totals.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

Chapter 22

Disk Space Monitor (Deprecated)

Use the Disk Space monitor to track how much disk space is currently in use on your server.

Note: The Disk Space monitor was deprecated and replaced by the "[Dynamic Disk Space Monitor](#)" on [page 210](#). However, Disk Space monitors configured in previous versions still work when upgrading to SiteScope 11.20.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Disk Space monitor.

Learn More

This section includes:

- "Disk Space Monitor Overview" below
- "Supported Versions" below
- "IPv6 Addressing Supported Protocols" below

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* in the *Using SiteScope Guide*.

Note: There is also a dynamic version of this monitor that automatically adds or removes counters and thresholds that measure the disk according to changes in the environment. For details, see "Dynamic Disk Space Monitor" on page 210.

Supported Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see *SiteScope Monitoring Using Secure Shell (SSH)* in the *Using SiteScope Guide*.
- This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see "How to Configure the HP NonStop Resources Monitor" on page 282.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see *Configure the WMI Service for Remote Monitoring* in the *Using SiteScope Guide*.
- To monitor Microsoft Windows Server 2008 using WMI, you should install the Microsoft hot fix (<http://support.microsoft.com/kb/961435/en-us>) on the target Windows system.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Disk Space Monitor

1. Prerequisites

You must have domain privileges or authenticated access to the remote Windows or UNIX server, and specify valid user credentials. The user specified in the **Credentials** section must have sufficient permissions to connect to and gather information from the remote server disk drives. On UNIX systems, the defined user must have privileges to execute a command to retrieve available mounted disks (for example, on Linux: `/bin/df -k <disk>`).

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Performance Counters Tool** is available when configuring this monitor to check performance counters on a specific machine in a Windows network (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Performance Counters Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Disk Space Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the disk space you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
Disk/File system	<p>Disk drive to monitor.</p>

Monitor Reference

Chapter 22: Disk Space Monitor (Deprecated)

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

Tips

This monitor supports setting fractional thresholds which are more useful than setting whole number thresholds when monitoring large disks (such as 1 terabyte and larger).

Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Disk Space monitor.

- "Disk Performance Counters Unavailable on Windows 2000" below
- "WMI Returns Incorrect Disk Space Values" below

Disk Performance Counters Unavailable on Windows 2000

Disk performance counters are unavailable by default in standard Windows 2000 installations. To monitor disk drives on servers running Windows 2000, you must enable these disk counters. Use the `diskperf -y` command line on each Windows 2000 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 Disk Space monitor dialog box.

WMI Returns Incorrect Disk Space Values

Due to a limitation with WMI, the WMI connection method returns incorrect results when this monitor is used on Windows Server 2008.

Workaround: To monitor Windows Server 2008 using WMI, you should install the Microsoft hot fix (<http://support.microsoft.com/kb/961435/en-us>) on the target Windows system.

Chapter 23

DNS Monitor

This monitor enables you to monitor your Domain Name Servers (DNS) to verify that they are working properly.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the DNS monitor.

Learn More

DNS Monitor Overview

Use the DNS monitor to monitor your Domain Name Servers (DNS) 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 using the server name (they can connect to it using the IP address only).

The DNS monitor checks your DNS 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; and returns a status and writes it in the monitoring log file with each running.

Most companies have both a primary and a secondary DNS server. If your company employs a firewall, these DNS 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.

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). To use this monitor, the TCP/IP protocol must be installed.

Tasks

How to Configure the DNS Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **DNS Lookup Tool** is available when configuring this monitor to look up names from a Domain Name Server and show you the IP address for a domain name (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see **DNS Tool** in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

DNS Monitor Settings

User interface elements are described below:

UI Element	Description
DNS server address	IP address of the DNS server that you want to monitor. Example: 206.168.191.1
Host to resolve	Host name to lookup. If you only want to verify that your DNS server is operating, the host name you enter 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, enter the IP address that corresponds to the host name you enter in the Expected IP address box.
Expected IP address	IP address or addresses that are mapped to the Host to resolve (domain name) entered above. You can use the DNS monitor to verify that a host name or domain name resolves to the correct IP address or addresses. Note: If you enter more than one IP address, the monitor reports a status of <i>good</i> , even if only one of the IP addresses that you enter is mapped correctly to the Host to resolve . When using this option, the monitor only reports an error if none of the IP addresses entered here are mapped to the given Host to resolve . When entering multiple IP addresses, separate them with a comma (",").

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

Troubleshooting and Limitations

- If the SiteScope server cannot reach a DNS server that is running (no ping to host), and there are no network connectivity issues, check the TCP/IP client configuration settings on the DNS server. Also verify that the DNS server itself does not have a connectivity issue.
- If the SiteScope server does not get a response to name resolution requests (even though it can ping the DNS server), ask your network administrator to verify that the DNS Server service is enabled and running on the DNS server.
- If the DNS server responds to queries for name resolution but with the incorrect information, it might be because the DNS server has incorrect or outdated information in its resource records for the specific zone. This situation can be due to a number of issues, including the following (should be managed by network administrator):
 - If administrators are manually creating and updating resource records, the incorrect information might have been inserted into the zone database file by the individual updating the resource records. To rectify this issue, you would have to manually verify the validity of each resource record.
 - If the DNS server is configured for dynamic updates, verify that dynamic updates have indeed occurred. If no dynamic updates have occurred, this would be the reason that the DNS server responded to SiteScope requests with outdated information. If the issue still persists, verify that the DNS server is configured for dynamic updates.
 - The DNS server might be incorrectly resolving names from a secondary DNS server due to zone transfer not occurring for the specific secondary DNS server. This would result in the secondary zone database file containing the incorrect information. To rectify this issue, manually force a zone transfer to ensure that the secondary DNS zone database file contains updated information.

Chapter 24

Dynamic Disk Space Monitor

The Dynamic Disk Space monitor tracks how much disk space is currently in use on your server. When dynamic monitoring is configured, the counters and thresholds are automatically updated as disks are added to or removed from the server. This enables you to configure the monitor once, and leave it to detect disks and file systems changes.

Note: The Dynamic Disk Space monitor replaces the Disk Space monitor that was deprecated in SiteScope 11.20. Disk Space monitors configured in previous versions will work when upgrading to SiteScope 11.20.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Dynamic Disk Space monitor.

Learn More

This section includes:

- ["Dynamic Disk Space Monitor Overview" below](#)
- ["Supported Versions" below](#)
- ["Dynamic Monitoring Mechanism" below](#)
- ["Monitor Run Frequency" on the next page](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)
- ["Dynamic Disk Space Monitor Topology" on page 213](#)

Dynamic Disk Space Monitor Overview

Use the Dynamic Disk Space monitor, an advanced version of the Disk Space monitor, to monitor the amount of disk space that is currently in use on your server. This monitor enables you to:

- Monitor specific disks and counters on a host server using static counters. You can select one or multiple disks to monitor.
- Monitor changes in the host server's disks that correspond to a defined counter pattern. Dynamic monitoring enables you to configure the monitor once, and leave it to discover the addition and removal of disks and file systems in the environment and update itself.

When configuring a dynamic monitor, you can define a counter pattern that specifies the disks and counters you want to monitor. You can also define the required thresholds for the counter's pattern. The monitor scans the target host periodically, and creates the counters that are aligned with the given counter pattern.

If a new disk (or mount) is added to the machine and that disk corresponds to the counter pattern, the counters and thresholds that measure the disk are automatically added to the monitor when the counters are next updated from the server. Similarly, if a disk that corresponds to the counter pattern is no longer available, counters and thresholds for that disk are removed from the monitor (unless you choose not to delete them, in which case they are still displayed in the monitor's counter list).

Supported Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see [SiteScope Monitoring Using Secure Shell \(SSH\)](#) in the [Using SiteScope Guide](#).
- This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see ["How to Configure the HP NonStop Resources Monitor" on page 282](#).
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see [Configure the WMI Service for Remote Monitoring](#) in the [Using SiteScope Guide](#).

Dynamic Monitoring Mechanism

To enable the monitor to dynamically update counters and thresholds, select the counter patterns

you want to monitor using a regular expression. For example, if you enter the pattern `/.*/.*platform.*/MB free/`, the monitor retrieves the MB free counters on disks that contain the word `platform` in their file system's name.

Note: SiteScope uses Perl regular expressions for pattern matching. For example, if you enter `/cpu.*/` or `cpu`, any counters with `cpu` in their name match this pattern and are added to the counters list.

You also set the frequency of the dynamic update mechanism at the monitor level. This is the frequency that SiteScope uses to update the counters retrieved from the server. This enables running the update mechanism at a frequency that is appropriate for the monitor type.

During each update, the monitor connects to the server and dynamically updates the status of each counter that matches the pattern defined by the regular expression. If no counters match the monitor patterns or no counters are returned from the server, the monitor is in error status.

The thresholds list always contains the counter patterns that were defined in the counters pattern table (not the final counters that were found). The values in this list are updated according to changes you make in the counter patterns table.

In this way, the monitor automatically configures itself with counters on the relevant dynamic environment components. Counters that are no longer available on the server are automatically removed from SiteScope and no errors are logged.

Note: When you define static counters (with no regular expression), these counters are never removed from the monitor, even if they are no longer available on the server.

Monitor Run Frequency

The Dynamic Disk Space monitor does not require many resources, so you can run 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* in the *Using SiteScope Guide*.

Note: The frequency for updating counters from the server cannot be less than the monitor run frequency in Monitor Run Settings.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

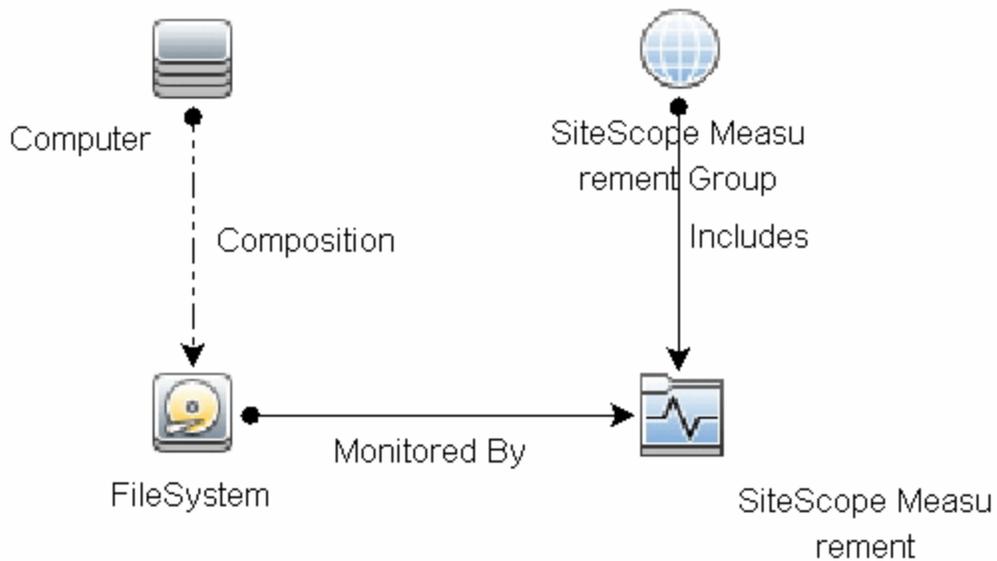
would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Dynamic Disk Space Monitor Topology

The Dynamic Disk Space monitor can identify the topology of the server disks being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

Tasks

How to Configure the Dynamic Disk Space Monitor

1. Prerequisites

- You must have domain privileges or authenticated access to the remote Windows or UNIX server, and specify valid user credentials. The user specified in the **Credentials** section must have sufficient permissions to connect to and gather information from the remote server disk drives.
- On UNIX systems, the defined user must have privileges to execute a command to retrieve available mounted disks (for example, on Linux: `/bin/df -T <disk>`).

2. Configure the monitor properties

- a. Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **Dynamic Disk Space**. The New Dynamic Disk Space Monitor dialog box opens. For monitor user interface details, see ["Dynamic Disk Space Monitor Settings" on page 217](#).
- b. In the General Settings panel, enter a name and description for the monitor.
- c. In the Dynamic Disk Space Monitor Settings panel, select the server where the disk space you want to monitor is running.
- d. In the Counter Settings section, click the **Get Counter** button, and select the disk and counters you want to monitor from the Select Counters Form (the form displays static counters only). The counters are added to the Counter Preview tree.

Tip: The **Performance Counters Tool** is available when configuring this monitor to check performance counters on a specific machine in a Windows network (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Performance Counters Tool in the Using SiteScope Guide.

- e. The default counter patterns are displayed in the Patterns & Counters table. You can add other patterns to counters to instruct the monitor which counters to use. You can either:
 - Click the **Add New Counter**  button to add an empty line to the table, and create a pattern format using a regular expression. By default the following counters are created:

Counter Pattern	Description
<code>./*/MB free/</code>	Measures the amount of free memory.
<code>./*/MB total/</code>	Measures the total amount of memory.
<code>./*/percent full/</code>	Measures the percentage of the file system that is full.

Tip:

- (1). The pattern should always start and end with the forward slash ("/") character.
- (2). [and] characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character).
- (3). Use "."* to describe any character any number of times.

- o Select a static counter, and edit the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.
- f. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counters Preview tree.
- g. Set the frequency for updating counters from the server, and then click **Verify & Save** or **Save** to save your settings. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- h. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful if a disk fails or for keeping track of the counters that were previously being monitored.
- i. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

Note: When configuring threshold settings for Dynamic Disk Space monitor:

- o The monitor **always(default)** counter configured in the **Good if** section of the monitor's properties means that the state of the monitor is good, unless one of the thresholds of any of the other counters is breached.
- o The **countersinError** counter configured in the **Error if** section of the monitor's properties means that the state of the monitor is error if one of the other counters is unavailable.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "Dynamic Disk Space Monitor Topology" on page 213.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

4. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the server where the disk space you want to monitor is running and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

Monitor Reference

Chapter 24: Dynamic Disk Space Monitor

You can check performance of the dynamic monitoring framework in:

- The SiteScope **Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Dynamic Disk Space Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the disk space you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. If the server you want to monitor does not appear in the Serverslist because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
Counter Settings	

UI Element	Description
Get Counters	Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.
Patterns & Counters	<p>Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.</p> <p>Click the Add New Counter  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the Delete Counter  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the View Matches for Selected Pattern Counter  button to display counters that match the selected patterns.</p> <p>Note: SiteScope uses Perl regular expressions for pattern matching. For example, if you enter <code>/cpu.* /</code> or <code>cpu</code>, any counters with <code>cpu</code> in their name match this pattern and are added to the counters list.</p>
Counters Preview	Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.
Frequency of updating counters from server	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p>Default value: 1 hour</p> <p>Note:</p> <ul style="list-style-type: none"> • The update frequency cannot be less than the monitor run frequency in Monitor Run Settings. • When configuring this setting in a template, the variable value can only be in time units of seconds. • Static counters are never deleted.

UI Element	Description
Continue displaying counters that no longer exist after update	<p>When selected, counters that no longer exist after running the update mechanism to retrieve counters from the monitored server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful, for example, if a disk fails or for keeping track of counters that were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings on the next update.</p> <p>Default value: Selected</p> <p>Note: This option is relevant for dynamic counters only (those set using a regular expression). Static counter that are no longer available are still displayed even when this check box is cleared.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- This monitor supports setting fractional thresholds which are more useful than setting whole number thresholds when monitoring large disks (such as 1 terabyte and larger).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).

Troubleshooting and Limitations

This section describes troubleshooting and limitations for Dynamic Disk Space monitors.

- ["Disk Performance Counters Unavailable on Windows 2000" below](#)
- ["WMI Returns Incorrect Disk Space Values" below](#)
- ["Unable to get counters from Red Hat Enterprise Linux about network file systems" below](#)
- ["Troubleshooting the Log Files" on the next page](#)

Disk Performance Counters Unavailable on Windows 2000

Disk performance counters are unavailable by default in standard Windows 2000 installations. To monitor disk drives on servers running Windows 2000, you must enable these disk counters. Use the `diskperf -y` command line on each Windows 2000 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 Disk Space monitor dialog box.

WMI Returns Incorrect Disk Space Values

Due to a limitation with WMI, the WMI connection method returns incorrect results when this monitor is used on Windows Server 2008.

Workaround: To monitor Windows Server 2008 using WMI, you should install the Microsoft hot fix (<http://support.microsoft.com/kb/961435/en-us>) on the target Windows system.

Unable to get counters from Red Hat Enterprise Linux about network file systems

By default, SiteScope is only able to display file systems under `/dev`. To change this, do the following:

1. Create a backup of the **<SiteScope root directory>/templates.os/Linux.config** and **<SiteScope root directory>/templates.os/RedHatEnterpriseLinux.config** files.
2. Edit the **<SiteScope root directory>/templates.os/Linux.config** as follows:
 - Search for "id=disks".
 - Add the following to the bottom of the "id=disks" section (the lines between the #s define each section):


```
noNameFilter=true
startLine=2
#
```
 - Save the file.
3. Repeat for the **<SiteScope root directory>/templates.os/RedHatEnterpriseLinux.config** file.
4. Restart SiteScope.

Troubleshooting the Log Files

- Check for dynamic framework errors in:
 - **<SiteScope root directory>\logs\dynamic_monitoring_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
 - **<SiteScope root directory>\logs\dynamic_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).
- Check for Dynamic Disk Space monitor errors in:
 - **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.
- Copy the following sections from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####
# Dynamic Monitoring
#####
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
false
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG,
dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFile
Appender
log4j.appender.dynamic.monitoring.appender.File=./${log.file.path}/dynamic_
monitoring.log
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.Pattern
Layout
```

Monitor Reference

Chapter 24: Dynamic Disk Space Monitor

```
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p -  
%m%n
```

```
# Dynamic monitors changes  
categoryog4j.category.DynamicMonitoringChanges=INFO,  
dynamic.monitoring.changes.appender  
log4j.additivity.DynamicMonitoringChanges=false
```

Chapter 25

e-Business Transaction Monitor

The e-Business Transaction monitor enables you to verify that the multiple tasks that make up an online transaction are completed properly.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the e-Business Transaction monitor.

Learn More

This section includes:

- [" e-Business Transaction Monitor Overview" below](#)
- ["Editing the Order of the Monitors in the Chain" below](#)

e-Business Transaction Monitor Overview

Use this monitor to verify that an end-to-end transaction and associated processes complete properly. This includes:

- Successful navigation through a series of URLs.
- Transmission of an email confirming the sequence.
- Logging the information into a database file.

The e-Business Transaction monitor runs a sequence of other SiteScope monitors, checking that each monitor returns a status of OK. It reports an Error status if any monitor in the sequence fails.

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 (see ["URL Sequence Monitor" on page 695](#)).
- Check that the order status was updated (see ["URL Sequence Monitor" on page 695](#)).
- Check that a confirmation email was received (see ["Mail Monitor" on page 334](#)).
- Check that the order was added to the order database (see ["Database Query Monitor" on page 167](#)).
- Check that the order was transferred to a legacy system (see ["Script Monitor" on page 556](#)).

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 e-Business 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 e-Business Transaction monitor reports an error.

Each time the e-Business Transaction monitor runs, it returns a status based on the number and percentage of items in the specified monitors, groups, or both, 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 e-Business Transaction monitor page lists monitor groups and individual monitors in alphabetical order. To have the e-Business Transaction monitor run the chain of monitors in the proper order, they must appear in the proper order in the **Selected** table on the New e-Business Transaction Monitor page. You can do this by selecting the individual monitors in the order in which they should be run.

Tasks

How to Configure the e-Business Transaction Monitor

1. Set up monitors for the e-Business chain

Before you can add an e-Business Transaction monitor, you must define other SiteScope monitors that report on the actions and results of the steps in the sequence chain.

- a. Create a new group that contains all the individual monitors to be included in the sequence chain (one or more URL Sequence monitor for verifying the sequence of online actions, a Mail monitor to confirm that an email acknowledgement is sent, and a Database Query monitor to see that information entered online is logged into a database).
- b. Open the new monitor group, and add the first individual monitor type needed for the sequence (for example, "URL Sequence Monitor" on page 695).

For task details on adding a monitor, see How to Deploy a Monitor in the Using SiteScope Guide.

Note: Monitors should be added in the order that they are run in the chain. For example, select a URL Sequence monitor which triggers an email event before you select the Mail monitor to check for the email.

- c. If necessary, set up the values to be passed from one monitor to another in the chain.
- d. Add the other monitors for this transaction chain in the required order of execution into the group.

Note: The individual monitors run by the e-Business Transaction monitor should generally not be run separately by SiteScope. You should make sure that the **Frequency** setting for each of these monitors is set to zero ("0").

- e. Create a new group or open an existing group that contains the e-business transaction chain monitor you are creating.
 - f. Click **New > Monitor** and select the **e-Business Transaction** monitor.
- #### 2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

e-Business Transaction Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Monitor delay (seconds)	<p>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> <p>Default value: 0 seconds</p>
When error	<p>Error handling option during the sequence:</p> <ul style="list-style-type: none"> • Continue to run the remainder of the monitors. This runs every monitor no matter what the status of a given monitor is. • Stop and 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>URL monitors use the same network connection and the same set of cookies.</p> <p>This is useful if you are using the e-Business Transaction monitor to group several URL Sequence monitors and do not want to include the login steps as part of each transaction.</p>
Item Settings	
Items	<p>Using the control key or equivalent, double-click the set of monitors that make up the e-Business Transaction monitor to move them to the Selected column.</p> <p>Note:</p> <ul style="list-style-type: none"> • Monitors are run in the order that they are listed in their group. For details, see "Editing the Order of the Monitors in the Chain" on page 224. • To control the order of the monitors in the chain, select monitors and not groups. If you select groups, they are run at random and not by group order.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

This monitor cannot be copied to a template. It must be created directly in a template.

Chapter 26

F5 Big-IP Monitor

This monitor enables you to monitor the content of event logs and other data from F5 Big-IP 4.0 load balancing device using SNMP. You can monitor multiple parameters or counters with a single monitor instance. This enables 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. The error and warning thresholds for the monitor can be set on one or more load balancer statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the F5 Big-IP monitor.

Learn More

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the F5 Big-IP Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **SNMP Browser Tool** is available when configuring this monitor to verify the connection properties of an SNMP agent and to gain more information about the MIBs which that agent implements (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Browser Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

F5 Big-IP Monitor Settings

User interface elements are described below:

UI Element	Description
SNMP Settings	
Server	Name of the server you want to monitor.
Port	Port to use when requesting data from the SNMP agent. Default value: 161
MIB file	MIB file option: <ul style="list-style-type: none">• LOAD-BAL-SYSTEM-MIBS file displays only those objects that are described within that MIB file.• 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. Default value: All MIBs
Counter calculation mode	Performs a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are: <ul style="list-style-type: none">• Calculate delta. Calculates a simple delta of the current value from the previous value.• Calculate rate Calculates a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements.• Do not calculate. No calculation is performed. 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.
Starting OID	Use 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 here. 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 enter a different value. Default value: 1 Note: This field is available in template mode only.

UI Element	Description
SNMP Connection Settings	
Timeout (seconds)	Amount of time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. Default value: 5
Number of retries	Number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. Default value: 1
Community	Community string (valid only for version 1 or 2 connections). Default value: public
SNMP version	Version of SNMP to use when connecting. Supports SNMP version 1, 2, and 3. Selecting V3 enables you to enter V3 settings in the SNMP V3 setting fields below. Default value: V1
Authentication algorithm	The authentication algorithm to use for version 3 connections. Default value: MD5 Note: This field is available only if SNMP V3 is selected.
User name	User name for version 3 connections. Note: This field is available only if SNMP V3 is selected.
Password	Authentication password to use for version 3 connections. Note: This field is available only if SNMP V3 is selected.
Privacy algorithm	The privacy algorithm used for authentication for SNMP version 3 (DES, 128-Bit AES, 192-Bit AES, 256-Bit AES). Default value: DES Note: This field is available only if SNMP V3 is selected.
Privacy password	Privacy password for version 3 connections. Leave blank if you do not want privacy. Note: This field is available only if SNMP V3 is selected.
Context name	Context Name to use for this connection. This is applicable for SNMP V3 only. Note: This field is available only if SNMP V3 is selected.

UI Element	Description
Context engine ID	Hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only. Note: This field is available only if SNMP V3 is selected.
SNMP Counters	
Counters	Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note: The counters displayed are those received during the timeout period, and may not include all the counters available on the server. Specifying a longer timeout in the Timeout (seconds) field in the SNMP Connection Settings panel may result in receiving more counters. The total time for receiving the counters may be longer than the timeout specified, due to additional processing time not part of the request/response period. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 27

File Monitor

The File monitor enables you to read a specified file and check the size and age of the file.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the File monitor.

Learn More

This section includes:

- ["File Monitor Overview"](#) below
- ["Supported Versions"](#) below
- ["Reading and Status"](#) below

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.

Supported Versions

- This monitor supports monitoring UNIX remote servers that have been configured in SiteScope and the local SiteScope machine only.
- This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop monitoring environment, see ["How to Configure the HP NonStop Resources Monitor"](#) on page 282.

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.

Tasks

How to Configure the File Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

File Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the file you want to monitor is located. Select a server from the server list (only UNIX remote servers that have been configured in SiteScope and the local SiteScope machine are displayed), or click Add Remote Server to add a new UNIX server.</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Add Remote Server	<p>Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
File name	<p>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 log on 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 Server box described above. For details on which UNIX user account to use for the applicable remote server, see Remote Servers Overview in the Using SiteScope Guide.</p> <p>For reading files on remote Windows 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 in the Using SiteScope Guide.</p>

UI Element	Description
File encoding	<p>File content is monitored using an encoding that is different than the encoding used on server where SiteScope is running. This may be necessary if the code page which SiteScope is using does not support the character set used in the target file. This enables SiteScope to match and display the encoded file content correctly.</p> <p>Default value: windows-1252</p>
Match content	<p>Text string 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 on regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.</p>
Open Tool	<p>Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.</p>

UI Element	Description
<p>Check for content changes</p>	<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 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>No error if file not found</p>	<p>The monitor remains in Good status even if the file is not found. The monitor status is Good regardless of how the monitor's thresholds have been configured.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 28

Formula Composite Monitor

This monitor enables you to monitor 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Formula Composite monitor.

Learn More

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.
- Microsoft Windows Performance Counter monitor.
- Script monitor.
- SNMP monitor.

If you need alert logic that is more complex than SiteScope's standard alerts permit, 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.

Tasks

How to Configure the Formula Composite Monitor

1. Prerequisites

- You must create at least two individual Database Query, Microsoft Windows Performance Counter, Script, or SNMP monitor instances before you can set up a Formula Composite monitor for those monitors. For details, see:
 - "Database Query Monitor" on page 167.
 - "Microsoft Windows Performance Counter Monitor" on page 445.

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 Microsoft Windows Performance Counter Monitor 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.

- "Script Monitor" on page 556.
- "SNMP Monitor" on page 596.
- 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.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Formula Composite Monitor Settings

User interface elements are described below:

UI Element	Description
Monitors	<p>Click the Add  button, and select two SNMP monitors, two Script monitors, two Database monitors, or two Microsoft Windows Performance Counter monitors that the Formula Composite monitor should operate on. Click Add Selected Monitors to display the selected monitors in the Monitors box. For details on the Add Items dialog box, see "Add Items Dialog Box" below.</p> <p>To remove monitors from the list, select the monitors and the Delete  button.</p>
Run monitors	<p>The Formula Composite monitor controls 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 set Frequency in Monitor Run Settings to 0. Those monitors then only run when scheduled by the Formula Composite monitor.</p>
Counters	<p>Server performance counters to check with this monitor. The list displays the available counters and those currently selected for this monitor.</p>
Monitor delay (seconds)	<p>Amount of time, in seconds, to wait between running each monitor (if Run monitors is selected).</p> <p>Default value: 0 seconds</p>
Operation	<p>Arithmetic operation to be performed on the results of the two monitors selected above. You can 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.</p>
Constant	<p>An operator and a constant to operate on the result of the calculation specified in the Operation item above.</p> <p>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>.</p> <p>Valid operators are + (addition), - (subtraction), * (multiplication), and / (division). Numbers may be integers or decimals.</p>
Result label	<p>Name for the result of the formula calculation.</p>

Add Items Dialog Box

This dialog box enables you to select the monitors, groups, or both, that you want in the Composite

Monitor Reference

Chapter 28: Formula Composite Monitor

monitor.

User interface elements are described below:

UI Element	Description
Add Selected Items	Click to add the selected groups, monitors, or both, to the Formula Composite monitor.
 SiteScope	Represents the SiteScope root directory.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors). If a group alert has been set up for the monitor group or subgroup, the alert  symbol is displayed next to the group icon.
	Represents a SiteScope monitor (enabled/disabled). If an alert has been set up for the monitor, the alert  symbol is displayed next to the monitor icon.

For information on configuring setting panels that are common to all monitors, see [Common Monitor Settings](#) in the [Using SiteScope Guide](#).

Tips/Troubleshooting

General Tips/Limitations

- When copying this monitor to a template, the subordinate monitors used to build a Formula Composite monitor are not copied. Therefore, it is recommended to create this monitor and its subordinate monitors directly in a template.
- 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.

Chapter 29

FTP Monitor

This monitor enables you to log on to an FTP server and retrieve a specified file. A successful file retrieval indicates that your FTP server is functioning properly. Use this page to add a monitor or edit the monitor's properties.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the FTP monitor.

Learn More

This section includes:

- ["FTP Monitor Overview" below](#)
- ["Status" below](#)
- ["Scheduling the Monitor" below](#)

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.

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. We recommend that you check one small file and one large 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`.

Scheduling the Monitor

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.

Tasks

How to Configure the FTP Monitor

1. Prerequisites

Before you can use this monitor, make sure you know:

- The relative paths, if any, to the files on the FTP server.
- An applicable user name and password to access the files.
- The filenames of one or more files available for FTP transfer.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **FTP Tool** is available when configuring this monitor to access an FTP server and view the interaction between SiteScope and the FTP server (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see FTP Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

FTP Monitor Settings

User interface elements are described below:

UI Element	Description
Basic FTP Settings	
Protocol	Select a protocol for the monitor: <ul style="list-style-type: none">• FTP. The monitor supports non-secure sockets only.• SFTP. The monitor supports Secure FTP. It typically uses SSH version 2 (TCP port 22) to provide secure file transfer. In this version, only password authentication is supported. <p>Note: SFTP protocol does not support Passive mode and SFTP is encrypted, rendering traditional proxies ineffective for controlling SFTP traffic (the proxy fields are not available).</p>
FTP server	IP address or the name of the FTP server that you want to monitor. Example: 206.168.191.22 or ftp.thiscompany.com (ftp.thiscompany.com:<port number> to specify a different port)
File	File name to retrieve from the FTP server. Example: /pub/docs/mydoc.txt You can use a regular expression to insert date and time variables. For details on using SiteScope's special data and time substitution variables in the file path, see SiteScope Date Variables in the Using SiteScope Guide. Example: s/C:\\firstdir\\\$shortYear\$\$0month\$\$0day\$/
User name	Name used to log into the FTP server. A common user name for general FTP access is user name <code>anonymous</code> .
Password	Password used to log into the FTP server. If using the anonymous login, the password is also <code>anonymous</code> .
Passive mode	SiteScope uses FTP passive mode. You use this mode to enable FTP to work through firewalls. (Not available in SFTP mode.)
Advanced FTP Settings	
Match content	Text string 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. Example: "/Size \d\d/" or "/size \d\d/i"

UI Element	Description
<p>Check for content changes</p>	<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.
<p>Timeout (seconds)</p>	<p>Amount of time, in 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.</p> <p>Default value: 60 seconds</p>
<p>Connection timeout (seconds)</p>	<p>Amount of time, in 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.</p> <p>Default value: 30 seconds</p>
<p>HTTP Proxy Settings (Not available in SFTP mode)</p>	
<p>HTTP proxy</p>	<p>SiteScope runs the FTP through an HTTP proxy. Generally, if you use an HTTP proxy you have it set up in your browser. Enter that same information here. Remember to include the port.</p> <p>Example: proxy.thiscompany.com:8080</p> <p>Note: The FTP monitor does not support an FTP Proxy server.</p>

UI Element	Description
Proxy user name	Proxy user name if the proxy server requires a name and password to access the file. The proxy server must support Proxy-Authenticate for these options to function.
Proxy password	Proxy password if the proxy server requires a name and password to access the file. The proxy server must support Proxy-Authenticate for these options to function.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 30

Generic Hypervisor Monitor

The Generic Hypervisor monitor provides a solution for monitoring Virtual Machines by using the virsh tool (a command line interface tool for managing guests and the hypervisor) to collect detailed information on nodes and guest virtual machines running on the host. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch key operational factors that can seriously affect availability and degrade performance. Create a separate monitor instance for each server you are running.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Generic Hypervisor monitor.

Learn More

This section includes:

- "Generic Hypervisor Monitor Overview" below
- "Supported Versions" below
- "Dynamic Monitoring Mechanism" below

Generic Hypervisor Monitor Overview

SiteScope simplifies the monitoring of virtual infrastructure changes in dynamic, virtualized environments by automatically changing the SiteScope configuration according to changes in the virtual environment. Generic Hypervisor monitors are dynamically updated over time by adding or removing counters and thresholds as virtual machines are added or removed. This enables you to configure the monitor one time, and leave it to automatically discover changes in the environment and update itself.

During initial monitor creation, the monitor uses the connection URI configured to access the VM 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.

Supported Versions

This monitor supports monitoring remote servers running on UNIX remotes only. It has been tested on a KVM environment.

Dynamic Monitoring Mechanism

To enable the monitor to dynamically update counters and thresholds, select the counter patterns you want to monitor using a regular expression. For example, if you enter the pattern `./*/Domains Information./*/Used Memory/`, the monitor retrieves the `Used Memory` counter for all VMs.

Note: SiteScope uses Perl regular expressions for pattern matching. For example, if you enter `/Used Memory.*/` or `Used Memory`, any counters with `Used Memory` in their name match this pattern and are added to the counters list.

You also set the frequency of the dynamic update mechanism at the monitor level. This is the frequency that SiteScope uses to update the counters retrieved from the server. This enables running the update mechanism at a frequency that is appropriate for the monitor type.

During each update, the monitor connects to the VM server and dynamically updates:

- The status of each counter that matches the pattern defined by the regular expression. If there are no available counters on the server, or no counters that match the monitor patterns, the monitor is not updated and it displays the previous counters set.
- Thresholds for the selected counters (every time counters are added or removed as a result of environment changes, the appropriate threshold is added or removed from the monitor).

In this way, the monitor automatically configures itself with counters on the relevant dynamic environment components. Counters that are no longer available on the VMs are automatically removed from SiteScope and no errors are logged.

Note: When you define static counters (with no regular expression), these counters are never removed from the monitor, even if they are no longer available on the server.

Tasks

How to Configure the Generic Hypervisor Monitor

1. Prerequisites

- The monitored VM server must be directly accessible by the SiteScope server (no proxy involved).
- The Virsh command-line tool should be installed on the system. For details, see <https://help.ubuntu.com/community/KVM/Virsh>.

2. Configure the monitor properties

- a. Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **Generic Hypervisor**. The New Generic Hypervisor Monitor dialog box opens.
- b. In the General Settings panel, enter a name and description for the monitor.
- c. In the Generic Hypervisor Monitor Settings panel, select the VM server you want to monitor (or add a new server) and specify the driver to which you want to connect in the **Connection URI** box. For user interface details, see the UI Descriptions section below.
- d. Click the **Get Counter** button, and select the counters you want to monitor from the Select Counters Form. The counters are added to the Preview tree in the **Patterns & Counters** section.
- e. For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
 - Clicking the **Add New Counter**  button to add an empty line to the table, and creating a pattern format using a regular expression.

Tip:

- (1). The pattern should always start and end with the forward slash ("/") character.
- (2). [and] characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character).
- (3). Use ".*" to describe any character any number of times.

For example, `./*/Domains Information./*/Used Memory/` displays Used Memory counter for all VMs.

- Selecting a static counter, and editing the counter to create a pattern format using a

regular expression. For details on using regular expressions, see [Regular Expressions Overview](#) in the *Using SiteScope Guide*.

Note: For details on the maximum number of counters that can be selected from the browsable tree and the maximum number of counters that can match the selected counter patterns when creating and updating dynamic monitors, see ["Maximum Number of Counters That Can be Saved" on page 259](#). If the maximum number of counters that can be deployed is exceeded, an error is written to the **RunMonitor.log**.

- f. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counters Preview tree.
- g. Set the frequency for updating counters from the server, and then click **Verify & Save** or **Save** to save your settings. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- h. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful if a disk fails or for keeping track of the counters that were previously being monitored.
- i. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see [Threshold Settings](#) in the *Using SiteScope Guide*.

3. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the VM server and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:

- The **SiteScope Health** group, using the Dynamic Monitoring Statistics monitor. For details, see [Dynamic Monitoring Statistics Page](#) in the *Using SiteScope Guide*.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see [Dynamic Monitoring Page](#) in the *Using SiteScope Guide*.

For additional troubleshooting suggestions, see ["Tips/Troubleshooting" on page 259](#).

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Generic Hypervisor Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the VM server that you want to monitor. Select a server from the server list (only those UNIX remote servers that have been configured in SiteScope are displayed), or click the Add Remote Server to add a new UNIX server.</p> <p>Note:</p> <ul style="list-style-type: none"> When configuring this monitor on SiteScopes running on UNIX versions, only remote servers that have been configured with an SSH connection method are displayed. For details, see How to Configure Remote Windows Servers for SSH monitoring. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.
Add Remote Server	Opens the Add UNIX Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.
Connection URI	URI of the driver of the VM server that you want to monitor.
Patterns & Counters	<p>Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.</p> <p>Click the Add New Counter  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the Delete Counter  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the View Matches for Selected Pattern  button to display counters that match the selected patterns.</p> <p>Note: SiteScope uses Perl regular expressions for pattern matching.</p>
Get Counters	Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.
Counter Preview	Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.

UI Element	Description
<p>Frequency of updating counters from server</p>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p>Default value: 15 minutes</p> <p>Note:</p> <ul style="list-style-type: none"> • The update frequency cannot be less than the monitor run frequency in Monitor Run Settings. • When configuring this setting in a template, the variable value can only be in time units of seconds. • Static counters are never deleted.
<p>Continue displaying counters that no longer exist after update</p>	<p>When selected, counters that no longer exist after running the update mechanism to retrieve counters from the monitored server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful, for example, if a disk fails or for keeping track of counters that were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings on the next update.</p> <p>Default value: Not selected</p> <p>Note: This option is relevant for dynamic counters only (those set using a regular expression). Static counter that are no longer available are still displayed even when this check box is cleared.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section includes:

- "General Notes" below
- "Maximum Number of Counters That Can be Saved" below
- "Troubleshooting Logs" below

General Notes

- When configuring this monitor in template mode, the **Add Remote Server** button is not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- This monitor supports setting fractional thresholds which are more useful than setting whole number thresholds when monitoring large disks (such as 1 terabyte and larger).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).

Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the `_browsableContentMaxCounters` parameter in the `master.config` file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the `_maxCountersForRegexMatch` parameter in the `master.config` file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The `_maxCountersForRegexMatch` parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both `_browsableContentMaxCounters` and `_maxCountersForRegexMatch` parameters in the `master.config` file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

Troubleshooting Logs

- Check for dynamic framework errors in:

- **<SiteScope root directory>\logs\dynamic_monitoring_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
- **<SiteScope root directory>\logs\dynamic_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).
- Check for Generic Hypervisor monitor errors in **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.
- Copy the following sections from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####
# Dynamic Monitoring
#####
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=false
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG,
dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFileAppender
log4j.appender.dynamic.monitoring.appender.File=./${log.file.path}/dynamic_monitoring.log
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p -
%m%n

# Dynamic monitors changes
category log4j.category.DynamicMonitoringChanges=INFO,
dynamic.monitoring.changes.appender
log4j.additivity.DynamicMonitoringChanges=false
```

Chapter 31

HAProxy Monitor

Use the HAProxy monitor to provide front- and back-end statistics to check that your HAProxy server is working properly. HAProxy is a solution that is used to provide high availability, load balancing, and proxying for TCP and HTTP-based applications. Using the HAProxy monitor provides a solution for monitoring infrastructures in the cloud.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HAProxy monitor.

Learn More

Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the HAProxy Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

HAProxy Monitor Settings

User interface elements are described below:

UI Element	Description
URL	URL of the stats-CSV report. Example: <code>http://server:port/haproxy?stats;csv</code>
Credentials	Option to use for authorizing credentials if the URL specified requires a name and password for access: <ul style="list-style-type: none">• Use user name and password. Select this option to manually enter user credentials. Enter the user name and password to access the URL in the User name and Password box.• Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password for the URL (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Authorization user name	User name to access the Web server stats page.
Authorization password	Password for accessing the Web server stats page.
HTTP proxy	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URL. Remember to include the port. Example: <code>proxy.thiscompany.com:8080</code>
Proxy server user name	Proxy user name if the proxy server requires a name and password to access the URL. Note: The proxy server must support Proxy-Authenticate for these options to function.
Proxy server password	Proxy password if the proxy server requires a name and password to access the URL. Note: The proxy server must support Proxy-Authenticate for these options to function.

UI Element	Description
Timeout (seconds)	Number of seconds (between 1 and 120) that the monitor should wait for a response from the server before timing-out. After this time period passes, the monitor logs an error and reports an error status. Default value: 60 seconds
Counters	Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 32

HP iLO (Integrated Lights-Out) Monitor

Use the HP iLO (Integrated Lights-Out) monitor that enables monitoring of hardware health on supported HP ProLiant servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server health status and hardware configuration for stability monitoring and fast response for critical hardware issues. You can create a separate HP iLO Monitor instance for each supported server in your environment.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP iLO monitor.

Learn More

This section includes:

- ["HP iLO Background" below](#)
- ["Supported Versions" below](#)
- ["What to Monitor" below](#)
- ["IPv6 Addressing" on the next page](#)

HP iLO Background

HP Integrated Lights-Out, or iLO, is an embedded server management technology exclusive to Hewlett-Packard but similar in functionality to the Lights out management (LOM) technology of other vendors.

iLO makes it possible to perform activities on an HP server from a remote location. iLO is currently available on all new ProLiant 300/500/blade server models and has a separate network connection (and its own IP address).

iLO actively participates in monitoring and maintaining server health, referred to as embedded health. iLO monitors temperatures in the server and sends corrective signals to the fans to maintain proper server cooling. In addition to temperature monitoring, iLO provides fan status monitoring and monitoring of the status of the power supplies, voltage regulators, and the internal hard drives.

System Information displays the health of the monitored system. These features are available without installing and loading the health driver for the installed operating system. The iLO microprocessor monitors these devices when the server is powered on during server boot, operating system initialization, and operation.

Supported Versions

The HP iLO monitor supports monitoring HP iLO 2.

What to Monitor

The HP iLO monitor makes use of performance counters to measure application server performance, and can be used to provide the following information:

- **Processors.** Displays the available processor slots and a brief status summary of the processor subsystem. If available, installed processor speed in MHz and cache capabilities are displayed.
- **Memory.** Displays the available memory slots and the type of memory, if any, installed in the slot.
- **Drives.** Displays the presence and condition of installed drive bays.
- **Power Supplies.** Displays the presence and condition of installed power supplies.
- **Voltage Regulator Modules (VRMs).** Displays VRM status. A VRM is required for each processor in the system. The VRM adjusts the power to meet the power requirements of the processor supported. A failed VRM prevents the processor from being supported and should be replaced.
- **Fans.** Displays the state of the replaceable fans in the server chassis. This data includes the

area that is cooled by each fan and current fan speeds.

- **Temperatures.** Displays the temperature conditions monitored at sensors in various locations in the server chassis, and the processor temperature. The temperature is monitored to maintain the location temperature below the caution threshold. If the temperature exceeds the caution threshold, the fan speed is increased to maximum.
- **Other.** Other information about the server, such as firmware version and available slots.

IPv6 Addressing

The HP iLO monitor supports IP version 6 addresses if the network and remote server support this protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the HP iLO Monitor

1. Prerequisites

The following are important requirements for using the HP iLO monitor:

- The HP iLO system administrator must configure the service on the ProLiant server so that it can access a command line interface over SSH.
- The configuration should be tested by connecting the server to the SSH client using the configured credentials, and running the following command:

```
show system1 -l 1
```

The result should contain targets and their properties available on the server.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

HP iLO Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>HP iLO server you want to monitor. Select a server from the server list (only those HP iLO remote servers that have been configured in SiteScope are displayed), or click Add Remote Server to add an HP iLO server.</p> <p>Note: When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p>
Add Remote Server	<p>Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
Counters	<p>The server performance counters selected for this monitor. Use the Get Counters button to select counters.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p>Note: When working in template mode, the maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

Chapter 33

HP NonStop Event Log Monitor

Use the HP NonStop Event Log monitor to monitor the Event Logs for added entries on HP NonStop Operating System servers. The HP NonStop Event Log monitor examines events that occurred after the time that the monitor was 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 Monitor Settings to specify values that must appear in the event entry for the entry to match.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP NonStop Event Log monitor.

Learn More

Supported Versions

The minimum officially supported version of the HP NonStop Open System Management (OSM) Event Viewer is T0682 H02 ABU (released May 2009).

Tasks

[How to Configure the HP NonStop Event Log Monitor](#)

Configure the monitor properties as described in the UI Descriptions section below.

[Related workflow](#)

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

HP NonStop Event Log Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
URL	URL of the OSM Event Viewer. Example: https://<nonstopserver>:9991
Match content	Text to look for in the log entries. You can also use a regular expression in this entry to match text patterns. The monitor reports how many times the matched pattern was found. To match text that includes more than one line of text, add an s search modifier to the end of the regular expression. For details, see Regular Expressions Overview in the Using SiteScope Guide. You can also use the Regular Expression Test tool to check your regular expressions. For details, see Regular Expression Tool in the Using SiteScope Guide.
Timeout (seconds)	Amount of time, in seconds, that the monitor should wait for an event before timing-out. Once this time period passes, the monitor logs an error and reports an error status. Default value: 60 seconds
Retries	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. Default value: 0
Time zone	Appropriate time zone, according to the location of the HP NonStop server.
Filter Settings	
Event sources	Collectors or log file name. You can type more than one collector, separated by comma. Events from multiple collectors are merged by generation time. You can also specify a single event log file. Default value: \$ZLOG
Options	Filter options. You can enter more than one option, using commas as separators. Example: CPU 0, PIN 253
Owner	Enter an owner in this field (up to 8 characters).

UI Element	Description
<p>Subsystem names</p>	<p>Subsystem name. You can enter more than one subsystem, using commas as separators.</p> <p>Example: PATHWAY, TMF</p> <p>You can use the full subsystem name (for example, PATHWAY), an existing abbreviated subsystem name (for example, PWY), or the subsystem number (for example, 8).</p>
<p>Event IDs</p>	<p>Event number to filter on a specific event number. You can enter a single event number, a set of event numbers separated by commas, a range a..b, or a set of ranges separated by commas. Event numbers may be signed. If you specify any event numbers, you can only have one subsystem.</p>
<p>Filter files</p>	<p>Filter names. You can enter more than one filter by using commas as separators. You can add more than one filter file, using commas as separators.</p>
<p>Authentication Settings</p>	
<p>Credentials</p>	<p>User name and password required to access the HP NonStop server. Select the option to use for providing credentials:</p> <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.

UI Element	Description
<p>Pre-emptive authorization</p>	<p>Authorization user name and password option if SiteScope requests the target UR:</p> <ul style="list-style-type: none"> • Use global preference. SiteScope uses the authenticate setting as specified in the Pre-emptive authorization section of the General Preferences page. This is the default value. • Authenticate first request. The user name and password are sent on the first request SiteScope makes for the target URL. <p>Note: If the URL does not require a user name and password, this option may cause the URL to fail.</p> <ul style="list-style-type: none"> • Authenticate if requested. The user name and password are sent on the second request if the server requests a user name and password. <p>Note: If the URL does not require a user name and password, this option may be used.</p> <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 user name and Default authentication password specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p>Note: Pre-emptive authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
<p>Client side certificate</p>	<p>The certificate file, if using a client side certificate to access the target URL. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You enter the password for the certificate in the Client side certificate password box.</p> <p>Note: Client side certificate files must be copied into the <SiteScope root directory>\templates.certificates directory.</p>
<p>Client side certificate password</p>	<p>Password if you are using a client side certificate and a password is required.</p>
<p>Accept untrusted certificates for HTTPS</p>	<p>Select if you need to use certificates that are untrusted in the certificate chain to access the target URL using Secure HTTP (HTTPS).</p> <p>Default value: Not selected</p>
<p>Accept invalid certificates for HTTPS</p>	<p>Select if you need to accept an invalid certificate to access the 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> <p>Default value: Not selected</p>
<p>Proxy Settings</p>	

UI Element	Description
HTTP proxy	Domain name and port of an HTTP Proxy Server if a proxy server can be used to access the URL.
Proxy server user name	Proxy server user name if the proxy server requires a name and password to access the URL. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Proxy server password	Proxy server password if the proxy server requires a name and password to access the URL. Note: Your proxy server must support Proxy-Authentication for these options to function.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When configuring this monitor in template mode, you can use regular expressions to define counters.

Chapter 34

HP NonStop Resources Monitor

The HP NonStop Resources monitor enables you to monitor multiple system statistics on a single HP NonStop Operating System server. The error and warning thresholds for the monitor can be set on one or more server system statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP NonStop Resources monitor.

Learn More

This section includes:

- "HP NonStop Resources Monitor Overview" below
- "HP NonStop Resources Monitor" on the previous page

HP NonStop Resources Monitor Overview

Use the HP NonStop Resources monitor to monitor the server system statistics on HP NonStop Operating System servers. You can monitor multiple parameters or measurements with a single monitor instance. This enables you to monitor the remote server for loading, performance, and availability at a basic system level. Create a separate HP NonStop Resources monitor instance for each HP NonStop Operating System server in your environment.

The HP NonStop Resources monitor queries the list of HP NonStop Servers currently configured in the UNIX Remote Servers container. To monitor a remote HP NonStop Operating System server, you must define a NonStop Remote connection profile for the server before you can add an HP NonStop Resources monitor for that server. For details on configuring a remote server, see Remote Servers Overview in the Using SiteScope Guide.

You can also use the Directory, Disk Space, Dynamic Disk Space, File, Log File, and Script monitors to monitor remote servers running on HP NonStop Operating Systems. Monitors that do not depend on a remote operating system, such as FTP, Port, SNMP, SNMP by MIB, and URL family monitors, can also support monitoring on an HP NonStop operating system server.

Tasks

How to Configure the HP NonStop Resources Monitor

1. Prerequisites

To enable monitoring of remote servers running on a HP NonStop Operating System (using either the HP NonStop Resources monitor or the Directory, Disk Space, Dynamic Disk Space, File, Log File, or Script monitor), you must perform the following on the HP NonStop Operating System server:

- a. Create a user for SiteScope monitoring.
- b. In the `/etc/profile` and `.profile` files, perform the following:
 - Comment out the string: `set -o vi`.
 - Set the following parameter: `export PS1='$PWD:`

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Note: When configuring a remote server for monitoring the HP NonStop server, if the remote server gives a choice of TACL shell only, select the remote server in **Remote Servers > UNIX Remote Servers**, and enter the following in the **Main Settings** panel:

- In the **Shell name** field, enter **tac1**.
- In the **Login prompt** field, enter **>**.
- In the **Secondary response** field, enter **OSH**.
- In the **User name** box in the **Credentials** section, enter the user name in the format:
`logon <user_name>`.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

HP NonStop Resources Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the resources you want to monitor are located. Select a server from the server list (only UNIX remote servers that have been configured in SiteScope to run on an HP NonStop operating system are displayed), or click Add Remote Server to add a UNIX server.</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p>
Add Remote Server	<p>Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details (in the Operating System list, you must select NonStopOS). For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
Available Counters	<p>Displays the available measurements for this monitor.</p> <p>For each measurement, select the Objects, Instances and Counters you want to check with the HP NonStop Resources monitor, and click the Add Selected Counters  button. The selected measurements are moved to the Selected Counters list.</p> <p>Note:</p> <ul style="list-style-type: none"> The performance objects and counters available for the HP NonStop Resources monitor vary depending on what operating system options and applications are running on the remote server. When configuring this monitor in template mode, you can use regular expressions to define counters.
Selected Counters	<p>Displays the measurements currently selected for this monitor, and the total number of selected counters.</p> <p>To remove measurements selected for monitoring, select the required measurements, and click the Remove Selected Counters  button. The measurements are moved to the Available Counters list.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 35

IPMI Monitor

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 enables you to watch key operational factors that can seriously affect availability and degrade performance. Create a separate monitor instance for each server you are running.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the IPMI monitor.

Tasks

How to Configure the IPMI Monitor

1. Prerequisites

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.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

IPMI Monitor Settings

User interface elements are described below:

UI Element	Description
Server name	IPMI server name or IP address of the IPMI network adapter. Note: The IP address is normally not the same as the ordinary ethernet NIC adapter address.
Port number	Port number of the IPMI device. Default value: 623
Credentials	Option for providing the user name and password to be used to access the IPMI server: <ul style="list-style-type: none">• Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box.• Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Counters	Displays the server performance counters to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 36

KVM Monitor

The KVM monitor provides a solution for monitoring Kernel-based Virtual Machines (KVM) on Linux x86 and x86_64 hardware that contains virtualization extensions. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch key operational factors that can seriously affect availability and degrade performance. Create a separate monitor instance for each server you are running.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the KVM monitor.

Learn More

This section includes:

- "KVM Monitor Overview" below
- "Supported Versions" below
- "Dynamic Monitoring Mechanism" below

KVM Monitor Overview

KVM is a virtualization technology that allows you to run multiple operating systems, including multiple instances of the same operating system, concurrently on the same physical computer.

SiteScope simplifies the monitoring of virtual infrastructure changes in dynamic, virtualized environments by automatically changing the SiteScope configuration according to changes in the virtual environment. KVM monitors are dynamically updated over time by adding or removing counters and thresholds as virtual machines are added or removed. This enables you to configure the monitor one time, and leave it to automatically discover changes in the environment and update itself.

During initial monitor creation, the monitor uses the connection URI configured to access the VM 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.

Supported Versions

This monitor supports monitoring remote servers running on UNIX remotes only. It has been tested on Linux #29-Ubuntu SMP 3.0.0-16-generic.

Dynamic Monitoring Mechanism

To enable the monitor to dynamically update counters and thresholds, select the counter patterns you want to monitor using a regular expression. For example, if you enter the pattern `./*/Domains Information/./*/Used Memory/`, the monitor retrieves the `Used Memory` counter for all VMs.

Note: SiteScope uses Perl regular expressions for pattern matching. For example, if you enter `/Used Memory.*/` or `Used Memory`, any counters with `Used Memory` in their name match this pattern and are added to the counters list.

You also set the frequency of the dynamic update mechanism at the monitor level. This is the frequency that SiteScope uses to update the counters retrieved from the server. This enables running the update mechanism at a frequency that is appropriate for the monitor type.

During each update, the monitor connects to the VM server and dynamically updates:

- The status of each counter that matches the pattern defined by the regular expression. If there are no available counters on the server, or no counters that match the monitor patterns, the monitor is not updated and it displays the previous counters set.

- Thresholds for the selected counters (every time counters are added or removed as a result of environment changes, the appropriate threshold is added or removed from the monitor).

In this way, the monitor automatically configures itself with counters on the relevant dynamic environment components. Counters that are no longer available on the VMs are automatically removed from SiteScope and no errors are logged.

Note: When you define static counters (with no regular expression), these counters are never removed from the monitor, even if they are no longer available on the server.

Tasks

How to Configure the KVM Monitor

1. Prerequisites

- The monitored VM server must be directly accessible by the SiteScope server (no proxy involved).
- The Virsh and Virt-top command-line tools should be installed on the system. For details, see:
 - <https://help.ubuntu.com/community/KVM/Virsh>.
 - <http://linux.die.net/man/1/virt-top>
 - <http://people.redhat.com/~rjones/virt-top/>

2. Configure the monitor properties

- a. Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **KVM**. The New KVM Monitor dialog box opens.
- b. In the General Settings panel, enter a name and description for the monitor.
- c. In the KVM Monitor Settings panel, select the VM server you want to monitor (or add a new server) and specify the driver to which you want to connect in the **Connection URI** box. For user interface details, see the UI Descriptions section below.
- d. Click the **Get Counter** button, and select the counters you want to monitor from the Select Counters Form. The counters are added to the Preview tree in the **Patterns & Counters** section.
- e. For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
 - Clicking the **Add New Counter**  button to add an empty line to the table, and creating a pattern format using a regular expression.

Tip:

- (1). The pattern should always start and end with the forward slash ("/") character.
- (2). [and] characters which appear as part of counter names should be escaped

(preceded with the backslash ("\") character).
(3). Use "."* to describe any character any number of times.

For example, `./*/Domains Information/./*/Used Memory/` displays Used Memory counter for all VMs.

- o Selecting a static counter, and editing the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.

Note: For details on the maximum number of counters that can be selected from the browsable tree and the maximum number of counters that can match the selected counter patterns when creating and updating dynamic monitors, see ["Maximum Number of Counters That Can be Saved" on page 294](#). If the maximum number of counters that can be deployed is exceeded, an error is written to the **RunMonitor.log**.

- f. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counters Preview tree.
- g. Set the frequency for updating counters from the server, and then click **Verify & Save** or **Save** to save your settings. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- h. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful if a disk fails or for keeping track of the counters that were previously being monitored.
- i. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

3. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the VM server and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:

- The **SiteScope Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

For additional troubleshooting suggestions, see ["Tips/Troubleshooting" on page 294](#).

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

KVM Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the VM server that you want to monitor. Select a server from the server list (only those UNIX remote servers that have been configured in SiteScope are displayed), or click the Add Remote Server to add a new UNIX server.</p> <p>Note:</p> <ul style="list-style-type: none"> When configuring this monitor on SiteScopes running on UNIX versions, only remote servers that have been configured with an SSH connection method are displayed. For details, see How to Configure Remote Windows Servers for SSH monitoring. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.
Server to get measurements from	(Available in template mode only) Name of any SiteScope remote server from which you want to get counters.
Add Remote Server	Opens the Add UNIX Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.
Connection URI	<p>URI of the driver of the VM server that you want to monitor.</p> <p>Default value: qemu:///system</p>
Patterns & Counters	<p>Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.</p> <p>Click the Add New Counter  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the Delete Counter  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the View Matches for Selected Pattern  button to display counters that match the selected patterns.</p> <p>Note: SiteScope uses Perl regular expressions for pattern matching.</p>

UI Element	Description
Get Counters	Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.
Counter Preview	Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.
Frequency of updating counters from server	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p>Default value: 15 minutes</p> <p>Note:</p> <ul style="list-style-type: none"> • The update frequency cannot be less than the monitor run frequency in Monitor Run Settings. • When configuring this setting in a template, the variable value can only be in time units of seconds. • Static counters are never deleted.
Continue displaying counters that no longer exist after update	<p>When selected, counters that no longer exist after running the update mechanism to retrieve counters from the monitored server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful, for example, if a disk fails or for keeping track of counters that were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings on the next update.</p> <p>Default value: Not selected</p> <p>Note: This option is relevant for dynamic counters only (those set using a regular expression). Static counter that are no longer available are still displayed even when this check box is cleared.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section includes:

- "General Notes" below
- "Maximum Number of Counters That Can be Saved" below
- "Troubleshooting Logs" below

General Notes

- When configuring this monitor in template mode, the **Add Remote Server** button is not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- This monitor supports setting fractional thresholds which are more useful than setting whole number thresholds when monitoring large disks (such as 1 terabyte and larger).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).

Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the `_browsableContentMaxCounters` parameter in the `master.config` file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the `_maxCountersForRegexMatch` parameter in the `master.config` file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The `_maxCountersForRegexMatch` parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both `_browsableContentMaxCounters` and `_maxCountersForRegexMatch` parameters in the `master.config` file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

Troubleshooting Logs

- Check for dynamic framework errors in:

- **<SiteScope root directory>\logs\dynamic_monitoring_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
- **<SiteScope root directory>\logs\dynamic_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).
- Check for KVM monitor errors in **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.
- Copy the following sections from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####
# Dynamic Monitoring
#####
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
false
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG,
dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFile
Appender
log4j.appender.dynamic.monitoring.appender.File=./${log.file.path}/dynamic_
monitoring.log
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.Pattern
Layout
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p -
%m%n

# Dynamic monitors changes
category log4j.category.DynamicMonitoringChanges=INFO,
dynamic.monitoring.changes.appender
log4j.additivity.DynamicMonitoringChanges=false
```

Chapter 37

JMX Monitor

This monitor enables you to monitor the performance statistics of those Java-based applications that provide access to their statistics by using the standard JMX remoting technology defined by JSR 160 (remote JMX).

You can also configure and use arithmetic counters in the JMX Monitor to evaluate the growth or contraction rate of linear-based metrics. For details, see ["Arithmetic Counters" on page 299](#).

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the JMX monitor.

Learn More

This section includes:

- ["JMX Monitor Overview" below](#)
- ["Supported Versions" below](#)
- ["Applications Supporting JSR 160" below](#)
- ["Arithmetic Counters" on page 299](#)
- ["WebLogic Application Server Topology" on page 299](#)

JMX Monitor Overview

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 11g (10.3.1-10.3.5) servers can be monitored using a JMX monitor only. For details on how to monitor a WebLogic 11g (10.3.1-10.3.5) server, see ["How to create a JMX Monitor for a WebLogic Server" on page 301](#).
- When monitoring a WebLogic Application Server using a t3 or t3s protocol, you need to use WebLogic's own protocol provider package. For details on how to use the t3 or t3s protocol, see ["How to monitor a WebLogic 10.0, 10.3, or 11g \(10.3.1-10.3.5\) server with an SSL connection using the t3, t3s, iiop or iiops protocol" on page 302](#).
- SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of a WebLogic Application server. For details, see WebLogic Solution Templates in the Using SiteScope Guide.

Supported Versions

This monitor supports monitoring on:

- WebLogic 11g (10.3.1-10.3.5)
- Apache Tomcat 5.0, 5.5, 6.0, 6.0.33, 7.0.25
- Oracle Application Server 10.1.3g
- JBoss servers 4.0.3, 4.2, 5.0, 5.1, 6.0, 6.1, 7.0
- Sun Glassfish Enterprise Server 2.1, 3.1

Applications Supporting JSR 160

Here are some applications that currently support JSR 160 and information about how to monitor them:

- Oracle WebLogic 11g (10.3.1-10.3.5) support JSR 160, which can be enabled on the WebLogic application server by following instructions found on the [Oracle Web site](http://download.oracle.com/docs/cd/E14571_01/apirefs.1111/e13952/taskhelp/channels/EnableAndConfigureIOP.html) (http://download.oracle.com/docs/cd/E14571_01/apirefs.1111/e13952/taskhelp/channels/EnableAndConfigureIOP.html).

Once enabled, the JMX URL for monitoring the server follows the following form:

```
service:jmx:iiop:///jndi/iiop://<host>:<port>/weblogic.management.mbeanservers.runtime
```

where <host> is the server name or IP address that is running your WebLogic application.

For instructions to create a JMX monitor for WebLogic 11g (10.3.1-10.3.5) servers, see "[How to create a JMX Monitor for a WebLogic Server](#)" on page 301.

- Tomcat 5.x and 6.0 support 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 [Oracle Web site](http://download.oracle.com/javase/1.5.0/docs/guide/jmx/tutorial/security.html) for more details (<http://download.oracle.com/javase/1.5.0/docs/guide/jmx/tutorial/security.html>). If the above properties are defined when starting Tomcat 5.x on <host>, the following would be the JMX URL for monitoring it:

```
service:jmx:rmi:///jndi/rmi://<host>:9999/jmxrmi
```

Note: SiteScope 8.x runs within Tomcat 5.x, and can be monitored as described above.

- JBoss 6.1 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.authenticate=false`
 - `-Dcom.sun.management.jmxremote.ssl=false`
 - `-Djboss.platform.mbeanserver`
 - `-Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServerBuilderImpl`
 - `-Djava.endorsed.dirs="%JBOSS_ENDORSED_DIRS%"`
 - `-classpath "%JBOSS_CLASSPATH%" org.jboss.Main %*`
- 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) (<http://www.jcp.org/en/jsr/detail?id=160>).

Arithmetic Counters

Arithmetic counters enable you to evaluate the growth or contraction rate of a selected linear-based metric; this is the linear approximation based on the last two samples collected for the metric. Setting arithmetic counters is useful for metrics that are constantly increasing, making it difficult to define status thresholds. For example, you might want to use arithmetic counters to check the rate of request failures by looking at the "failed request count" metric on a virtual machine.

When using arithmetic counters, you create a new metric based on the original metric for each metric that you want to measure. You can then configure thresholds based on the rate of growth or contraction of these metrics. The threshold status is based on the growth or contraction rate of the counter results or metrics returned by the monitor action as compared with the thresholds set for the monitor.

For example, you can add an arithmetic counter to measure error count (Servlet/ReportsCGI/Adapter///localhost/SiteScope/none/none/errorCount), and set a **Warning** status if Rate on <Server_name>Servlet/ReportsCGI/Adapter///localhost/SiteScope/none/none/errorCount > 2. This means that if average error count grows by more than 2, the status changes from **Good** to **Warning**. Conversely, to measure the rate of contraction in error count, use the less than (" $<$ ") operator.

Results are calculated for arithmetic counters based on the current counter result and on the previous result, and are displayed in the SiteScope Dashboard.

Note: The counter result **n/a** appears where:

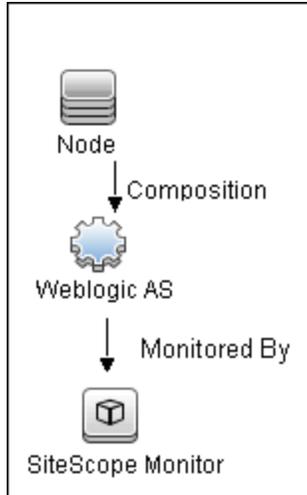
- This is the first monitor run (since there is no previous run result).
- The result of the run (previous and/or current) is not available.
- The result is non-numeric.

For task details, see ["How to create arithmetic counters for a JMX monitor"](#) on page 303.

Note: The JMX monitor currently supports both arithmetic counters and calculated metrics. However, it is planned that arithmetic counters will be removed from the JMX monitor in the future and upgraded to calculated metrics. For details about calculated metrics, see Calculated Metrics Settings in the Using SiteScope Guide.

WebLogic Application Server Topology

The JMX monitor can identify the topology of WebLogic Application Servers. If **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting), the monitor creates the following topology in BSM's RTSM.



Note: The JMX monitor can report topology data to BSM only when monitoring the WebLogic application server, not when monitoring any other environment.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

Tasks

This task includes the following steps:

- "How to create a JMX Monitor for an Apache Tomcat, JBoss, Sun Glassfish Enterprise, or Oracle Application Server" below
- "How to create a JMX Monitor for a WebLogic Server" below
- "How to monitor a WebLogic 11g (10.3.1-10.3.5) server with an SSL connection using the t3, t3s, iiop or iiops protocol" on the next page
- "How to create arithmetic counters for a JMX monitor" on page 303

How to create a JMX Monitor for an Apache Tomcat, JBoss, Sun Glassfish Enterprise, or Oracle Application Server

Configure the monitor properties as described in the UI Descriptions section below.

How to create a JMX Monitor for a WebLogic Server

1. To monitor a WebLogic 11g (10.3.1-10.3.5) server, create a JMX monitor, and enter the following in the **JMX URL** box:

```
service:jmx:iiop:///jndi/iiop://<server_
name>:7001/weblogic.management.
mbeanservers.runtime
```

2. (For WebLogic 6.x, 7.x, and 8.x) To help you to select the counters that you require, you can open a WebLogic monitor for versions prior to WebLogic 9.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.
3. (For WebLogic 11g) To enable monitoring of a WebLogic Application Server 11g, enter the **wfullclient.jar** in the **Additional Classpath** field in the JMX Monitor Settings. You can specify the timeout for JMX task execution (mbeans retrieval and conversion into xml) by modifying the **_overallJMXCountersRetrievalTimeout** property in the **master.config** file. The default value is 15 minutes. This is not an ORB timeout.

Note: For details on creating the **wfullclient.jar**, refer to the Oracle documentation on Using the WebLogic JarBuilder Tool (http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html).

4. Configure the other monitor properties as required

Configure the monitor properties as described in the UI Descriptions section below.

5. Enable topology reporting - optional

To enable topology reporting for WebLogic Application Servers, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "WebLogic Application Server Topology" on page 299.

For user interface details, see BSM Integration Data and Topology Settings in the Using SiteScope Guide.

How to monitor a WebLogic 11g (10.3.1-10.3.5) server with an SSL connection using the t3, t3s, iiop or iiops protocol

When monitoring a WebLogic Application Server using a t3, t3s, iiop or iiops protocol, you need to use WebLogic's own protocol provider package.

Note: When monitoring a WebLogic server with the Administration port enabled, the t3s protocol must be used.

1. Enter the URL in the following format in the **JMX URL** box of JMX Monitor Settings:

■ **For t3 protocol:**

```
service:jmx:t3://<host>:<port>/jndi/weblogic.management.mbeanservers.runtime
```

where the default port for t3 protocol is 7001

■ **For t3s protocol:**

```
service:jmx:t3s://<host>:<port>/jndi/weblogic.management.mbeanservers.runtime
```

where the default port for t3s protocol is 7002

■ **For iiop protocol:**

```
service:jmx:iiop:///jndi/iiop://host:port/weblogic.management.mbeanservers.runtime
```

■ **For iiops protocol:**

```
service:jmx:iiops://host:port/jndi/weblogic.management.mbeanservers.runtime
```

2. (For t3 or t3s protocols) Copy the following jars from the WebLogic library to any folder on the SiteScope server:

- **%WEBLOGIC_HOME%\server\lib\wlclient.jar**
- **%WEBLOGIC_HOME%\server\lib\wljmxclient.jar**
- **%WEBLOGIC_HOME%\server\lib\weblogic.jar**
- **%WEBLOGIC_HOME%\server\lib\wlfullclient.jar**
- **%WEBLOGIC_HOME%\server\lib\webserviceclient+ssl.jar** (for t3s protocol only)
- **%WEBLOGIC_HOME%\server\lib\cryptoj.jar** (for t3s protocol only, if this file is present in WebLogic library)

Specify the full path to the copied jars in the **Additional Classpath** field in the JMX Monitor Settings separated by “;”.

Note: For details on creating the **wfullclient.jar**, refer to the Oracle documentation on Using the WebLogic JarBuilder Tool (http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html).

3. (For iiop or iiops protocols) Copy the following jars from the WebLogic library to any folder on the SiteScope server:

- **%WEBLOGIC_HOME%\serverlib\wfullclient.jar**
- **%WEBLOGIC_HOME%\serverlib\wlcipher.jar** (for iiops protocol only)

Specify the full path to **wfullclient.jar** in the **Additional Classpath** field in the JMX Monitor Settings.

For details on creating the **wfullclient.jar**, refer to the Oracle documentation on Using the WebLogic JarBuilder Tool (http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html).

4. (For t3s and iiops protocols) Enable SSL on the WebLogic server and import the SSL certificate into the SiteScope keystore. For details, see Certificate Management Overview.
5. Configure the other monitor settings as required.

For details, see [Settings Common to All Monitors](#) in the Using SiteScope Guide.

How to create arithmetic counters for a JMX monitor

To evaluate the growth or contraction rate of linear-based metrics:

1. Create a JMX monitor, and add counters in the JMX Monitor Settings panel. For user interface details, see "JMX Monitor Settings" on page 305.
2. In the Arithmetic Counters area, click the **Add Arithmetic Counters**  button. In the **Original Counter** box, select the counter on which to base the arithmetic counter.

The new counter is added to the table with **Operator** set to **Rate**, and the arithmetic counter name is added to the **Arithmetic Counter Name** box in the format `Rate on <original counter name>`.

Note: When working in template mode, you cannot use arithmetic counters that contain variables in the original counter.

3. In the **Threshold Settings** tab, select the arithmetic counter and set logic conditions that determine the reported status of each monitor instance.

Results are calculated for arithmetic counters based on the current counter result and on the previous result, and appear in the Dashboard.

Note: The counter result **n/a** appears where:

- This is the first monitor run (since there is no previous run result).

- The result of the run (previous and/or current) is not available.
- The result is non-numeric.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

JMX Monitor Settings

User interface elements are described below:

UI Element	Description
JMX URL	<p>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:</p> <ul style="list-style-type: none">When creating a JMX monitor for a WebLogic 11g server, enter the following URL: <code>service:jmx:iiop:///jndi/iiop://<host>:<port>/weblogic.management.mbeanservers.runtime.</code>When creating a JMX monitor for a JBoss server, your system administrator should configure the JBoss server, and then report which ports are enabled for JMX access.If you are using a t3 or t3s protocol, you need to use WebLogic's own protocol provider package and the JMX URL is in a different format. For details, see "How to monitor a WebLogic 11g (10.3.1-10.3.5) server with an SSL connection using the t3, t3s, iiop or iiops protocol" on page 302.The JMX over RMI protocol is not firewall friendly.
Domain filter	<p>Domain filter to show only those counters existing within a specific domain (optional). This filter does not have full regular expression support.</p> <p>You can specify the domain name or full path to MBean. The full path can be taken from the MBean objectName property using JConsole.</p> <p>Example: Note that these MBean examples have different node properties in the path: <code>type-host-path</code> in the first and <code>type-resourcetype-name</code> in the second.</p> <ul style="list-style-type: none">For MBean "Catalina/Cache/localhost/SiteScope" specify: <code>"Catalina:type=Cache,host=localhost,path=/SiteScope"</code>For MBean "Catalina/Environment/Global/simpleValue" specify: <code>"Catalina:type=Environment,resourceType=Global,name=simpleValue"</code>
User name	User name for connection to the JMX application (optional).
Password	Password for connection to the JMX application (optional).

UI Element	Description
Timeout (seconds)	Amount of time, in seconds, to wait for a response from the server before timing-out. After this time period passes, the monitor logs an error and reports an error status. Default value: 60 seconds (using a value other than the default timeout value may adversely affect performance)
Additional Classpath	Specify the classpath library that is used to resolve unknown classes retrieved from the JMX server. Multiple libraries can be entered separated by a semicolon. Note: When monitoring a WebLogic Application Server 11g, this field is mandatory, and the wfullclient.jar must be used. For details on creating the wfullclient.jar , refer to Using the WebLogic JarBuilder Tool (http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html).
Counters	Server performance counters to check with this monitor. Use the Get Counters button to select counters. When the server being monitored is a WebLogic 11g server, see "How to create a JMX Monitor for a WebLogic Server" on page 301 for further details.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.
Arithmetic Counters	
	Add Arithmetic Counter. Adds a row to the Arithmetic Counters table, enabling you to add an arithmetic counter. Note: When working in template mode, you cannot use arithmetic counters that contain variables in the original counter.
	Delete Arithmetic Counter. Deletes the selected arithmetic counter from the Arithmetic Counters table.
Original Counters	The path and name of the original counter on which the arithmetic counter is calculated.
Operator	The operator (Rate) that is performed on the counter. The value in this column is not editable.
Value	This column is blank, and is not editable for the Rate operator.
Arithmetic Counter Name	The name of the arithmetic counter. This is the name of the original counter on which the arithmetic counter is calculated with "Rate on" prefix. The value in this column is not editable.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section includes:

- "General Notes/Tips" below
- "Troubleshooting and Limitations" below

General Notes/Tips

- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- The maximum number of counters that you can select for the JMX monitor is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.
- The JMX over RMI protocol is not firewall friendly.

Troubleshooting and Limitations

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 platforms, 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 in the SiteScope 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**.

Chapter 38

LDAP Monitor

This monitor enables you to verify 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the LDAP monitor.

Learn More

This section includes:

- ["LDAP Monitor" on the previous page](#)
- ["Status" below](#)

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.

LDAP traffic is transmitted unsecured by default. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL) and installing a properly formatted certificate.

Status

Each time the LDAP monitor runs, it returns a status based on the time it takes to perform the connection. An error status or warning status is returned if the current value of the monitor is anything other than good. Errors occur if SiteScope is unable to connect, receives an unknown host name error, or the IP address does not match the host name.

Tasks

How to Configure the LDAP Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **LDAP Authentication Tool** is available when configuring this monitor to test an LDAP server can authenticate a user by performing a simple authentication (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Link Check Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

LDAP Monitor Settings

User interface elements are described below:

UI Element	Description
Authentication Settings	
LDAP service provider	<p>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.</p> <p>Note:</p> <ul style="list-style-type: none">• By default, LDAP version 2 is used. To use LDAP version 3, type [LDAP-3] before the URL.• To enable LDAP over SSL, type [LDAP-SSL] before the URL.
Security principal	<p>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.</p> <p>Example: <code>uid=testuser,ou=TEST,o=mydomain.com</code></p> <p>Note: To prevent binary data appearing in the output of LDAP queries, all binary attributes should be listed in the LDAP binary attributes field in Preferences > Infrastructure Preferences > General Settings.</p>
Security credential	<p>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.</p>
LDAP Settings	

UI Element	Description
Content match	<p>Text string 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.</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>
Object query	<p>An object query to look at an LDAP object other than the default user <code>dn</code> object. For example, enter the mail object to check for an email address associated with the <code>dn</code> object entered above. You must enter a valid object query in this text box if you are using a LDAP filter (see the description below).</p> <p>For more information on LDAP queries, see http://technet.microsoft.com/es-es/library/aa996205(EXCHG.65).aspx.</p> <p>Note: To use LDAP version 3 for a particular monitor, type <code>[LDAP-3]</code> before the query. If you want to use version 2 and version 3, type <code>[LDAP-ANY]</code>.</p>
LDAP filter	<p>Performs an LDAP 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://download.oracle.com/javase/jndi/tutorial/basics/directory/filter.html.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

The monitor run summary string is limited to 100 characters. If the LDAP response is larger than the default value, you can increase this limit by adding the property **_ldapMaxSummary=<# of symbols in summary>** to the **<SiteScope root>\groups\master.config** file, and then restart SiteScope.

Chapter 39

Link Check Monitor

This monitor 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Link Check monitor.

Learn More

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 a link report log file named `LinkReport_<group name><number>.log` (this should not be confused with the daily logs). It also writes the total number of link errors, 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 **Maximum hops** box of the Monitor Settings panel.

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.

Tasks

How to Configure the Link Check Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Link Check Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
URL	<p>URL that is the starting point for checking links. The link monitor retrieves the page for this URL and 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:<code>http://demo.thiscompany.com</code></p>
Search external links	<p>The monitor follows 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.</p> <p>Default value: Not selected</p>
Pause (milliseconds)	<p>Delay, in milliseconds, between each link check. Larger numbers lengthen the total time to check links but decrease the load on the server.</p> <p>Default value: 250 milliseconds</p>
Timeout (seconds)	<p>Amount of time, in seconds, that the monitor should wait for a page to begin downloading before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p>Default value: 60 seconds</p>
Maximum links	<p>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.</p> <p>Default value: 800</p>

UI Element	Description
Maximum hops	<p>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 enter your own limit, enter a numeric value in the Other values box.</p> <p>Default value: Main page links</p> <p>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.</p>
POST data	<p>Form values required for the first page being checked. This is useful if you need to log on using an HTML form to reach the rest of the site that you are checking. Enter form values in the format <code>key=value</code> (one on each line).</p>
Authorization Settings	
Authorization user name	User name to access the URL if required.
Authorization password	Password to access the URL if required.
Proxy Settings	
HTTP proxy	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URL.
Proxy server user name	Proxy server user name if the proxy server requires a name to access the URL. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Proxy server password	Proxy server password if the proxy server requires a name to access the URL. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 40

Log File Monitor

The Log File monitor checks for specific entries added to a log file by looking for entries containing a text phrase or a regular expression.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Log File monitor.

Learn More

This section includes:

- "Log File Monitor Overview" below
- "Supported Versions" below
- "Customizing Log File Content Matches and Monitor Alerts" below
- "Support for IPv6 Addresses" on the next page

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 329.

Supported Versions

The Log File monitor supports monitoring remote servers running on Windows, UNIX, and HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see "How to Configure the HP NonStop Resources Monitor" on page 282.

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 Log File Monitor Settings, configure the following settings:
 - **Run alerts:** Select the **For each log entry matched** option.
 - **Content match:** Enter the text to look for in the log entries. For example, to find text entries `redflag` and `disaster` in the log file, enter `/(redflag|disaster)/`.
 - **Match value label:** Enter a label name for the matched values found in the target log file. For example, type `matchedValue`.
2. In the Threshold Settings, set the error and warning threshold. For example, set `Error if matchedValue == disaster` and set `Warning if matchedValue == redflag`.
3. 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 How to Configure an Alert in the Using SiteScope Guide.

Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the following protocols are supported:

- NetBIOS (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

This section includes:

- "How to Configure the Log File Monitor" below
- "How to Use the Rules File" below

How to Configure the Log File Monitor

1. Prerequisites

The following configuration requirements must be performed or verified before the Log File monitor can be used:

- The log file to be monitored must exist, and be accessible under credentials used for connecting to the remote server, or under which SiteScope is running (if monitoring a local file).
- The remote server should be created with credentials that grant read access on the monitored file.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Note: 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.

How to Use the Rules File

In special cases, it may be necessary to create a custom rules file to specify different alerts for different log entry matches. When an application log message is read, this file is used to decide what action to take. An example rules file is located in **<SiteScope root directory>\examples\log_monitor\sample.rules**.

To use the sample.rules file:

1. Make a copy of the sample.rules file located in the <SiteScope root directory>\examples\log_monitor directory, and rename it. There is no required naming convention.
2. Open the renamed file with an editor of your choice, and edit the file to meet your needs.

Each rule is a line of tab delimited fields in the format:

```
column<tab>match<tab>continue<tab>action<sp>actionParam1<sp>  
actionParam2<sp>...
```

where:

column is the column number (in ascending order starting from 0) of the log file to read, or ANY, or RULE to define a rule. Using ANY for the column checks the entire log message.

match is the text to match.

continue determines whether to continue searching the table.

action is the name of the alert action: SNMPTrap, Mailto, Page, Run, DatabaseAlert, Disable, NTLogEvent, SMS, Sound.

actionParameters are action specific parameters.

Note: Lines starting with "#" are ignored as comments.

Action descriptions:

Action	Parameters
SNMP	The first parameter is the beginning of the SNMP message (use "^" for spaces). The second parameter is the template file from the templates.snmp directory.
Mailto	The first parameter is the address where the message is sent. The second parameter is the template file from the templates.mail directory.
Page	The first parameter is added to the beginning of the pager message (use "_" for spaces). The second parameter is the template file from the templates.page directory.
Run	The first parameter is the machine. If the script is to be run on a local machine, this parameter should be skipped. For a remote machine, the machine name should be prefixed with "remote:". The second parameter is the script file from the scripts directory. The third parameter is the template file from the templates.script directory. The fourth parameter is for the parameters. Use "_" as a separator between each parameter passed to a script. Use "#" before the property name to pass parameters from a monitor. You can use any property from the SiteScope Alert Template and Event Properties Directory. Note that "_" should be replaced with "#" when passed as a parameter to a script.
Using counters	Whenever linkCategory is set to a linkError, there is a linkErrorCount that counts the number of errors found. This is reset only when linkCategory is set to linkOk (when this occurs, linkOkCount starts counting matches).

- When you are finished, enter the full path to your rules file.

Examples:

Here are some examples for rules. Note that most of them use SNMP as the action, but you can define any other action in your rules file.

Sample rule to forward trap if second column of log entry contains ERROR:

```
2 ERROR n SNMPTrap error^in^column^two LogMessage
```

Sample rule to forward trap if any part of log entry contains ERROR:

```
ANY ERROR n SNMPTrap error^in^log LogMessage
```

Sample rule to forward trap and override default SNMP preferences:

```
ANY ERROR n SNMPTrap error^in^log LogMessage _snmpHost=206.168.191.19 _  
snmpObjectID=.1.3.6.1.4.1.11.2.17.1 _snmpCommunity=public _snmpGeneric=6 _  
snmpSpecific=411
```

Sample rule to send a pager message when first column contains DOWN:

```
1 DOWN n Page help_help_help
```

Sample rule to send email when first column contains DOWN:

```
1 DOWN n Mailto sysadmin@this-company.com
```

Sample rule to send two alerts when second column contains DEAD:

```
2 DEAD y SNMPTrap app^is^dead LogMessage  
2 DEAD n Mailto sysadmin@this-company.com
```

Sample default rule to always forward log messages as SNMP traps:

```
ANY ANY n SNMPTrap default^rule LogMessage
```

Sample rule to run script when the log file contains ERROR:

```
ANY Error n Run mailtest.bat
```

Sample rule that runs a script with default template, and passes as parameters the value matching the regular expression between the () found in the log file and the log file name:

```
ANY /(regularExp)/ y Run LogIt-LF.vbs Default <value>_<#logFile>
```

Sample matching rules to set link category used by escalation:

```
ANY LinkDowny SetCategory linkCategory linkError
ANY LinkUp SetCategory linkCategory linkOk
```

Sample escalation rules for link category:

```
# first, send trap when problem happens the first time
RULE linkCategory y SNMPTrap first^alert LogMessage linkCategory = linkError and
linkErrorCount = 1

#

# second, after a minute send four traps

RULE linkCategory y SNMPTrap second^alert LogMessage linkCategory = linkError and
linkErrorTimeSinceFirst > 60 and linkErrorAlertCount < 4

#

# third, after five minutes, send five traps, at the rate of no more than one trap per minute

RULE linkCategory y SNMPTrap third^alert LogMessage linkCategory = linkError and
linkErrorTimeSinceFirst > 300 and linkErrorTimeSinceAlert > 60 and linkErrorAlertCount <
5

#

# send trap when problem is fixed

RULE linkCategory y SNMPTrap fourth^alert LogMessage linkCategory = linkOk and
linkOkCount = 1

#

# run script when problem happens the first time

RULE linkCategory y Run mailtest.bat linkCategory = linkError and linkErrorCount = 1
```

Sample rule to always send a trap:

```
ANY ANY n SNMPTrap default^rule LogMessage
```

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Log File Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Server	<p>Server where the file you want to monitor is located. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note: If using NetBIOS to connect to other servers in an Windows domain, use the UNC format to specify the path to the remote log file.</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none">• Browse servers. Select a server from the drop-down list of servers visible in the local domain.• Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server (if the monitor does not work for one of these conditions, the other condition must be fulfilled, since both conditions do not always work on some machines). For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Log file path	<p>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 on to the remote machine.• For reading log files on remote Windows servers using the NetBIOS method, use UNC to specify the path to the remote log file. Example: <code>\\remoteserver\sharedfolder\filename.log</code>• For reading log files on remote Windows servers using the SSH method, specify the local path of the remote log file on the remote machine. Example: <code>C:\Windows\System32\filename.log</code> 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 <i>How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide</i>. <p>You can also monitor files local to the server where SiteScope is running. Example: <code>C:\application\appLogs\access.log</code></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 <i>SiteScope Date Variables in the Using SiteScope Guide</i>.</p>

UI Element	Description
<p>Run alerts</p>	<p>Method for running alerts for this monitor.</p> <ul style="list-style-type: none"> • For each log entry matched. The monitor triggers alerts according to thresholds applied to each matching entry found. Since status can change according to thresholds for each matched entry, each alert action could be triggered many times within a monitor run. <p>Example: If you want to send a warning alert on matched text value "power off" and an error alert if more than one server is turned off, set the following thresholds:</p> <ul style="list-style-type: none"> ▪ <code>Error if matchCount > 1</code> ▪ <code>Warning if value == 'power off'</code> <p>To send an error alert if only one threshold is matched, set <code>Error if value == 'power off'</code>.</p> <p>For details on how to create a Log File monitor that triggers customized alerts for content matches, see "Customizing Log File Content Matches and Monitor Alerts" on page 321.</p> <ul style="list-style-type: none"> • Once, after all log entries have been checked. 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>
<p>Check from beginning</p>	<p>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>
<p>Content match</p>	<p>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. The <code>/c</code> search modifier is not supported when Server-side processing is enabled. For details, see Regular Expressions Overview in the Using SiteScope Guide.</p> <p>Note: When you create a report by clicking the monitor title, the report includes up to 10 values.</p>

UI Element	Description
Open Tool	Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.
Advanced Settings	
Log file encoding	<p>If the log file content to be monitored uses an encoding that is different than the encoding used on the server where SiteScope is running, select 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>Default value: windows-1252</p>
Rules file path	<p>Enter the full path to your rules file. In special cases, it may be necessary to create a custom rules file to specify different alerts for different log entry matches. You can also set a parameter in the rules file to run script alerts. You can use any of the properties in the SiteScope Alert Template and Event Properties Directory in the Using SiteScope Guide.</p> <p>An example rules file is located in <SiteScope root directory>\examples\log_monitor\sample.rules. For instructions on how to use the file and example rules, see "How to Use the Rules File" on page 323, or read the instructions in the file itself.</p>
Match value labels	<p>Use to enter 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 enter more than four match value labels, when you create a report by clicking the monitor title, the report includes only the first four values.</p>
Multi-line match	<p>Runs a regular expression match on multiple lines of text.</p> <p>Default value: Not selected</p>

UI Element	Description
<p>Server-side processing</p>	<p>Processes log file data on the server-side. Benefits include low memory usage and low CPU utilization on the SiteScope server, and faster monitor run. Server-side processing does however cause high CPU utilization on the remote server when processing the file.</p> <p>Default value: Not selected (we recommend using this option only if SiteScope performance is affected by large amounts of data being appended to the target log file between monitor runs, and the Log File monitor is performing badly in regular mode).</p> <p>Note:</p> <ul style="list-style-type: none"> • Server-side processing is enabled for remote Linux, Red Hat Enterprise Linux, and Oracle Solaris servers only. Windows SSH is not supported. • To enable server-side processing to work correctly when monitoring on a Solaris server, open the remote server settings for the monitored host (Remote Servers > UNIX Remote Servers > Main Settings), and enter a path to the bash interpreter in the Initialize shell environment field. • "Rule files" are not supported in this mode. • The <code>/c</code> search modifier is not supported in this mode. • The encoding for the remote server must be Unicode, or match the encoding of the log file (if the remote file is in Unicode charset).
<p>No error if file not found</p>	<p>Monitor remains in Good status if the file is not found. The monitor status remains Good regardless of the monitor threshold configuration.</p> <p>Default value: Not selected</p>
<p>Timeout Settings</p>	
<p>Enable timeout</p>	<p>The monitor stops its run after the specified timeout period has been exceeded.</p> <p>Default value: Not selected</p>
<p>After timeout, resume reading from end of file</p>	<p>If selected, the monitor resumes reading from the end of the log file during the next run, instead of from the current location.</p> <p>Default value: Selected</p> <p>Note: This setting is only available when Enable timeout is selected.</p>
<p>Status after timeout</p>	<p>The status condition that the monitor goes into if the monitor times out.</p> <p>The status categories include: Error, Warning, Good</p> <p>Default value: Warning</p> <p>Note: This setting is only available when Enable timeout is selected.</p>

UI Element	Description
Timeout (seconds)	Amount of time, in seconds, that SiteScope should wait before the monitor times out. Default value: 60 seconds Note: This setting is only available when Enable timeout is selected.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Tips/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When monitoring a log file on a FreeBSD remote server, make sure the correct path to the "cat" command is used in **<SiteScope root directory>\templates.os/FreeBSD.config**, since the command was moved in the latest FreeBSD versions.

Chapter 41

Mail Monitor

The Mail monitor checks to see that the mail server is both accepting and delivering messages. Use this monitor to verify that all your mail servers, including internal servers where a firewall is used, are working properly.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Mail monitor.

Learn More

Mail Monitor Overview

The Mail monitor checks 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. 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. If SiteScope is unable to complete the entire loop, it generates an error message.

We recommend that you 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 email messages send by SiteScope.

Tasks

How to Configure the Mail Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Mail Round Trip Tool** is available when configuring this monitor to verify that the mail server is accepting requests and that a message can be sent and retrieved (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Mail Round Trip Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Mail Monitor Settings

User interface elements are described below:

UI Element	Description
Action	<p>Action the Mail monitor should take with respect to the mail server:</p> <ul style="list-style-type: none">• Send and receive. This option enables 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 enables 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. <p>Note: If the this option is selected, the Match content box must have a value to match against. Also, if this 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, and neither can retrieve the messages.</p> <ul style="list-style-type: none">• Send only. This option checks that the receiving mail server has accepted the message.
Sending email server (SMTP)	<p>Host name of the SMTP mail server to which the test mail message should be sent.</p> <p>Example:mail.thiscompany.com</p>
Send to address	<p>Mail address to which the test message should be sent.</p>
Receiving protocol	<p>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 email server	<p>Host name 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>

UI Element	Description
Receiving email server user name	<p>POP user account name on the receiving mail server. A test email 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: <code>support</code></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 email server password	<p>Password, if necessary, for the receiving mail account.</p>
Receive only content match	<p>Text string to match against the contents of the incoming message. If the text is not contained in the incoming message, the monitor reports an error. This is for the receiving only option. The search is case sensitive.</p> <p>Example: <code>Subject:MySubject</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 (for example, <code>< B> Hello< /B> World</code>). 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 <code>i</code> after the trailing slash indicating case-insensitive matching.</p> <p>Example: <code>/href=Doc\d+\.html/ or /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.</p> <p>Example: <code>/Temperature: (\d+)/</code></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>
Attachment	<p>Full path of a file to add as an attachment to the email message. Use this option to check that your email 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: <code>s/C:\firstdir\shortYear\$\$0month\$\$0day\$/</code></p>

UI Element	Description
Attachment encoding	The code page or encoding to use if the attachment file content uses an encoding that is different than the encoding used on server where SiteScope is running. This may be necessary if the code page which SiteScope is using does not support the character sets used in the attachment file. Default value: windows-1252
Timeout (seconds)	Amount of time, in 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. Default value: 300 seconds
POP check delay (seconds)	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. Default value: 10 seconds
SMTP user	User name required for SMTP authentication if the SMTP server requires authentication before sending messages.
SMTP password	Password for the SMTP authentication (if required).
NTLM authentication	NTLM authentication version (1 or 2) if used by the email server. Default value: none

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 42

MAPI Monitor

This monitor enables you to monitor the availability of Microsoft Exchange 2003 and 2007. The monitor checks for email delivery time. This enables you to verify availability of the MAPI server by sending and receiving a test message in a Microsoft Exchange email account.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the MAPI monitor.

Learn More

This section includes:

- ["MAPI Monitor Overview" below](#)
- ["Supported Versions" below](#)

MAPI Monitor Overview

The MAPI monitor checks a Messaging Application Program Interface (MAPI) server to confirm that email operations can be run. The monitor is designed to test the operation of a Microsoft Exchange Server 2003/2007, and for Outlook 2007. 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 email 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 email 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 email delivery time. Create a separate MAPI monitor instance for each Microsoft Exchange server in your environment.

Supported Versions

This monitor is supported in SiteScopes that are running on Windows versions only.

Tasks

This section includes:

- "How to Prepare the System for Using the MAPI Monitor" below
- "How to Configure the MAPI Monitor" on page 344

How to Prepare the System for Using the MAPI Monitor

Note: The following are 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).

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 Settings panel supports up to two mailboxes per Exchange Server. If only one mailbox is specified in the MAPI Monitor Settings the same mailbox can be used for the sender and receiver accounts.

Consult your Exchange system administrator for 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 the previous step, which are by definition domain logons, must be added to the Administrators group on the SiteScope server.

- a. 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.
- b. Double-click the Administrators group icon to open the Administrators Properties window.
- c. 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 on to the SiteScope server as the MailBox User created in the first step, the Outlook wizard may start setting up an Outlook profile for the mail box. If an Outlook client is already installed, you can use 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.

Creating an Outlook profile is not necessary, although it may be helpful for the purpose of troubleshooting. After the wizard prompts you to set up a profile you can cancel to exit the wizard.

5. Verify the SiteScope user logon is a member of Administrators group or a domain administrator account

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:

- a. Open the **Services** control utility on the SiteScope server.
- b. Right-click the SiteScope service entry and click **Properties**. The SiteScope Properties settings page opens.
- c. Click the **Log On** tab.
- d. 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 enter the SiteScope user logon.
- e. 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.

- a. Click **Start > Programs > Administrative Tools > Local Security Policy**. The Local Security Policy panel opens.
- b. Click the **Local Policies** folder in the left pane and then click the **User Rights Assignments** folder to display the list of policies.
- c. Double-click the **Act as part of the operating system** policy item in the right pane. The Local Security Policy Setting list opens.
- d. 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.
- e. Enter the SiteScope user logon using the **domain\logon** format if the SiteScope user is a

domain account.

- f. 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**.
- g. Restart the SiteScope service after making changes to security policy.

How to Configure the MAPI Monitor

1. Prerequisites

Before configuring the monitor, make sure the system is prepared for using the MAPI monitor as described in ["How to Prepare the System for Using the MAPI Monitor" on page 342](#).

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

MAPI Monitor Settings

User interface elements are described below:

UI Element	Description
Receiver server	Host name 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. We recommend that you copy the server name as it appears in the Properties of the email account you are using with this monitor.
Receiver mailbox	Name (alias) of the mailbox to be used for this monitor. This is often the email account name but it may be a different name. We recommend that you copy the mailbox name as it appears in the E-Mail Account properties for the email account you are using with this monitor.
Receiver domain	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	Windows account login name for the user associated with the above email account.
Receiver password	Windows account login password for the user name above.
Sender server	Sender's Microsoft Exchange server name. Note: <ul style="list-style-type: none"> • The MAPI sender is ignored if an SMTP sender is specified in the Sender box below. • If any of the SMTP sender values are not specified, the receiver values are used instead.
Sender mailbox	Alias of the sending mailbox.
Sender domain	Domain to which both the sending mailbox owner and the sending Microsoft Exchange server belong.
Sender user name	Login name for the Windows account of the sending mailbox owner.
Sender password	Windows account login password for the sender account above.

UI Element	Description
Transaction timeout (seconds)	Amount of time, in 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 email message is delivered. Default value: 25 seconds
SMTP server	SMTP server through which an outgoing message is sent. Note: If you set any of the SMTP values (SMTP server , Sender or Receiver) they override the MAPI sender options.
Sender	Email address of the SMTP sender.
Receiver	Email address of the receiver. This must match the Receiver mailbox alias specified above.
Attachment	Full path of a file to attach to the outgoing SMTP message.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 43

Memcached Statistics Monitor

The Memcached Statistics monitor checks whether a memcached server is responding to a remote stats request, and stores the values returned in the response to a successful stats request.

Memcached is a high-performance, distributed memory object caching system, intended for use in speeding up dynamic web applications by alleviating database load. You can create a separate monitor instance for each Memcached server you are running. You may want to set up multiple monitors per server if several Memcached services were started on the different ports.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Memcached Statistics monitor.

Learn More

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the TCP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Memcached Statistics Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Memcached Statistics Monitor Settings

User interface elements are described below:

UI Element	Description
Host	Name of the Memcached server that you want to monitor.
Port	Port used by the Memcached Statistics server. Default value: 11211
Timeout (milliseconds)	Amount of time, in milliseconds, to wait for the connection to the port, and for any sending and receiving to complete. Once this time period passes, the Memcached Statistics monitor logs an error and reports an error status. Default value: 10000 milliseconds
Counters	Server statistics selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note: <ul style="list-style-type: none"> The counters displayed are those received during the timeout period, and may not include all the counters available on the server. Specifying a longer timeout in the Timeout (milliseconds) field may result in receiving more counters. The total time for receiving the counters may be longer than the timeout specified, due to additional processing time not part of the request/response period. The total number of counters that can be monitored is limited to 100. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 44

Memory Monitor

This monitor enables you to track how much physical and 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. Use this page to add a monitor or edit the monitor's properties.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Memory monitor.

Learn More

This section includes:

- "Memory Monitor Overview" below
- "Supported Platforms/Versions" below
- "IPv6 Addressing Supported Protocols" below

Memory Monitor Overview

Memory is one of the primary factors that can affect your server's performance. Use the Memory monitor to monitor how much physical and virtual memory (which consists of both physical memory and swap memory) is currently in use on a server and how much space is free. Use the pages per second and value of free memory measurements to help detect problems in this area. Each time the Memory monitor runs, it collects the measurements and displays the status in the SiteScope Dashboard.

In most environments, the Memory monitor does not put a heavy load on your server. For monitoring remote UNIX servers, SiteScope needs to open the connection, while getting the data from 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 can use the error and warning thresholds to have SiteScope notify you if memory on a remote server starts to get low.

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms.
 - If you are monitoring a Windows remote server using the NetBIOS method, only virtual memory counters are available.
 - This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see *Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide*.
 - Physical memory (free space and used %) can only be monitored on Windows remote servers using the WMI connection method.
- This monitor is also supported in SiteScopes that are running on UNIX versions if the remote server being monitored has been configured for SSH. For details, see *SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide*.
 - On UNIX remote servers, monitoring physical and virtual memory is not supported using the rlogin connection method.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Memory Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Performance Counters Tool** is available when configuring this monitor to check performance counters on a specific machine in a Windows network (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Performance Counters Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Memory Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the memory you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note: When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none">• Browse servers. Select a server from the drop-down list of servers visible in the local domain.• Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section describes troubleshooting and limitations for the Memory monitor.

- ["General Notes/Tips" below](#)
- ["Troubleshooting and Limitations" below](#)

General Notes/Tips

When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Memory monitor.

- ["Percentage of Virtual Memory Used Reaches 100%" below](#)
- ["Pages Per Second is Affecting System Performance" below](#)
- ["WMI Returns Incorrect Memory Values" on the next page](#)

Percentage of Virtual Memory Used Reaches 100%

Problem: The number of virtual memory used % reaches 100%, and services that are running may fail and new ones are unable to start. Virtual memory used % measures the percentage of memory and paging file space used.

Solution 1: Increase the size of the paging file. This 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** to view the memory used by each service. For details on using the tool, see [Processes Tool](#) in the [Using SiteScope Guide](#).

Solution 2: 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](#) in the [Using SiteScope Guide](#). For details on using the Service monitor, see ["Service Monitor" on page 567](#).

Solution 3: Install an upgraded version of the service without the leak.

Note: 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" on page 653](#).

Pages Per Second is Affecting System Performance

Problem: The number of pages per second is consistently high (>10 pages/sec) and is affecting system performance. Pages per second measures the number of virtual memory pages that are moved between main memory and disk storage.

Solution 1: Add more memory.

Solution 2: 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.

WMI Returns Incorrect Memory Values

WMI returns incorrect values for the memory used % and MB free counters when the WMI connection method is used on a Windows Server 2008. This is due to an issue with WMI (not SiteScope).

Monitor running on AIX remote servers does not monitor physical memory usage

Problem: When the Memory monitor is configured to monitor a remote server running on an AIX operating system, the monitor does not monitor physical memory usage.

Solution: Make sure that the login account used for the remote connection has access to the `svmon` command.

Chapter 45

Microsoft ASP Server Monitor

This monitor enables you to monitor the availability of a Microsoft ASP server on Windows systems. The error and warning thresholds for the monitor can be set on one or more ASP server performance statistics. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each ASP Server you are running.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft ASP Server monitor.

Learn More

This section includes:

- "Supported Platforms/Versions" below
- "IPv6 Addressing Supported Protocols" below

Supported Platforms/Versions

- Use the Microsoft ASP Server monitor to monitor Active Server Pages (ASP) performance parameters on Microsoft Windows NT Terminal Server 4.0 and Microsoft Windows 2000 Server.
- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Microsoft ASP Server Monitor

1. Prerequisites

- 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 Microsoft ASP Server monitor makes use of performance counters to measure application server performance. SiteScopes running on Windows platforms need 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 Servers option in the remote server view. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Microsoft ASP Server Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Server where the Microsoft ASP Server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. If the server you want to monitor does not appear in the Serverslist because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters. Note when working in template mode: To update counters in template browsable monitors that need a target server, click the Select measurement from button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 46

Microsoft Exchange 2007/2010 Monitor

This monitor enables you to monitor statistics of Microsoft Exchange Server 2007 or 2010 on Windows platforms only.

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 Exchange 2007/2010 server. For details, see Microsoft Exchange Solution Templates in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Exchange Server 2007/2010 monitor.

Learn More

This section includes:

- "Microsoft Exchange Server 2007/2010 Monitor Overview" below
- "Setup Requirements" below

Microsoft Exchange Server 2007/2010 Monitor Overview

Use the Microsoft Exchange 2007/2010 monitor to display important statistics about the messaging system handled by a Microsoft Exchange Server 2007 with PowerShell v1.0 or Microsoft Exchange Server 2010 with PowerShell v2.0. 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 servers and objects.

By default, the Microsoft Exchange 2007/2010 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 Exchange Server 2007/2010. For details, see "How to Prepare the System for Using the Microsoft Exchange Server 2007/2010 Monitor" on page 367.

Create a separate Microsoft Exchange 2007/2010 monitor instance for each Microsoft Exchange server in your environment. The Microsoft Exchange 2007/2010 monitor is supported on Windows versions of SiteScope only.

Setup Requirements

- To configure Microsoft Exchange 2007/2010 monitor, Exchange Management Shell must be installed on SiteScope server. Windows PowerShell 1.0 or 2.0 must be installed on the computer that runs the Exchange Management Shell.
- 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 "How to Prepare the System for Using the Microsoft Exchange Server 2007/2010 Monitor" on page 367.
- For each cmdlet, the account you use must be delegated as follows (according to Microsoft Exchange Server 2007/2010, Permission Considerations section: <http://technet.microsoft.com/en-us/library/aa996881.aspx>):

cmdlet	Description
Test-MAPIConnectivity	<p>To run the Test-MapiConnectivity cmdlet, the account you use must be delegated the Exchange Server Administrators role and local Administrators group for the target server.</p> <p>To run the Test-MapiConnectivity cmdlet on a computer that has the Mailbox server role installed, you must log on by 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.</p>

cmdlet	Description
Test-ExchangeSearch	To run the Test-ExchangeSearch cmdlet, the account you use must be delegated the following: <ul style="list-style-type: none"> Exchange Recipient Administrator role Exchange Server Administrators role and local Administrators group for the target server
Test-MailFlow	To run the Test-Mailflow cmdlet, the account you use must be delegated the Exchange Server Administrators role and local Administrators group for the server where the cmdlet is run.
Test-OWAConnectivity	To run the Test-OwaConnectivity cmdlet to test Outlook Web Access connectivity for all Exchange 2007/2010 virtual directories on a Client Access server, the account you use must be delegated the Exchange Server Administrators role and membership in the local Administrators group for the target server.
Test-WebServicesConnectivity	To run the Test-WebServicesConnectivity cmdlet, the account you use must be delegated the Exchange Administrator role and local Administrators group for the target server.

- To run each cmdlet, the server roles that correspond to the cmdlets you want to run must be installed on the Microsoft Exchange Server. When monitoring Microsoft Exchange Server 2007 or 2010, 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-MAPIConnectivity Test-ExchangeSearch
Hub Transport, Mailbox	Test-MailFlow
Client Access	<ul style="list-style-type: none"> Test-OWAConnectivity Test-WebServicesConnectivity

Tasks

This section includes:

- "How to Prepare the System for Using the Microsoft Exchange Server 2007/2010 Monitor" below
- "How to Configure the Microsoft Exchange Server 2007/2010 Monitor" on the next page

How to Prepare the System for Using the Microsoft Exchange Server 2007/2010 Monitor

There are several important configuration requirements that must be performed or verified before the Microsoft Exchange 2007/2010 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.

Terminology	Description
Exchange Server Administrators	An account that has administrative privileges on the Exchange server.
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 2007/2010 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 and delegated the Exchange Server Administrators role (see definition above).

1. Create mailbox accounts on each Exchange Server to be monitored with the Microsoft Exchange 2007/2010 monitor

Exchange mailbox accounts are used by Microsoft Exchange 2007/2010 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 2007/2010 monitor.

2. Add each Exchange Mailbox Owner to the Administrators users group on the SiteScope server

The Mailbox Owner accounts setup in the previous step which are by definition domain logons, must be added as to the Administrators group on the SiteScope server.

- a. 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.

- b. Double-click the **Administrators** group icon to open the Administrators Properties window.
- c. Click the **Add** button to add each Mailbox Owner you expect to use with the Exchange 2007/2010 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 and delegated the Exchange Server Administrators role**

For more information about permissions, delegating roles, and the rights that are required for SiteScope user logon to monitor Microsoft Exchange Server 2007/2010, see "Setup Requirements" on page 365.

Caution: The SiteScope user account must be a Local Administrator or a member of the domain admins group and delegated the Exchange Server Administrators role.

To change the logon account for the SiteScope user:

- a. Open the **Services** control utility on the SiteScope server.
- a. Right-click the SiteScope service entry and click **Properties**. The SiteScope Properties settings page opens.
- b. Click the **Log On** tab.
- c. 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 enter the SiteScope user logon.
- d. Restart the SiteScope server after making changes to the SiteScope service logon account.

How to Configure the Microsoft Exchange Server 2007/2010 Monitor

1. **Prerequisites**

Prepare the system for using the Microsoft Exchange 2007/2010 monitor as described in "How to Prepare the System for Using the Microsoft Exchange Server 2007/2010 Monitor" on the previous page.

There are several other key requirements for using this monitor. For details on this topic, see "Setup Requirements" on page 365.

2. **Enter the PowerShell execute command when using the Microsoft Exchange 2007/2010 monitor on a 64-bit version of Windows 2003, 2008, or XP**

To enable use of the Microsoft Exchange 2007/2010 monitor on 64-bit version of Windows

2003, Windows 2008, or Windows XP (since a 32-bit application cannot access the system32 folder on a computer that is running a 64-bit version of Windows Server 2003, 2008, or of Windows XP), perform the following:

- a. Apply the Microsoft hotfix available from <http://support.microsoft.com/?scid=kb;en-us;942589>.
- b. In the **Power Shell execute command** box in **Preferences > Infrastructure Preferences > General Settings**, enter the PowerShell execute command. For example:
`C:\Windows\Sysnative\WindowsPowerShell\v1.0\powershell.exe`

Note: Symlink Sysnative is not available by default on Windows 2003 or Windows XP.

3. **Configure additional Microsoft Exchange Server counters - optional**

You must configure a test mailbox in the Microsoft Exchange Server to retrieve health information for the Outlook Web Access and Web Services cmdlets.

- a. To configure a test mailbox in the Microsoft Exchange Server, run the script **New-TestCasConnectivityUser.ps1** in the Exchange Server to create a test mailbox. The script can be found under **<Exchange installation directory>\Scripts**.
- b. 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.

- c. Repeat this process for each Exchange Mailbox Server that is to be tested.

4. **Configure the monitor properties**

Configure the monitor properties as described in the UI Descriptions section below.

5. **Schedule the monitor - optional**

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. We do not recommend setting monitor run frequency to less than 10 minutes.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Microsoft Exchange Server 2007/2010 Monitor Settings

User interface elements are described below:

UI Element	Description
Exchange server	Name of the server running Microsoft Exchange Server 2007/2010 that you want to monitor.
Exchange domain	Domain name and the mailbox of the server running Microsoft Exchange Server 2007/2010 that you want to monitor.
Mailbox	Name (alias) of the mailbox to be used for this monitor. This is often the email account name but it may be a different name. We recommend that you copy the mailbox name as it appears in the E-Mail Account properties for the email account you are using with this monitor.
Exchange PS console file path	Full path to the Microsoft Exchange Server Management Shell console file. Example: <ul style="list-style-type: none"> On Microsoft Exchange 2007: C:\Program Files\Microsoft\Exchange Server\Bin\ExShell.psc On Microsoft Exchange 2010: C:\Program Files\Microsoft\Exchange Server\V14\Bin\ExShell.psc
Timeout (seconds)	Amount of 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. Default value: 120 seconds
Counters	Displays the server performance counters selected for 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"> UnitType. 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	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

Monitor Reference

Chapter 46: Microsoft Exchange 2007/2010 Monitor

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 47

Microsoft Exchange 2003 Mailbox Monitor

The Microsoft Exchange 2003 Mailbox monitor enables you to monitor mailbox statistics of Microsoft Exchange Server 2003. 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:

- The Microsoft Exchange 2003 Mailbox monitor is an optional SiteScope monitor that requires additional licensing to enable the monitor 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 in the Using SiteScope Guide.

To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click **Microsoft Exchange 2003**, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

Learn More

Supported Versions

- This monitor is supported in SiteScopes that are running on Windows versions only.
- This monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.

Tasks

How to Configure the Microsoft Exchange 2003 Mailbox Monitor

1. Prerequisites

- The Microsoft Exchange 2003 Mailbox monitor requires additional licensing to enable the monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- 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`.

2. Deploy the Microsoft Exchange Solution template

This monitor can only be added by deploying the Microsoft Exchange 2003 solution template. For information about using templates to deploy monitors, see [SiteScope Templates in the Using SiteScope Guide](#).

3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors.

Configure the monitor properties as described in the [UI Descriptions](#) section below.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Microsoft Exchange 2003 Mailbox Monitor Settings

User interface elements are described below:

UI Element	Description
Server	Server running Microsoft Exchange Server 2003 that you want to monitor.
User name	User name to use when querying the server for mailbox statistics. The statistics are gathered by using WMI (Windows Management Instrumentation). The user name entered here must have permissions to read WMI statistics on the server from WMI namespace <code>root\MicrosoftExchangeV2</code> . Default value: If this box is left blank, the user that SiteScope is running is used.
Password	Password for the user name entered above, or blank if user name is blank.
N largest mailboxes	Number (N) of mailboxes to display when reporting the N largest mailboxes. Default value: 5
Days since access	Number of days (N) to use when reporting the number of mailboxes that have not been accessed in N days. Default value: 30
Reporting directory	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 (seconds)	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. Default value: 60 seconds

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

Troubleshooting and Limitations

Problem: You encounter one of the following errors when using the Microsoft Exchange 2003 Mailbox monitor (even though the monitor is in Good status):

- 1- Query failed: Cannot send request. Driver is not ready
- 2- Query failed: Request timed out
- 3- Query failed: Could not connect to the server

Solution 1: Enable WMI requests on the Microsoft Exchange 2003 server by setting the Remote Enable permission in the WMI Control for a namespace. If a user tries to connect to a namespace they are not allowed access to, they receive an error.

1. On the target server, select **Control Panel > Administrative Tools > Computer Management**.
2. Expand **Services and Applications**.
3. Right-click **WMI Control** and select **Properties**.
4. In the **Security** tab, select the namespace and click **Security**.
5. Locate the appropriate account and select **Remote Enable** in the **Permissions** list.

Solution 2: Enable WMI requests through Windows firewall.

If the target server is running Windows Firewall (also known as Internet Connection Firewall), enable it to let remote WMI requests through. On the target server, run the following command:

```
netsh firewall set service RemoteAdmin enable
```

For more details, see the Microsoft documentation (<http://msdn.microsoft.com/en-us/library/aa389286.aspx>).

Chapter 48

Microsoft Exchange 5.5 Message Traffic Monitor

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. 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:

- The Microsoft Exchange 5.5 Message Traffic monitor is an optional SiteScope monitor that requires additional licensing to enable the 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 in the Using SiteScope Guide.

To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click **Microsoft Exchange 5.5**, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

Tasks

How to Configure the Microsoft Exchange 5.5 Message Traffic Monitor

1. Prerequisites

The Microsoft Exchange 5.5 Message Traffic monitor requires additional licensing to enable the monitor type in the SiteScope interface. Contact your HP sales representative for more information.

2. Deploy the Microsoft Exchange Solution template

This monitor can only be added by deploying the Microsoft Exchange 5.5 solution template. For information about using templates to deploy monitors, see SiteScope Templates in the Using SiteScope Guide.

3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors.

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Microsoft Exchange 5.5 Message Traffic Monitor Settings

User interface elements are described below:

UI Element	Description
Recipient limit	Number (N) of recipients to use when computing the number of messages sent to more than N recipients. Default value: 10
Query interval	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. Default value: 1440 minutes (one day)
Message size limit	Number (N) of bytes to use when computing the number of messages sent larger than N bytes. Default value: 2000
Number of domains	Number (N) of domains to use for reporting the top N sending domains. Default value: 5
Number of outgoing users	Number (N) of users to use for reporting the top N outgoing users. Default value: 5
Log directory	UNC path to the directory where message tracking logs are stored for the Exchange 5.5 server. Default value: \\<server name>\tracking.log.
Reporting directory	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.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 49

Microsoft Exchange 2000/2003/2007 Message Traffic Monitor

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 in the Using SiteScope Guide.

To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click the Microsoft Exchange solution template version that you require, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

Learn More

Supported Versions

This monitor is supported in SiteScopes that are running on Windows versions only.

Tasks

How to Configure the Microsoft Exchange 2000/2003/2007 Message Traffic Monitor

1. Prerequisites

- The Microsoft Exchange 2000/2003/2007 Message Traffic monitor requires additional licensing to enable the monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- 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.

2. Deploy the Microsoft Exchange Solution template

This monitor can only be added by deploying the Microsoft Exchange solution template version that you require. For information about using templates to deploy monitors, see SiteScope Templates in the Using SiteScope Guide.

3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors. Since this monitor returns statistics that do not normally change very rapidly and are not critical to system availability, it should be scheduled to run infrequently, or on demand only.

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Settings

User interface elements are described below:

UI Element	Description
Recipient limit	Number (N) of recipients to use when computing the number of messages sent to more than N recipients. Default value: 10
Query interval	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. Default value: 1440 minutes (one day)
Message size limit	Number (N) of bytes to use when computing the number of messages sent larger than N bytes. Default value: 2000
Number of domains	Number (N) of domains to use for reporting the top N sending domains. Default value: 5
Number of outgoing users	Number (N) of users to use for reporting the top N outgoing users. Default value: 5
Log directory	UNC path of the messaging tracking log file directory. Default value: <ul style="list-style-type: none"> • For 2000/2003 versions: \\<server name>\<server name>.log • For 2007 version: \\<server name>\MessageTracking
Reporting directory	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.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 50

Microsoft Exchange 2003 Public Folder Monitor

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 in the Using SiteScope Guide.

To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click **Microsoft Exchange 2003**, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

Learn More

Supported Versions

- This monitor is supported in SiteScopes that are running on Windows versions only.
- This monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.

Tasks

How to Configure the Microsoft Exchange 2003 Public Folder Monitor

1. Prerequisites

- The Microsoft Exchange 2003 Public Folder monitor requires additional licensing to enable the monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- 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.

2. Deploy the Microsoft Exchange Solution template

This monitor can only be added by deploying the Microsoft Exchange 2003 solution template version that you require. For information about using templates to deploy monitors, see *SiteScope Templates* in the *Using SiteScope Guide*.

3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors. Since this monitor returns statistics that do not normally change very rapidly and are not critical to system availability, it should be scheduled to run infrequently, or on demand only.

Configure the monitor properties as described in the *UI Descriptions* section below.

Related workflow

How to Deploy a Monitor in the *Using SiteScope Guide*

UI Descriptions

Microsoft Exchange 2003 Public Folder Monitor Settings

User interface elements are described below:

UI Element	Description
Server	Name of the server running Microsoft Exchange Server 2003 that you want to monitor.
User name	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 <code>root\MicrosoftExchangeV2</code> . Default value: If this box is left blank, the user that SiteScope is running as is used.
Password	Password for the user name entered above, or blank if user name is blank.
Days since access	Number of days (N) to use when reporting the number of public folders that have not been accessed in N days. Default value: 7
Timeout (seconds)	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. Default value: 60
Reporting directory	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.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 51

Microsoft Hyper-V Monitor

This monitor enables you to monitor performance statistics of the Microsoft Hyper-V infrastructure for various server applications.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Hyper-V monitor.

Learn More

This section includes:

- ["Microsoft Hyper-V Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)

Microsoft Hyper-V Monitor Overview

Use the Microsoft Hyper-V monitor to monitor vital performance metrics in Hyper-V environments. Microsoft Hyper-V is a server virtualization that runs on Windows 2008 or higher. It is a hypervisor-based virtualization system for x64 Windows operating systems. The Microsoft Hyper-V monitor enables monitoring of Microsoft Hyper-V hosts and virtual machines.

You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate Microsoft Hyper-V monitor instance for each Hyper-V Server in your environment. The error and warning thresholds for the monitor can be set on one or more Microsoft Hyper-V Server performance statistics. The Microsoft Hyper-V monitor makes use of performance objects and counters to measure application server performance.

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see [SiteScope Monitoring Using Secure Shell \(SSH\)](#) in the [Using SiteScope Guide](#).
- This monitor supports monitoring remote servers running on:
 - Microsoft Hyper-V Server 2008 R2 (stand-alone product)
 - Microsoft Windows Server 2008 (Hyper-V role enabled)
 - Microsoft Windows Server 2008 R2 (Hyper-V role enabled)
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see [Configure the WMI Service for Remote Monitoring](#) in the [Using SiteScope Guide](#).

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

For details on using IPv6, see [Support for IP Version 6](#) in the [Using SiteScope Guide](#).

Tasks

[How to Configure the Microsoft Hyper-V Monitor](#)

Configure the monitor properties as described in the UI Descriptions section below.

[Related workflow](#)

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Microsoft Hyper-V Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of server that you want to monitor. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none">• Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.• When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none">• Browse servers. Select a server from the drop-down list of servers visible in the local domain.• Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Counters	<p>The server performance counters selected for this monitor. Use the Get Counters button to select counters.</p> <p>Note when working in template mode: To update counters in template browsable monitors that need a target server, click the Select measurement from button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 52

Microsoft IIS Server Monitor

Use the Microsoft IIS Server monitor to monitor server performance statistics from IIS servers on Windows systems. You can monitor multiple parameters or counters with a single monitor instance. This enables 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. The error and warning thresholds for the monitor can be set on one or more IIS server performance counters.

Tip: 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 Templates in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft IIS Server monitor.

Learn More

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["Microsoft IIS Server Topology" below](#)

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see [SiteScope Monitoring Using Secure Shell \(SSH\)](#) in the [Using SiteScope Guide](#).
- The Microsoft IIS Server monitor supports monitoring the following:
 - HTTP/HTTPS services on IIS 4.0, 5.0, 7.0, and 7.5, Windows Server 2008 R2, and Windows 7
 - HTTP/HTTPS, FTP, NNTP and MSMQ Queue on IIS 6 and 7.0.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see [Configure the WMI Service for Remote Monitoring](#) in the [Using SiteScope Guide](#).

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

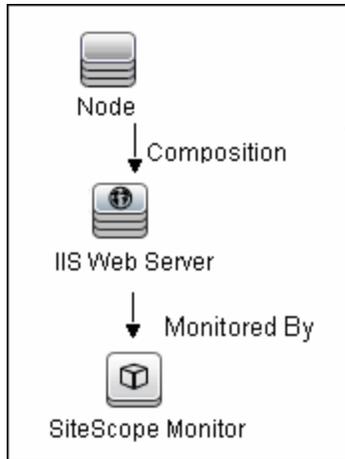
For details on using IPv6, see [Support for IP Version 6](#) in the [Using SiteScope Guide](#).

Microsoft IIS Server Topology

The Microsoft IIS Server monitor can identify the topology of the Microsoft IIS Server being monitored. The monitor creates the following topology in BSM's RTSM.

Monitor Reference

Chapter 52: Microsoft IIS Server Monitor



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

Tasks

How to Configure the Microsoft IIS Server Monitor

1. Prerequisites

- The Microsoft IIS Server monitor makes use of performance counters to measure application server performance. If the servers you want to monitor require a unique login different than the account SiteScope is running under, you must define the connection to these servers in the Microsoft Windows Remote Servers container. Alternatively, you can enter the credentials of a user with administrative permissions on the server in the **Default authentication user name** and **Default authentication password** boxes in **Preferences > General Preferences**, and create the monitor without creating a Microsoft Windows Remote Server.
- The Remote Registry service must be running on the machine where the IIS server is running if IIS is running on Windows 2000.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "[Microsoft IIS Server Topology](#)" on page 395.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Microsoft IIS Server Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server where the Microsoft IIS performance statistics you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> Remote servers that have been configured with the WMI method are also displayed here. For details, see <i>Configure the WMI Service for Remote Monitoring</i> in the <i>Using SiteScope Guide</i>. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see <i>How to Configure SiteScope to Monitor a Remote Microsoft Windows Server</i> in the <i>Using SiteScope Guide</i>.</p>
Add Remote Server	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see <i>New/Edit Microsoft Windows Remote Server Dialog Box</i> in the <i>Using SiteScope Guide</i>.</p>

UI Element	Description
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters. Note when working in template mode: To update counters in template browsable monitors that need a target server, click the Select measurement from button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General General Notes/Limitations

- When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the **Browse Servers** and **Add Remote Server** buttons are not displayed.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Troubleshooting and Limitations

- Check if the Microsoft IIS server is available and the services that should be monitored are up and running.
- If SiteScope is unable to get counters, run a test on the target remote server. If counters do not contain the required service (for example, FTP or Web Server), check if the corresponding service is running on the target machine.

Chapter 53

Microsoft Lync Server 2010 Monitors

Enables you to monitor the performance of the various Microsoft Lync Server 2010 monitors (Microsoft A/V Conferencing Server, Microsoft Archiving Server, Microsoft Director Server, Microsoft Edge Server, Microsoft Front End Server, Microsoft Mediation Server, Microsoft Monitoring and CDR Server, and Microsoft Registrar Server) as described in "[Microsoft Lync Server 2010 Monitor Overview](#)" on the next page.

You can monitor multiple parameters or counters on a single, remote server with each monitor instance. Create one or more Microsoft Lync Server 2010 monitor instances for each remote server in your environment. The error and warning thresholds for the monitor can be set on one or more performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the required Microsoft Lync Server 2010 monitor.

Learn More

This section includes:

- ["Microsoft Lync Server 2010 Monitor Overview" below](#)
- ["Supported Versions" on the next page](#)
- ["Support for IPv6 Addresses" on page 404](#)
- ["Server-Centric Report" on page 404](#)
- ["Configuring the Monitor to Run on Windows 2008 R2 as a Non-Administrator User" on page 404](#)

Microsoft Lync Server 2010 Monitor Overview

Use the Microsoft Lync Server 2010 monitors to watch server loading for performance, availability, and capacity planning on the following:

- **Microsoft A/V Conferencing Server.** Monitors the server performance statistics of the Microsoft Lync A/V Conferencing Server. A/V conferencing, enables real-time audio and video A/V communications between your users (that is, provided they have appropriate client devices such as headsets for audio conferences, and web cams for video conferences). A/V Conferencing Server provides A/V conferencing functionality to your deployment. It can be collocated with Front End Server, or deployed separately as a single server or A/V Conferencing Server pool.
- **Microsoft Archiving Server.** Monitors the server performance statistics of the Microsoft Lync Archiving Server. The Archiving Server enables you to archive instant messaging (IM) communications and meeting content for compliance reasons. Corporations and other organizations are subject to an increasing number of industry and government regulations that require the retention of specific types of communications. With the Archiving Server feature, Microsoft Lync Server 2010 communications software provides a way for you to archive IM content, conferencing (meeting) content, or both that is sent through Lync Server 2010. If you deploy Archiving Server and associate it with Front End pools, you can set it to archive instant messages and conferences and specify the users for which archiving is enabled.
- **Microsoft Director Server.** Monitors the server performance statistics of the Microsoft Lync Director Server. A Director is a server running Microsoft Lync Server communications software that authenticates user requests, but does not home any user accounts or provide presence or conferencing services. Directors are most useful in deployments that enable external user access, where the Director can authenticate requests before sending them on to internal servers. Directors can also improve performance in organizations with multiple Front End pools.
- **Microsoft Edge Server.** Monitors the server performance statistics of the Microsoft Lync Edge Server. The Edge Server enables your users to communicate and collaborate with users outside the organization's firewalls. These external users can include the organization's own users who are currently working offsite, users from federated partner organizations, and outside users who have been invited to join conferences hosted on your Lync Server deployment. Edge Server also enables connectivity to public IM connectivity services, including Windows Live, AOL, and Yahoo!.
- **Microsoft Front End Server.** Monitors the server performance statistics of the Microsoft Lync Front End Server. The Front End Server is the core server role, and runs many basic Lync Server functions. The Front End Server, along with the Back End Servers, which provide the

database, are the only server roles required to be in any Lync Server Enterprise Edition deployment.

A Front End pool is a set of Front End Servers, configured identically, that work together to provide services for a common group of users. A pool provides scalability and failover capability your users.

Front End Server includes the following functionality:

- User authentication and registration
 - Presence information and contact card exchange
 - Address book services and distribution list expansion
 - IM functionality, including multiparty IM conferences
 - Web conferencing and application sharing (if deployed)
 - Application hosting services, for both applications included with Lync Server (for example, Conferencing Attendant and Response Group application) and third-party applications
 - Application services for application hosting and hosts applications (for example, Response Group application, and several others)
- **Microsoft Mediation Server.** Monitors the server performance statistics of the Microsoft Lync Mediation Server. The Mediation Server is a necessary component for implementing Enterprise Voice and dial-in conferencing. The Mediation Server translates signaling and, in some configurations, media between your internal Lync Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk. On the Lync Server side, Mediation Server listens on a single mutual TLS (MTLS) transport address. On the gateway side, Mediation Server listens on a single TCP and single TLS transport address or a single TLS transport address. All qualified gateways must support TLS, but can enable TCP as well.
 - **Microsoft Monitoring and CDR Server.** Monitors the server performance statistics of the Microsoft Lync Monitoring and CDR Server. The Monitoring Server collects data about the quality of your network media, in both Enterprise Voice calls and A/V conferences. This information can help you provide the best possible media experience for your users. It also collects call error records (CERs), which you can use to troubleshoot failed calls. Additionally, it collects usage information in the form of call detail records (CDRs) about various Lync Server features, so that you can calculate return on investment of your deployment, and plan the future growth of your deployment.
 - **Microsoft Registrar Server.** Monitors the server performance statistics of the Microsoft Lync Registrar Server. The Lync Server 2010 Registrar is a new server role that enables client registration and authentication and provides routing services. It resides along with other components on a Standard Edition Server, Enterprise Front End Server, Director, or Survivable Branch Appliance. A Registrar pool consists of Registrar Services running on the Lync Server pool and residing at the same site.

Supported Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.

- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see *Configure the WMI Service for Remote Monitoring* in the *Using SiteScope Guide*.

Support for IPv6 Addresses

These monitors support the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the following protocols are supported:

- WMI (from SiteScope installed on Windows platforms only)
- NetBIOS (from SiteScope installed on Windows platforms only)

Note:

- When using the **Direct registry queries** collection method with a NetBIOS connection, counters are not displayed in the Available Counters table. However, you can still use monitoring process if you modify the counters using the IPv4 protocol, or copy the counters from an already configured monitor (copy the monitor), and then change back to the IPv6 address or host.
- When using the **Microsoft Windows PDH Library** collection method with a NetBIOS connection, IPv6 does not work if the name of the monitored server is specified as a literal IPv6 address.
- When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:
 1. Replacing any colon (":") characters with a dash ("-") character.
 2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`
would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see *Support for IP Version 6* in the *Using SiteScope Guide*.

Server-Centric Report

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 Lync Server 2010 monitor in the SiteScope Dashboard. For details, see *Server-Centric Report* in the *Using SiteScope Guide*.

Configuring the Monitor to Run on Windows 2008 R2 as a Non-Administrator User

For the Microsoft Lync Server 2010 monitors to monitor a Windows 2008 R2 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. For details on how to perform this task, see ["How to Configure the Microsoft Lync Server 2010 Monitor"](#) on the next page.

Tasks

How to Configure the Microsoft Lync Server 2010 Monitor

1. Prerequisites

SiteScopes running on Windows platforms need 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 Servers option in the remote server view.

For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

2. Configure user account settings on SiteScope

The user account settings on SiteScope must be configured to log on using the selected non-administrator user account.

- a. In the **Services** control panel, right-click the SiteScope service, and then click **Properties**. The SiteScope Properties dialog box opens.
- b. Click the **Log On** tab, and configure the user account to log on using the selected non-administrator user account (domain or local account).

3. Configure user account settings on the remote monitored machine

The user account settings on the monitored remote server must be configured to log on using the selected non-administrator user account.

- a. Check that you can access the remote machine. Perform a ping test and check DNS resolves the server name with its IP address.

We recommend that you check that 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.

- b. 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`.

- c. 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]
```

Note: 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.

- d. Make sure that the domain or local user account to be used has at least read permissions on the following objects:
 - o Registry key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg]
 - o 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.

4. Verify that the non-administrator user account works

After configuring the user account settings, verify that they work.

- a. Launch a standard Windows perfmon utility. You can either:
 - o Launch it interactively when logged on to the SiteScope machine with the selected user account by typing `perfmon`, or
 - o Launch it when logged on to the SiteScope machine with some other account through the `RunAs` command, which enables you to launch commands under different user account. Enter the following command:

```
runas /env /netonly /user:tester "mmc.exe perfmon.msc"
```

Then enter the password (in this example, for the `tester` account), and the command is run under the `tester` user account.

- b. After the Performance window opens, right-click in the right graph area and select **Add Counters**. The Add Counters dialog box opens.
- c. Select **Choose counters from computer** and enter the remote monitored machine name or its IP address in the box.

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.

5. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Microsoft Lync Server 2010 Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server where the Microsoft Lync Server 2010 performance statistics you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Server to get measurements from	<p>(Available in template mode only) Name of any SiteScope remote server from which you want to get counters (it must be accessible in the domain using NETBIOS). Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. If the server you want to monitor does not appear in the Serverslist because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>

UI Element	Description
Add Remote Server	Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see <i>New/Edit Microsoft Windows Remote Server Dialog Box</i> in the <i>Using SiteScope Guide</i> .
Collection method	<p>Select the collection method option. The Available Counters list is dynamically updated according to the collection method selected. This enables you to see the counters when creating or editing the monitor instead of when running the monitor:</p> <ul style="list-style-type: none"> • Microsoft Windows PDH Library. This is the default and most common option. • Use global setting. Instructs the monitor to use the value configured in Default collection method for Microsoft Windows Resources monitor in Preferences > Infrastructure Preferences > General Settings. The default value for this setting is PDH. • 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. <p>Note: The collection method option is available only when the target remote server uses the NetBIOS protocol (not SSH or WMI).</p>
Enable Server-Centric Report	Enables collecting data specifically for generating the Server-Centric Report. The report displays various measurements for the server being monitored. For details, see <i>Server-Centric Report</i> in the <i>Using SiteScope Guide</i> .
Available Counters	Displays the available measurements for this monitor. For each measurement, select the Object , Instances and Counters you want to check with the monitor, and click the Add Selected Counters  button. The selected measurements are moved to the Selected Counters list.
Selected Counters	Displays the measurements currently selected for this monitor, and the total number of selected counters. To remove measurements selected for monitoring, select the required measurements, and click the Remove Selected Counters  button. The measurements are moved to the Available Counters list.

For information on configuring setting panels that are common to all monitors, see *Common Monitor Settings* in the *Using SiteScope Guide*.

Tips/Troubleshooting

General Notes/Tips

- When configuring these monitors in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Microsoft Lync Server 2010 monitors.

- Getting invalid CPU value error message in **<SiteScope root directory>\logs\RunMonitor.log** file when using perfmon monitors on VMware host servers.
Workaround: Use the VMWare Performance monitor to measure CPU on VMWare host servers.
- If you encounter "Error: Object Processor not found on host" or "Error: Failed to collect the data" when running the Microsoft Lync Server 2010 monitors, change the collection method to the **Direct registry queries method** option.

Chapter 54

Microsoft SQL Server Monitor

Use the Microsoft SQL Server monitor to monitor the server performance metrics pages for SQL Servers on Windows systems. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Microsoft SQL Server you are running. The error and warning thresholds for the monitor can be set on one or more SQL Server performance statistics.

Tip: 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 Server 2005, 2008, and 2008 R2. For details, see Microsoft SQL Server Solution Templates in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft SQL Server monitor.

Learn More

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["Microsoft SQL Server Topology" below](#)

Supported Platforms/Versions

- The Microsoft IIS Server monitor supports monitoring SQL Servers 6.5, 7.1, 2000, 2005, 2008, and 2008 R2 on Windows systems.
- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see [SiteScope Monitoring Using Secure Shell \(SSH\)](#) in the [Using SiteScope Guide](#).
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see [Configure the WMI Service for Remote Monitoring](#) in the [Using SiteScope Guide](#).

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

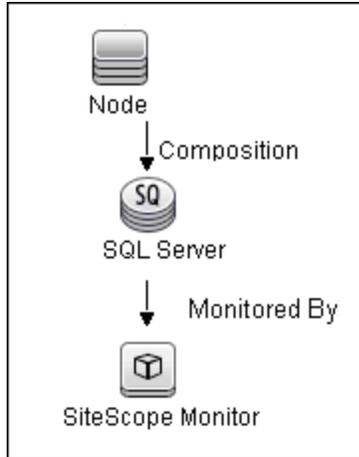
For details on using IPv6, see [Support for IP Version 6](#) in the [Using SiteScope Guide](#).

Microsoft SQL Server Topology

The Microsoft SQL Server monitor can identify the topology of the Microsoft SQL Servers being monitored. The monitor creates the following topology in BSM's RTSM.

Monitor Reference

Chapter 54: Microsoft SQL Server Monitor



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

Tasks

How to Configure the Microsoft SQL Server Monitor

1. Prerequisites

The following are requirements for using the Microsoft SQL Server monitor:

- JDBC drivers for connecting to the DB2 Database server. These can be found in your DB2 server installation directories. Copy the **db2jcc.jar** file to the **<SiteScope root directory>\WEB-INF\lib** folder.
- This monitor uses the Snapshot mirroring functionality supported by DB2. You must enable the Snapshot Mirror on your DB2 instance to retrieve counters. For details, refer to the relevant IBM DB2 documentation.
- The Microsoft SQL Server monitor uses performance counters to measure application server performance. SiteScopes running on Windows platforms need 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 Servers option in the remote server view. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.
- 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.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "[Microsoft SQL Server Topology](#)" on page 412.

For user interface details, see [BSM Integration Data and Topology Settings](#) in the Using SiteScope Guide.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Microsoft SQL Server Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server where the Microsoft SQL Server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>
SQL instance name	<p>The Microsoft SQL server instance you want to monitor from the list of SQL instances running on the selected server.</p> <p>Default value: SQLServer (this value is displayed even if SiteScope is unable to get the instance list).</p>

UI Element	Description
Counters	<p>Displays 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.</p> <p>Note when working in template mode: To update counters in template browsable monitors that need a target server, click the Select measurement from button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Tips

- When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the **Browse Servers** and **Add Remote Server** buttons are not displayed.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Troubleshooting and Limitations

Problem: SiteScope is unable to retrieve instances and counters from a Microsoft SQL Server 2008 when using the WMI connection method.

Solution:

1. Configure the monitor to use the NetBIOS connection.
2. If this does not work, you can monitor Microsoft SQL Server 2008 using the Microsoft Windows Resources monitor.

Chapter 55

Microsoft Windows Dial-up Monitor

The Microsoft Windows Dial-up monitor uses the Windows 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Dial-up monitor.

Learn More

This section includes:

- ["Microsoft Windows Dial-up Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Status" below](#)
- ["Scheduling the Monitor" below](#)

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.

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 dial-up 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 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.

Supported Platforms/Versions

This monitor is supported in SiteScopes that are running on Windows versions only.

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 be used), and the percentage of the monitors run that were OK.

Scheduling the 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.

Tasks

[How to Configure the Microsoft Windows Dial-up Monitor](#)

Configure the monitor properties as described in the UI Descriptions section below.

[Related workflow](#)

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Microsoft Windows Dial-up Monitor Settings

User interface elements are described below:

UI Element	Description
Account Settings	
Phone number	Phone number for the dial-up account, adding any extra modem digits or pauses that are required. Example: 9, 4432266 includes a "9, " for getting an outside line. Insert a comma wherever you need a short pause.
Account user name	Login name for the dial-up account.
Account password	Password for the dial-up account.
Advanced Settings	
Timeout (seconds)	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. Default value: 60 seconds
Monitor Settings	
Monitor (s) to run	Groups, monitors, or both, that you want to run while the dial-up connection is established. 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. Make sure that the Frequency box for these monitors is set to 0. For details, see Monitor Run Settings in the Using SiteScope Guide.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Tips

This monitor cannot be copied to a template. It must be created directly in a template.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Microsoft Windows Dial-up monitor.

- 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 can be 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.

Chapter 56

Microsoft Windows Event Log Monitor

The Microsoft Windows Event Log monitor enables you to monitor the Microsoft Windows Event Logs (System, Application, or Security) for added entries.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Event Log monitor.

Learn More

This section includes:

- ["Microsoft Windows Event Log Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Configuring SiteScope Alerts" below](#)
- ["Status" below](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)

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 log entries made only 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 Monitor Settings to specify values that must appear in the event entry for the entry to match.

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see [SiteScope Monitoring Using Secure Shell \(SSH\)](#) in the [Using SiteScope Guide](#).
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see [Configure the WMI Service for Remote Monitoring](#) in the [Using SiteScope Guide](#).

Configuring SiteScope Alerts

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 root directory>\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.

IPv6 Addressing Supported Protocols

This monitor supports the NetBIOS protocol when **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**).

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Microsoft Windows Event Log Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Event Log Tool** is available when configuring this monitor to display portions of the Windows Event Log (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Event Log Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Microsoft Windows Event Log Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server where the event log you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. When configuring this monitor on SiteScopes running on UNIX versions: <ul style="list-style-type: none"> Only remote servers that have been configured with an SSH connection method and SSH using preinstalled SiteScope remote Windows SSH files is selected are displayed. For details, see How to Configure Remote Windows Servers for SSH monitoring. If you create a new remote server from the Monitor Settings panel, the SSH using preinstalled SiteScope remote Windows SSH files setting is automatically selected and cannot be cleared. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>

UI Element	Description
Add Remote Server	Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.
Log name	<p>Select the event log to monitor. The list of event logs is automatically generated from the target server (from the registry for NetBIOS/SSH connections, and from WMI Classes for WMI connections).</p> <p>Note: When using a NetBIOS or WMI connection, only the IDs (names) are displayed for independent libraries. For example, if you install Microsoft Office Diagnostics, only <code>ODiag</code> is displayed as the log name. To display the whole name, manually add the log name to the <code>event_log_names.properties</code> file in <code><SiteScope root directory>\template.applications</code>.</p> <p>For example:</p> <ul style="list-style-type: none"> • <code>ODiag=Microsoft Office Diagnostics</code> • <code>OSession=Microsoft Office Sessions</code> • <code>HardwareEvents=Hardware Events</code> <p>Note: You should only add names to <code>event_log_names.properties</code> that are different from the IDs, otherwise all names will be the same as IDs.</p>
Event type	<p>The event types to match. Select from the following event types:</p> <ul style="list-style-type: none"> • Any • Audit Failure • Audit Success • Warning • Error or warning • Information
Run alerts	<p>Method for running alerts:</p> <ul style="list-style-type: none"> • For each event matched. The monitor triggers alerts for every matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error). For useful information, see "Configuring SiteScope Alerts" on page 424. • Once, after all events have been checked. The monitor counts up the number of matches and triggers alerts based on the warning and error threshold settings.

UI Element	Description
<p>Source and ID match</p>	<p>The match string identifying the source of the event and the event ID in the form: <Event Source>:<Event ID>.</p> <p>Example: <code>Print:20</code> matches event source named <code>Print</code> and event ID of <code>20</code>.</p> <p>To match against all events from a specific source, enter just the event source name.</p> <p>Example: <code>w3svc</code></p> <p>To match an exact event ID from an event source, specify both.</p> <p>Example: <code>Service Control Mar:7000</code></p> <p>Note: You can click the Open Tool button to use the Regular Expression Test tool to check your regular expressions. For details, see Regular Expression Tool in the Using SiteScope Guide.</p>
<p>Source and ID do not match</p>	<p>The string identifying the source of the event and the event ID to NOT MATCH in the form: <Event Source>:<Event ID>.</p> <p>Example: <code>Print:20</code> means an event source named <code>Print</code> and event ID of <code>20</code> must not be in the event to have a match.</p> <p>To not match all events from a particular source, specify just the source name.</p> <p>Example: <code>w3svc</code></p> <p>To not match an exact event ID from an event source, specify both.</p> <p>Example: <code>Service Control Mar:7000</code></p> <p>You can also use a regular expression for a more complex NOT MATCH.</p> <p>Example:</p> <ul style="list-style-type: none"> • to not match all Perflib sources from 200 to 299 use: <code>/Perflib:2\d\d/</code> • to not match all events from the Perflib source, use: <code>Perflib:*</code> <p>Note: You can click the Open Tool button to use the Regular Expression Test tool to check your regular expressions. For details, see Regular Expression Tool in the Using SiteScope Guide.</p>

UI Element	Description
Description match	<p>Text string to match against the description text for the event entry. Thresholds that are defined as <code>value/value 2/value3/value4</code> refer to the matches found in the event description.</p> <p>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.</p> <p>Note: You can click the Open Tool button to use the Regular Expression Test tool to check your regular expressions. For details, see Regular Expression Tool in the Using SiteScope Guide.</p>
Description does not match	<p>Text string description that must not be in the event to have a match.</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>Note: You can click the Open Tool button to use the Regular Expression Test tool to check your regular expressions. For details, see Regular Expression Tool in the Using SiteScope Guide.</p>
Event category	<p>Matches the category number of the event entry. Leaving this blank matches events with any category.</p>
Event machine	<p>Matches against the machine that added the entry to the log file. Leaving this blank matches events with any machine.</p>
Interval (minutes)	<p>Time period 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> <p>Note: This field is not available when For each event matched is selected in the Run alert field.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section describes troubleshooting and limitations for the Microsoft Windows Event Log monitor.

- "General Notes/Tips" below
- "Monitor fails to get data from Windows remote servers with large amounts of log items when using a WMI connection" below
- "Unable to monitor custom event logs on a remote Microsoft Windows Server 2008" below

General Notes/Tips

When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the **Browse Servers** and **Add Remote Server** buttons are not displayed.

Monitor fails to get data from Windows remote servers with large amounts of log items when using a WMI connection

If the Microsoft Event Log monitor fails to get data from Windows remote servers with large amounts of log items when using the WMI connection type, change the query hour range of the first monitor run in the `_ntEventLogWMIQueryHourRangeFirstRun` property in **Preferences > Infrastructure Preferences > Custom Settings** or in the `<SiteScope root directory>\groups\master.config` file. The default query range is the last 168 hours (7 days).

Unable to monitor custom event logs on a remote Microsoft Windows Server 2008

To make a custom log file accessible:

1. Add the file to the registry.

For example, to monitor a custom event log called `TaskScheduler` (`C:\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler\Operational.evtx`), you must add a registry key **Microsoft-Windows-TaskScheduler/Operational** under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog**.

2. After adding the registry key, you can see the log in the list of available log files:

```
PS C:\Users\Administrator> get-eventlog -list
```

Max(K)	Retain	OverflowAction	Entries	Log
20,480	0	OverwriteAsNeeded	162	Application
20,480	0	OverwriteAsNeeded	0	HardwareEvents
512	7	OverwriteOlder	0	Internet Explorer
20,480	0	OverwriteAsNeeded	0	Key Management Service
512	7	OverwriteOlder	162	Microsoft-Windows-TaskScheduler/Operational
20,480	0	OverwriteAsNeeded	304	Security
20,480	0	OverwriteAsNeeded	769	System
15,360	0	OverwriteAsNeeded	9	Windows PowerShell

3. The log is automatically displayed in the Microsoft Windows Event Log Monitor Settings:

Monitor Reference

Chapter 56: Microsoft Windows Event Log Monitor

The screenshot shows a configuration window for monitoring Microsoft Windows Event Logs. The interface includes the following fields and options:

- Server:** A dropdown menu showing the IP address `172.24.151.110`. To its right are two buttons: `Browse Servers` and `Add Remote Server`.
- Log name:** A dropdown menu with the selected value `Microsoft-Windows-Task Scheduler/Operational`.
- Event type:** A list of event types including `Application`, `Hardware Events`, `Internet Explorer`, `Key Management Service`, `Microsoft-Windows-Task Scheduler/Operational` (highlighted), `Security`, `System`, and `Windows PowerShell`.
- Run alerts:** A text input field.
- Source and ID match:** A text input field.
- Source and ID do not match:** A text input field.
- Description match:** A text input field.
- Description does not match:** A text input field.

An `Open Tool` button is located at the bottom right of the configuration area.

4. Configure the events to match in the log, and use SiteScope to monitor this log for events.

Example

Matching an exact event ID (200) in the TaskScheduler log file:

The screenshot shows the 'Microsoft Windows Event Log Monitor Settings' window. The configuration is as follows:

- Server: 172.24.151.110 (with 'Browse Servers' and 'Add Remote Server' buttons)
- Log name: Microsoft-Windows-Task Scheduler/Operational (highlighted with a red box)
- Event type: Any
- Run alerts: For each event matched
- Source and ID match: Microsoft-Windows-Task Scheduler:200 (highlighted with a red box)
- Source and ID do not match: (empty text box)
- Description match: (empty text box)
- Description does not match: (empty text box)
- Event category: (empty text box)
- Event machine: (empty text box)
- Interval (minutes): 0

Each of the 'do not match' fields has an 'Open Tool' button to its right.

Chapter 57

Microsoft Windows Media Player Monitor

The Microsoft Windows Media Player monitor enables you 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 enables 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. The error and warning thresholds for the monitor can be set on one or more Windows Media Player performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Media Player monitor.

Learn More

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows versions only.
- This monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.
- This monitor supports monitoring Windows Media Player 7.x, 9.x, 10.x, 11.0, and 12.
- You should monitor only video streams, not audio streams, with this monitor.
- This monitor does not support the .asx or .mov formats.

Tasks

How to Configure the Microsoft Windows Media Player Monitor

1. Prerequisites

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 the next page.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Microsoft Windows Media Player Tool** is available when configuring this monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see [Microsoft Windows Media Player Tool](#) in the [Using SiteScope Guide](#).

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Microsoft Windows Media Player Monitor Settings

User interface elements are described below:

UI Element	Description
URL	<p>URL of the media file or streaming source you want to monitor. This should be the URL of the media file.</p> <p>Example: <code>mms://<servername>/sample.asf</code> for a unicast stream or <code>http://<servername>/stationid.nsc</code> 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>
Duration (milliseconds)	<p>Playback duration that the monitor should use for the media file or streaming source. The duration value does not need to match the duration of the media contained in the file.</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> <p>Default value: 15000 milliseconds</p>
Counters	<p>Media player performance parameters or counters to check with the Microsoft Windows Media Player monitor.</p> <p>For details on the available parameters or counters, see "Performance Counters" below.</p>
Performance Counters	
<p>The media player performance parameters or counters you can check with the Microsoft Windows Media Player monitor include:</p>	
Buffering count	Number of times the Player had to buffer incoming media data due to insufficient media content.
Buffering time	Time spent waiting for sufficient media data to continue playing the media clip.
Interrupts	Number of interruptions encountered while playing a media clip. This includes buffering and playback errors.
Packets lost	Number of lost packets not recovered (applicable to network playback).
Packets recovered	Number of lost packets successfully recovered (applicable to network playback).

UI Element	Description
Packet quality	Percentage ratio of packets received to total packets.
Ratio bandwidth	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%.
Recommended bandwidth	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	Total duration of the media clip in seconds. This value is not effected by what was already played.
Sampling rate	Sampling rate in milliseconds, for collecting statistics.
Stream count	Packet count.
Stream max	Maximum number of packets.
Stream min	Minimum number of packets.
Stream rate	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	Percentage of stream samples received on time (no delays in reception).

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 58

Microsoft Windows Media Server Monitor

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 enables you to watch server loading for performance, availability, and capacity planning.

Create a separate monitor instance for each Windows Media Server you are running. The error and warning thresholds for the monitor can be set on one or more Windows Media server performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Media Server monitor.

Learn More

This section includes:

- "Supported Platforms/Versions" below
- "IPv6 Addressing Supported Protocols" below

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports all versions of Microsoft Windows Media Server through perfmon.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Microsoft Windows Media Server Monitor

1. Prerequisites

The Microsoft Windows Media Server monitor uses performance counters to measure application server performance. SiteScopes running on Windows platforms need 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 Servers option in the remote server view.

For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Note: By default, SiteScope monitors the Microsoft Windows Media Server default services, **Windows Media Station Service** and **Windows Media Unicast Service**. To monitor other services, add the service names (separated by commas) to the **Microsoft Windows Media Server monitor service names** box in **Preferences > Infrastructure Preferences > Monitor Settings**.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Microsoft Windows Media Server Monitor Settings

User interface elements are described below:

UI Element	Description
<p>Server</p>	<p>Name of the server where the Windows Media Server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
<p>Browse Servers</p>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<p>Add Remote Server</p>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Counters	Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters. Note when working in template mode: To update counters in template browsable monitors that need a target server, click the Select measurement from button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Tips

- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

Chapter 59

Microsoft Windows Performance Counter Monitor

The Microsoft Windows Performance Counter monitor enables you to track the values of any Windows performance statistic. These are the same statistics that can be viewed using the Microsoft Management Console under Windows.

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 details table for the monitor which represents the current value returned by this monitor. The status is logged as either good, warning, or error. An error occurs if the counter could not be read, or if measurements are within the error threshold range.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Performance Counter monitor.

Learn More

Supported Platforms/Versions

- This monitor supports monitoring remote servers running on Windows XP Pro, Windows NT Server 4.0, and Windows Server 2000/2003/2008.
- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.

Tasks

How to Configure the Microsoft Windows Performance Counter Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Performance Counters Tool** is available when configuring this monitor to check performance counters on a specific machine in a Windows network (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Performance Counters Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Microsoft Windows Performance Counter Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server on which you want to monitor Windows performance statistics. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</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> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> • Browse servers. Select a server from the drop-down list of servers visible in the local domain. • Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
<p>PerfMon chart file</p>	<p>The Microsoft Windows Performance Counter monitor setting file you want to use for your settings. These files can be saved in the Microsoft Management Console (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. 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 in the Counter box below.</p> <p>If you create your own .pmc file, any server specified in the .pmc file is ignored by SiteScope. The queried server is the one in the Server box (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 Management Console instance, but any single instance of the Microsoft Management Console only queries one server regardless of the servers assigned in the .pmc.</p> <p>If you have specified the settings directly in the Object box below, this list displays (Custom object).</p>
<p>Object</p>	<p>Name of the high level item that is being measured, such as Processor or Server. It is the same as the Object in the Microsoft Management Console. The object name is case sensitive. If you are using a Performance monitor file for counter settings, leave this item blank.</p>
<p>Counter</p>	<p>The specific aspect of the Object that is measured, such as Interrupts/sec. It is the same as the Counter in the Microsoft Windows Performance monitor application. The counter name is case sensitive. If you are using a Microsoft Windows Performance monitor file for counter settings, leave this item blank.</p>
<p>Units</p>	<p>The units to be displayed with the counter's values to make them more readable.</p>
<p>Instance</p>	<p>The instance in the Microsoft Windows Performance monitor application. The instance name is case sensitive. Some counters can have multiple instances, for example, on machines with two CPUs, there are two instances of the Processor object. If you are using a Microsoft Windows Performance monitor file for counter settings, leave this item blank. If you leave this blank and there are multiple instances, the first instance in the list is selected.</p>

UI Element	Description
Scale	<p>If you want the raw performance counter value scaled to make it more readable, select one of the predefined choices using the Commonly used values list, or enter a numeric value in the Other values box.</p> <p>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 Microsoft Windows Performance monitor file, this scaling applies to all counters.</p> <p>Default value: 1</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the **Browse Servers** and **Add Remote Server** buttons are not displayed.

Chapter 60

Microsoft Windows Resources Monitor

The Microsoft Windows Resources monitor enables you to monitor system performance data on Windows systems. This enables 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. The error and warning thresholds for the monitor can be set on one or more performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Resources monitor.

Learn More

This section includes:

- "Supported Platforms/Versions" below
- "Support for IPv6 Addresses" below
- "Server-Centric Report" on the next page
- "Configuring the Monitor to Run on Windows 2003 as a Non-Administrator User" on the next page

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on Windows XP Pro, Windows NT Server 4.0, Windows Server 2000, 2003 and 2008, 2008 R2, Windows Vista, and Windows 7
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the following protocols are supported:

- WMI (from SiteScope installed on Windows platforms only)
- NetBIOS (from SiteScope installed on Windows platforms only)

Note:

- When using the **Direct registry queries** collection method with a NetBIOS connection, counters are not displayed in the Available Counters table. However, you can still use monitoring process if you modify the counters using the IPv4 protocol, or copy the counters from an already configured monitor (copy the monitor), and then change back to the IPv6 address or host.
- When using the **Microsoft Windows PDH Library** collection method with a NetBIOS connection, IPv6 does not work if the name of the monitored server is specified as a literal IPv6 address.
- When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:
 1. Replacing any colon (":") characters with a dash ("-") character.

2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`
would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Server-Centric Report

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 the SiteScope Dashboard. For details, see Server-Centric Report in the Using SiteScope Guide.

Configuring the 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. For details on how to perform this task, see ["How to Configure the Microsoft Windows Resources Monitor" on the next page](#).

Tasks

How to Configure the Microsoft Windows Resources Monitor

1. Prerequisites

SiteScopes running on Windows platforms need 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 Servers option in the remote server view.

For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

2. Configure user account settings on SiteScope

The user account settings on SiteScope must be configured to log on using the selected non-administrator user account.

- a. In the **Services** control panel, right-click the **SiteScope** service, and then click **Properties**. The SiteScope Properties dialog box opens.
- b. Click the **Log On** tab, and configure the user account to log on using the selected non-administrator user account (domain or local account).

3. Configure user account settings on the remote monitored machine

The user account settings on the monitored remote server must be configured to log on using the selected non-administrator user account.

- a. Check that you can access the remote machine. Perform a ping test and check DNS resolves the server name with its IP address.

We recommend 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.

- b. 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`.

- c. 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]
```

Note: 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, select the user that SiteScope uses to access the remote machine, and make sure that the **Allow** check box for **Read** is selected in the **Permissions** pane.

- d. Make sure that the domain or local user account to be used has at least read permissions on the following objects:
 - o Registry key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg]
 - o 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.

4. Verify that the non-administrator user account works

After configuring the user account settings, verify that they work.

- a. Launch a standard Windows perfmon utility. You can either:
 - o launch it interactively when logged on to the SiteScope machine with the selected user account by typing `perfmon`, or
 - o launch it when logged on to the SiteScope machine with some other account through the `RunAs` command, which enables you to launch commands under different user account. Enter the following command:

```
runas /env /netonly /user:tester "mmc.exe perfmon.msc"
```

Then enter the password (in this example, for the `tester` account), and the command is run under the `tester` user account.

- b. After the Performance window opens, right-click in the right graph area and select **Add Counters**. The Add Counters dialog box opens.
- c. Select **Choose counters from computer** and enter the remote monitored machine name or its IP address in the box.

Press the TAB key. If the perfmon utility can connect to the remote machine, the Performance object box is filled in with the performance objects that can be monitored from the remote machine.

5. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Microsoft Windows Resources Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server that you want to monitor. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> • Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. • When configuring this monitor on SiteScopes running on UNIX versions, only remote servers that have been configured with an SSH connection method are displayed. For details, see How to Configure Remote Windows Servers for SSH monitoring. • When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Server to get measurements from	<p>(Available in template mode only) Name of any SiteScope remote server from which you want to get counters (it must be accessible in the domain using NETBIOS). Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.</p>

UI Element	Description
<p>Browse Servers</p>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> • Browse servers. Select a server from the drop-down list of servers visible in the local domain. • Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<p>Add Remote Server</p>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>
<p>Collection method</p>	<p>Select the collection method option. The Available Counters list is dynamically updated according to the collection method selected. This enables you to see the counters when creating or editing the monitor instead of when running the monitor:</p> <ul style="list-style-type: none"> • Microsoft Windows PDH Library Uses the Windows PDH library which is the most common option. • Use global setting. Instructs the monitor to use the value configured in Default collection method for Microsoft Windows Resources monitor in Preferences > Infrastructure Preferences > General Settings. The default value for this setting is PDH. This is the default option. • 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. <p>Note: The collection method option is available only when the target remote server uses the NetBIOS protocol (not SSH or WMI).</p>
<p>Enable Server-Centric Report</p>	<p>Enables collecting data specifically for generating the Server-Centric Report. The report displays various measurements for the server being monitored. For details, see Server-Centric Report in the Using SiteScope Guide.</p>
<p>Available Counters</p>	<p>Displays the available measurements for this monitor.</p> <p>For each measurement, select the Objects, Instances and Counters you want to check with the Microsoft Windows Resources monitor, and click the Add Selected Counters  button. The selected measurements are moved to the Selected Counters list.</p>

UI Element	Description
Selected Counters	Displays the measurements currently selected for this monitor, and the total number of selected counters. To remove measurements selected for monitoring, select the required measurements, and click the Remove Selected Counters  button. The measurements are moved to the Available Counters list.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Tips

- 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.
- When monitoring Windows servers configured using SSH, you must use the **Direct registry queries** option for the **Collection method**.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When configuring this monitor in template mode:
 - You can use regular expressions to define counters.
 - The **Add Remote Server** button is not displayed.

Troubleshooting and Limitations

- Getting invalid CPU value error message in **<SiteScope root directory>\logs\RunMonitor.log** file when using perfmon monitors on VMware host servers.
Workaround: Use the VMWare Performance monitor to measure CPU on VMWare host servers.
- If you encounter "Error: Object Processor not found on host" or "Error: Failed to collect the data" when running the Microsoft Windows Resources monitor, change the collection method to the **Direct registry queries method** option.
- If you encounter inconsistent data when configuring Microsoft Windows Resources monitors with many counters on a loaded network environment, you can specify a timeout value for the monitor (for example, 300 seconds) in **Preferences > Infrastructure Preferences > Monitor Settings > Perfex options**.

Chapter 61

Microsoft Windows Services State Monitor

The Microsoft Windows Services State monitor enables you 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.

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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Services State monitor.

Learn More

This section includes:

- "Supported Platforms/Versions" below
- "IPv6 Addressing Supported Protocols" below

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on Windows XP Pro, Windows NT Server 4.0, Windows Server 2000, 2003 and 2008, 2008 R2.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

[How to Configure the Microsoft Windows Services State Monitor](#)

Configure the monitor properties as described in the UI Descriptions section below.

[Related workflow](#)

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Microsoft Windows Services State Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>The name of the server you want to monitor. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. When configuring this monitor on SiteScopes running on UNIX versions: <ul style="list-style-type: none"> Only remote servers that have been configured with an SSH connection method and SSH using preinstalled SiteScope remote Windows SSH files is selected are displayed. For details, see How to Configure Remote Windows Servers for SSH monitoring. If you create a new remote server from the Monitor Settings panel, the SSH using preinstalled SiteScope remote Windows SSH files setting is automatically selected and cannot be cleared. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>

UI Element	Description
Add Remote Server	Opens the Add New Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.
Services to include	Optional regular expression to filter the list of services returned by the monitor. 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. Default value: <code>/(.*)/</code> (All of the services detected on the remote machine) Examples: <code>/. *Network. */</code> includes all services that contain the word Network.
Services to ignore	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. Examples: <code>/. *Remote. */</code> ignores all services that contain the word Remote (the services that are ignored are listed in the Services Deleted field).
Include driver services	Includes all low-level driver services in the monitor. 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.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- 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).
- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- 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.

Chapter 62

Network Bandwidth Monitor

This monitor enables you 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Network Bandwidth monitor.

Learn More

This section includes:

- "Network Bandwidth Monitor Overview" below
- "Performing Sanity Checks" below
- "IPv6 Addressing Supported Protocols" below

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.

The MIB files in **<SiteScope root directory>\templates.mib** are used to create a browsable tree that contains names and descriptions of the objects found during a traversal. Note that an object may or may not be displayed with a textual name and description, depending on the MIBs available in **<SiteScope root directory>\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 sanitycheck** box in the Infrastructure Settings Preferences page (**Preferences > Infrastructure Settings Preferences > Monitor Settings**).

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

[How to Configure the Network Bandwidth Monitor](#)

Configure the monitor properties as described in the UI Descriptions section below.

[Related workflow](#)

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Network Bandwidth Monitor Settings

User interface elements are described below:

UI Element	Description
Basic SNMP Settings	
Server	Name of the server you want to monitor.
Port	Port to use when requesting data from the SNMP agent. Default value: 161
SNMP Connection Settings	
Timeout (seconds)	Amount of time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. Default value: 5 seconds
Number of retries	Number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. Default value: 1
Community	Community string (valid only for version 1 or 2 connections). Default value: public
SNMP version	Version of SNMP to use when connecting. SiteScope supports SNMP versions 1, 2, and 3. Selecting V3 enables you to enter V3 settings in the SNMP V3 settings fields below. Default value: V1
Authentication algorithm	Authentication algorithm to use for version 3 connections. Default value: MD5 Note: This field is available only if SNMP V3 is selected.
User name	User name for version 3 connections. Note: This field is available only if SNMP V3 is selected.
Password	Authentication password to use for version 3 connections. Note: This field is available only if SNMP V3 is selected.

UI Element	Description
Privacy algorithm	<p>The privacy algorithm used for authentication for SNMP version 3 (DES, 128-Bit AES, 192-Bit AES, 256-Bit AES).</p> <p>Default value: DES</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
Privacy password	<p>Privacy password for version 3 connections. Leave blank if you do not want privacy.</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
Context engine ID	<p>Hexadecimal string representing the Context Engine ID to use for this connection.</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
Context name	<p>Context Name to use for this connection.</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
Network Counters	
Counters	<p>Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p>Note:</p> <ul style="list-style-type: none"> The counters displayed are those received during the timeout period, and may not include all the counters available on the server. Specifying a longer timeout in the Timeout (seconds) field in the SNMP Connection Settings panel may result in receiving more counters. The total time for receiving the counters may be longer than the timeout specified, due to additional processing time not part of the request/response period.
Advanced Network Settings	
Device type	<p>Optional device type for device specific monitoring. 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.</p> <p>Default value: Do not monitor device-specific metrics</p>

UI Element	Description
Duplex or half-duplex	<p>Duplex state (Half-duplex or Full-duplex) to use when calculating percent bandwidth utilized for all selected interfaces on this device.</p> <p>Default value: Full-duplex</p>
Interface index	<p>Metrics for network interfaces on an SNMP-enabled device are presented as a table of management information (the ifTable). Each row corresponds to a different interface. There is no requirement that the mappings 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 (for example, Cisco) 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> <p>Default value: Indexed by ifTable row number.</p>
Show bytes in/out	<p>Displays a graph for bytes in/out along with the percent bandwidth utilized on the Real-Time Metrics page.</p> <p>Default value: Not selected</p>
Real-Time data vertical axis	<p>Maximum value on the vertical axis for real-time graphs (leave blank to have this automatically calculated by SiteScope).</p>
Real-Time data time window (hours)	<p>Number of hours for which real-time graph data should be stored.</p> <p>Default value: 24 hours</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- When working in template mode, the monitor's non-default thresholds are not copied properly to a template.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 63

News Monitor

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. This enables you to manage the number of articles that can queue up, and delete them before they cause disk space problems.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the News monitor.

Learn More

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, enter a user name and password under the Monitor 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 **good**.

Tasks

How to Configure the News Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **News Server Tool** is available when configuring this monitor to access a news server and view the NNTP interaction between SiteScope and the news server (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see News Server Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

News Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
News server	IP address or the name of the news server that you want to monitor. Example: 206.168.191.21 or news.thiscompany.com. If the port is not the standard news port, add the port after the server with a colon. Example: news.thiscompany.com:7777
News groups	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.
User name	User name if your News server requires authorization.
Password	Password if your News server requires authorization.
Advanced Settings	
Connect from	Name or IP address of the server that connects to the News monitor.
Timeout (seconds)	Amount of time, in 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. Default value: 60 seconds

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 64

Oracle 10g Application Server Monitor

Use the Oracle 10g Application Server monitor to monitor the server performance data for Oracle 10g and 10g R3 application servers. You can monitor multiple parameters or counters with a single monitor instance. This enables 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. The error and warning thresholds for the monitor can be set on one or more Oracle 10g server performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Oracle 10g Application Server monitor.

Tasks

How to Configure the Oracle 10g Application Server Monitor

1. Prerequisites

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**.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Oracle 10g Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
Authorization user name	User name to access the server if required.
Authorization password	Password to access the server if required.
Proxy server	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the server.
Proxy server user name	Proxy server user name if the proxy server requires a name and password to access the server. Your proxy server must support Proxy-Authenticate for these options to function.
Proxy server password	Proxy server password if the proxy server requires a name and password to access the server. Your proxy server must support Proxy-Authenticate for these options to function.
Host name	Server administration URL for the server you want to monitor.
Metric type	The type of metrics to monitor. Options are App Server (OC4J) and Web Server (DMS).
Port	Server port for the server you want to monitor. Default value: 7201 (configured in the <code>dms.conf</code> file)
Secure server	Select to use a secure server.
Timeout (seconds)	Amount of time, in 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. Default value: 60 seconds
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

Monitor Reference

Chapter 64: Oracle 10g Application Server Monitor

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 65

Oracle 9i Application Server Monitor

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 enables 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. The error and warning thresholds for the monitor can be set on one or more Oracle 9i server performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Oracle 9i Application Server monitor.

Tasks

How to Configure the Oracle 9i Application Server Monitor

1. Prerequisites

You must enable Web caching on the Oracle 9i Application Server to use the Oracle 9i Application Server monitor.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **URL Tool** is available when configuring this monitor to request a URL from a server, print the returned data, and test network routing (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see **URL Tool** in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Oracle 9i Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
URL	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	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor.
Authorization user name	User name if the server you want to monitor requires a name and password for access.
Authorization password	password if the server you want to monitor requires a name and password for access.
HTTP Proxy	Domain name and port of an HTTP Proxy Server. if a proxy server is used to access the server.
Proxy user name	Proxy server user name if the proxy server requires a name and password to access the server. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Proxy password	Proxy server password if the proxy server requires a name and password to access the server. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Timeout (seconds)	Amount of time, in 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.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 66

Oracle Database Monitor

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 enables 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. The error and warning thresholds for the monitor can be set on one or more Oracle server performance statistics.

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 Templates in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Oracle Database monitor.

Learn More

This section includes:

- "Supported Platforms/Versions" below
- "IPv6 Addressing Supported Protocols" below
- "Oracle Database Topology" below

Supported Platforms/Versions

The monitor supports monitoring server performance statistics from Oracle Database 8i, 9i, 10g, 11i, and 11g R2 (11.2.0.1) servers.

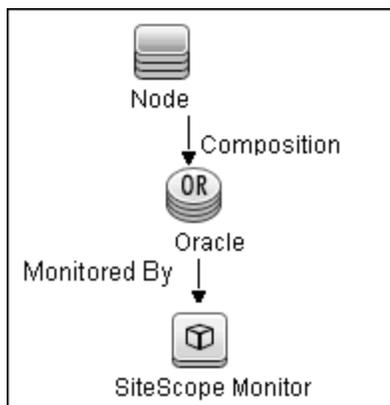
IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the TCP (JDBC) protocol. Support for IPv6 might also depend on the JDBC driver being used.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Oracle Database Topology

The Oracle Database monitor can identify the topology of the Oracle databases being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

To ensure that the topology is reported accurately, you should enter the values for the **Database machine name** and the **SID**. These fields appear in the **BSM Integration Data and Topology Settings** section of **HP Integration Settings**.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

Tasks

This section includes:

- "How to Configure the Oracle Database Monitor" below
- "How to Access Oracle Databases Using OCI Driver" on the next page

How to Configure the Oracle Database Monitor

1. Prerequisites

The following are 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:@<server name or IP address>:<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: The colon (:) and the at (@) symbols must be included as shown.

- You must know the syntax for accessing the Oracle **Database driver** that was installed on the SiteScope server. Examples of common database driver strings are:
 - **oracle.jdbc.driver.OracleDriver.** SiteScope supports the following categories of JDBC driver that are supplied by Oracle: JDBC thin driver for Oracle 7 and 8 databases, and JDBC OCI (thick) driver. For details on accessing Oracle databases using OCI driver, see ["How to Access Oracle Databases Using OCI Driver" on the next page](#).
 - **com.mercury.jdbc.oracle.OracleDriver.** A driver for Oracle databases. This driver is deployed with SiteScope. When using the Oracle mercury driver, the database connection URL has the form of: `jdbc:mercury:oracle://<server name or IP address>:<database server port>;sid=<sid>`
- You should have only one version of each driver installed on the SiteScope machine. If there is more that version is installed, SiteScope may report an error and be unable to connect to the database.

- The user specified in the **Credentials** section must be granted the permission to execute SELECT queries to the following tables:
 - V\$INSTANCE
 - V\$STATNAME
 - V\$SYSSTAT
 - V\$SESSION
 - V\$SESSTAT
 - V\$PROCESS
 - DBA_DATA_FILES
 - DBA_FREE_SPACE
 - DBA_DATA_FILES
 - DBA_DATA_FILES

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "Oracle Database Topology" on page 488.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

How to Access Oracle Databases Using OCI Driver

You can monitor an Oracle database using an OCI driver. If the port or SID are changed, you only need to make the change in the **tnsnames.ora** file (the SiteScope Oracle monitors remain unchanged).

1. On the SiteScope server, install the version of Oracle client that you are using.
2. Connect to the Oracle database using the Oracle OCI driver.
 - Set **ORACLE_HOME** environment variable (**ORACLE_HOME** is the folder where the Oracle client or database has been installed).
 - Add **ORACLE_HOME\lib** to System PATH (on Windows platforms), or **LD_LIBRARY_PATH** env variable (on UNIX platforms).
 - Set **CLASSPATH** environment variable to use Oracle JDBC driver from **ORACLE_HOME\jdbc\lib**.
3. In the `\oracle\oraX\network\admin\tnsnames.ora` file, configure the service name. You can test this using a SQL+ tool or the SiteScope Database Connection tool (see Database Connection Tool in the Using SiteScope Guide).
4. Add a database monitor within SiteScope, and configure the following settings in the Monitor Settings panel:

Monitor Reference

Chapter 66: Oracle Database Monitor

- **Database connection URL:** `jdbc:oracle:oci8:@<service name>`
- **Database driver:** `oracle.jdbc.driver.OracleDriver`
- Enter the database user credentials in the **Database user name** and **Database password** boxes

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Database Connection Settings

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.

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 and 9, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.

User interface elements are described below:

UI Element	Description
Physically close if idle connection count exceeds	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. Default value: 10
Query timeout	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. Default value: 1 minute
Idle connection timeout	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. Default value: 5 minutes
Use connection pool	Enables SQL connection sharing. This means that you use a connection pool rather than open and close a new connection for each monitor query. Default value: Selected

Oracle Database Monitor Settings

User interface elements are described below:

UI Element	Description
Database connection URL	<p>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=<sid></code>.</p> <p>Example: To connect to the ORCL database on a machine using port 1521, use:</p> <pre>jdbc:oracle:thin:@206.168.191.19:1521:ORCL.</pre> <p>Note: The colon (:) symbol must be included as shown.</p>
Database driver	<p>Driver used to connect to the database.</p> <p>Example: <code>oracle.jdbc.driver.OracleDriver</code></p>
Credentials	<p>Option for providing the user name and password to be used to access the database server:</p> <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Counters	<p>Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- If you are using a third-party database driver and you upgrade SiteScope, you must deploy the driver to SiteScope again, since the driver configuration data is not saved during an upgrade.
- For information about troubleshooting the Oracle Database monitor, refer to the [HP Software Self-solve Knowledge Base](http://support.openview.hp.com/selfsolve/document/KM189298) (<http://support.openview.hp.com/selfsolve/document/KM189298>). To enter the knowledge base, you must log on with your HP Passport ID.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 67

Ping Monitor

The Ping monitor enables you to check the availability of a host by using ICMP (Internet Control Message Protocol). Use this monitor to check network connectivity and response time.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Ping monitor.

Learn More

This section includes:

- "Ping Monitor Overview" below
- "What to Monitor" below
- "IPv6 Addressing Supported Protocols" below

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

We recommend 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.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the ICMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Ping Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Ping Tool** is available when configuring this monitor to check if the host can be reached, and the round-trip time along the path (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Ping Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Ping Monitor Settings

User interface elements are described below:

UI Element	Description
Host name to resolve	<p>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> <p>Note: You can monitor only one IP or host name at a time for each monitor instance.</p>
Packet size (bytes)	<p>The size, in bytes (including the IP and ICMP headers), of the ping packets sent. To change the threshold, enter the new value in the text box.</p> <p>Default value: 32 bytes</p>
Time to wait for replies before ping timeouts	<p>Amount of time, in milliseconds, that should pass before the ping times out. To change the threshold, enter the new value in the text box.</p> <p>Default value: 5000 milliseconds</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Tips

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.

Troubleshooting and Limitations

If you are unable to ping a remote machine, there are several possible causes:

- If you are trying to ping a host name, make sure the name you are pinging is fully qualified.
- If pinging the fully qualified host name does not work, try pinging the IP address of the destination machine. If ping fails when you try the name of the site, but works when you try the IP address, it is a problem with DNS.
- If pinging both the name and the IP address fail, it might be because they are administratively denied by an access control list. Sometimes routers block ping with an access list. Try a traceroute instead, or if it is a Web site, try browsing it.
- If the traceroute shows multiple hops between you and the destination, try pinging each host in the path. Start pinging the host closest to you, and work your way towards the destination until you find the host that fails to respond to ping. Use a traceroute to get a list of the hosts between you and the destination for this purpose.

Chapter 68

Port Monitor

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 after the connection is made. You can 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Port monitor.

Learn More

This section includes:

- "Status" below
- "IPv6 Addressing Supported Protocols" below

Status

Each time the Port 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 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.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the TCP and UDP protocols.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Port Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Ping Tool** is available when configuring this monitor to check if the host can be reached, and the round-trip time along the path (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Ping Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Port Monitor Settings

User interface elements are described below:

UI Element	Description
Host name	IP address or the name of the host that you want to monitor. Example: 206.168.191.21 or demo.thiscompany.com
Port number	Port number to connect to from the list of Commonly used ports , or enter a port number in the Other ports text box. Additional entries can be added to the list by editing the <SiteScope root directory>\groups\master.config file.
Timeout (seconds)	Amount of time, in seconds, to 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. Default value: 60 seconds
Send string	Customizes the string sent to the host after a connection is made.
Match string	Checks for a string of text after a connection is made. If the text is not received, the monitor displays the message <code>no match on content</code> . Note: <ul style="list-style-type: none">• The search is case sensitive.• You cannot use regular expressions in this field.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

Tips

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.

Chapter 69

Radius Monitor

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. A RADIUS server is used to authenticate users, often connecting through a remote connection such as a dialup modem or a DSL line. If the RADIUS server fails, any users that try to use it are unable to log on and access any services.

Create a separate monitor instance for each server you are running. You may want to set up multiple monitors per server if you want to test different kinds of login accounts.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Radius monitor.

Learn More

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**.

Tasks

How to Configure the Radius Monitor

1. Prerequisites

- 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 can communicate with. This must be done 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.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Radius Monitor Settings

User interface elements are described below:

UI Element	Description
Radius server	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	Secret used to encrypt all requests to this RADIUS server.
User name	User name to authenticate.
Password	Password to authenticate.
Called Station Id	Telephone number on which the call was received. For virtual private network (VPN) connections, the IP address of the VPN server.
Calling Station Id	Telephone number from which the call was made. For virtual private network (VPN) connections, the IP address of the VPN client.
Port	UDP port used by the RADIUS server. Default value: 1812
Timeout (seconds)	Amount of time, in seconds, to 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. Default value: 30 seconds
Match content	Text string 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 can also perform a regular expression match by enclosing the string in forward slashes, with an i after the trailing slash indicating case-insensitive matching. Example: / \d\d/ or /size \d\d/i Note: The search is case sensitive.
Open Tool	Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.

For information on configuring setting panels that are common to all monitors, see Common

Monitor Settings in the Using SiteScope Guide.

Chapter 70

Real Media Player Monitor

Use the Real Media Player monitor to monitor availability and delivery quality parameters for media files and streaming data compatible with RealNetworks Real Media Player.

You can monitor multiple parameters or counters with a single monitor instance. This enables 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. The error and warning thresholds for the monitor can be set on one or more Real Media Player performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Real Media Player monitor.

Learn More

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows versions only.
- This monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.
- This monitor supports monitoring RealNetworks Real Media Player versions 7.x, 8.x, 9.x, and 10.x
- This monitor does not support metadata files such as the .smi format.

Tasks

How to Configure the Real Media Player Monitor

1. Prerequisites

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.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Real Media Player Tool** is available when configuring this monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Real Media Player Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Real Media Player Monitor Settings

User interface elements are described below:

UI Element	Description
URL	<p>URL of the media file or streaming source you want to monitor. This should be the URL of the media file.</p> <p>Note:</p> <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.
Counters	<p>Select the server performance counters you want to check with this monitor. The list displays the available counters and those currently selected for this monitor.</p>
Duration (milliseconds)	<p>Playback duration that the monitor should use for the media file or source. The duration value does not need to match the duration of the media contained in the file.</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> <p>Default value: 15,000 milliseconds</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 71

Real Media Server Monitor

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 enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each RealSystem Server you are running.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Real Media Server monitor.

Learn More

This section includes:

- "Supported Platforms/Versions" below
- "IPv6 Addressing Supported Protocols" below

Supported Platforms/Versions

This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Real Media Server Monitor

1. Prerequisites

- 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.
- The Real Media Server monitor makes use of Performance Counters to measure application server performance. SiteScopes running on Windows platforms need 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 Servers option in the remote server view. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Note: By default, SiteScope monitors the Real Media Server default service, **RMServer**. To monitor other services, add the service names (separated by commas) to the **Real Media Server monitor service names** box in **Preferences > Infrastructure Preferences > Monitor Settings**.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Real Media Server Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server you want to monitor. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note:</p> <ul style="list-style-type: none"> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. When working in template mode, you can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box. <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> Browse servers. Select a server from the drop-down list of servers visible in the local domain. Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Counters	<p>Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p> <p>Note when working in template mode: To update counters in template browsable monitors that need a target server, click the Select measurement from button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the Server field.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 72

SAP CCMS Monitor

The SAP CCMS monitor enables you to monitor the performance of your SAP R/3 System landscape in a centralized manner using SAP's centralized monitoring architecture, CCMS (Computer Center Management System).

Note:

- The SAP CCMS monitor is an optional SiteScope monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. 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 in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP CCMS monitor.

Learn More

This section includes:

- ["SAP CCMS Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["SAP CCMS Topology" below](#)

SAP CCMS Monitor Overview

Use the SAP CCMS monitor to retrieve and report metrics using SAP's centralized monitoring architecture, CCMS. With CCMS, a SAP administrator can monitor all servers, components and resources in the SAP landscape from a single centralized server, greatly facilitating not only problem discovery but also problem diagnosis.

Using the SAP CCMS monitor, you can also enable reporting of the host topology to BSM. If enabled, BSM automatically populates the RTSM with CIs based on the monitored hardware in SiteScope.

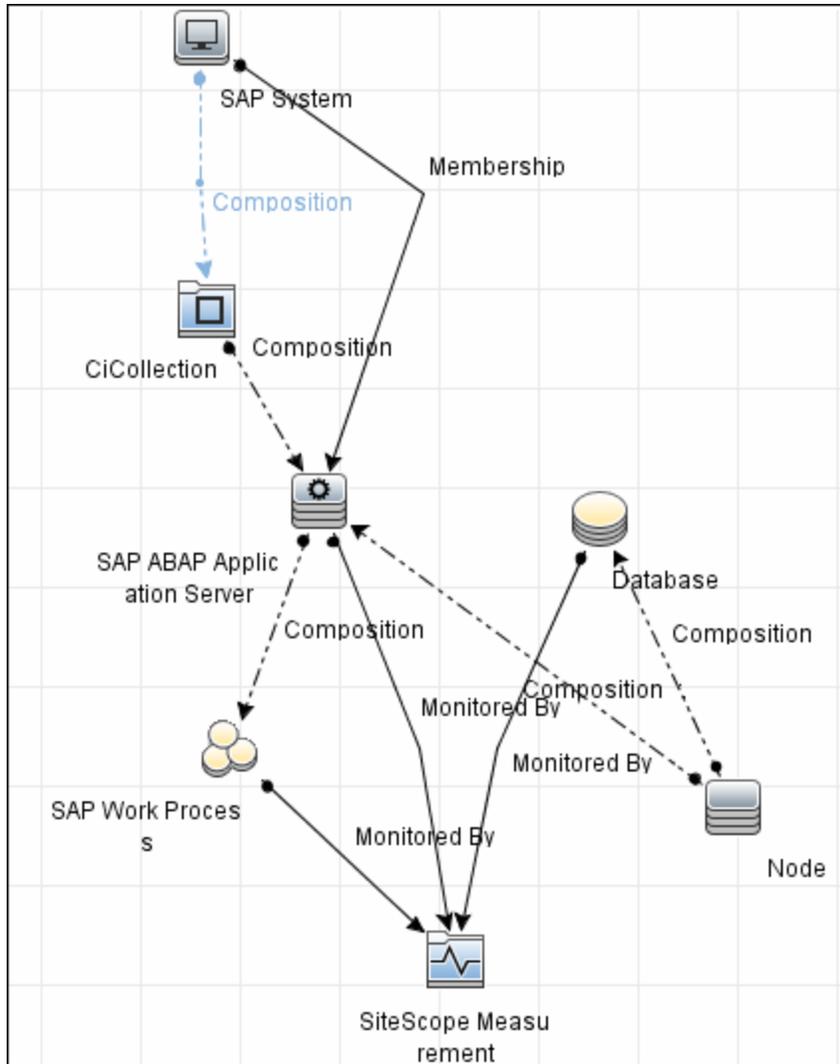
Using SAP's advanced CCMS interface BC-XAL 1.0, the SiteScope SAP CCMS monitor exposes hundreds of performance and availability metrics. The error and warning thresholds for the monitor can be set for one or more of the nearly 120 SAP server performance statistics available by using the CCMS interface.

Supported Platforms/Versions

This monitor supports monitoring all servers, components and resources in the R/3 4.6B, R/3 4.6C, R/3 4.7E, SAP ECC5 and SAP ECC6 landscape.

SAP CCMS Topology

The SAP CCMS monitor can identify the topology of the SAP System being monitored. The monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM as SiteScope Measurement Groups and SiteScope Measurement CIs.

Note:

- This direct integration between SiteScope and BSM is available only when the Application Management for SAP license is installed.
- When you add a new application server to the SAP System, you must clear the **Report monitor and related CI topology** 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 details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

For information about the SAP topology, see SAP Systems View in the BSM User Guide in the BSM Help.

Tasks

How to Configure the SAP CCMS Monitor

1. Prerequisites

- The SAP CCMS monitor requires additional licensing to enable the monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- Before configuring the monitor, make sure you have the necessary setup requirements and user privileges to log on to the CCMS server and retrieve metrics.
 - Consult your SAP documentation to determine if your R/3 landscape components requires additional software installed to run or work with CCMS.

Note: The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and later only.

- You must have SAP authorization of the remote system user. For details on the minimum SAP permission required by SiteScope, see the sections on “AAAB - Cross-application Authorization Objects” and “BC_A - Basis: Administration” in [SAP RFC User privileges](http://help.sap.com/saphelp_nw73/helpdata/de/49/bb35b8623a489aa63abd9f5ebf2448/content.htm) in the SAP documentation (http://help.sap.com/saphelp_nw73/helpdata/de/49/bb35b8623a489aa63abd9f5ebf2448/content.htm).
- 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 log on 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 user interface and see if the CCMS monitor sets can be displayed.

- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries.

2. Download the SAP Java Connector

The SAP Java Connector (SAP JCo version 2.0.6 or later) component must be downloaded and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

- a. To download SAP Java Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>).

Note: You need a valid Service Marketplace login to access the SAP Web site

- b. After you log on, select **SAP NetWeaver > SAP NetWeaver in Detail > Application Platform > Connectivity > Connectors > SAP Java Connector**, and then click **Tools and Services**.

3. Enable the SAP CCMS monitor

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.

- a. Download the following .jar file and .dll files from the SAP support Web site (<http://www.service.sap.com/connectors>):

On a Windows environment:

File	Copy to...
sapjco.jar	<SiteScope root directory>\WEB-INF\lib
librfc32.dll sapjcorfc.dll	<p><SiteScope root directory>\bin</p> <p>Note: 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), you must overwrite them with these .dll files before copying them into the SiteScope directory.</p>

On a UNIX environment:

File	Copy to...
sapjco.jar	<p><SiteScope root directory>/WEB-INF/lib</p> <p>Note: JCO native libraries must be copied to /usr/lib for 32-bit platforms and to /usr/lib64 for 64-bit platforms. To check that a JCO connector is installed correctly, run the following command:</p> <pre>/opt/HP/SiteScope/java/bin/java -jar /opt/HP/SiteScope/WEB-INF/lib/sapjco.jar</pre>
librfccm.so libsapjcorfc.so	<ul style="list-style-type: none"> o For Sun installations: <SiteScope root directory>/java/lib/sparc o For Linux installations: /usr/lib for 32-bit platforms and /usr/lib64 for 64-bit platforms.

- b. Restart SiteScope.

4. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

5. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "SAP CCMS Topology" on page 521.

Monitor Reference

Chapter 72: SAP CCMS Monitor

For user interface details, see BSM Integration Data and Topology Settings in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

SAP CCMS Monitor Settings

User interface elements are described below:

UI Element	Description
Application server	Address of the SAP server you want to monitor.
SAP client	Client to use for connecting to SAP.
System number	System number for the SAP server.
SAP router string	<p>Router address string if your connection is being made through a router (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>
Credentials	<p>Option for providing the user name and password to access the SAP server:</p> <ul style="list-style-type: none">• Use user name and password. Select this option to manually enter user credentials. Enter the user name and password to access the SAP server in the User name and Password box.• Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
CCMS monitor sets match	Enter a regular expression to match the SAP CCMS monitor sets you want to view (top level nodes of the CCMS tree). Only counters of matched tree sets are requested from SAP and displayed in the counter tree. To change the match, you must reload the counters. If the field is empty, all monitor sets are shown.
Collect all types of counters	<p>Select to enable the monitor to collect all other types of counters in addition to collecting SAP performance counters.</p> <p>Note: If this option is selected, it is recommended to use CCMS monitor sets match to prevent performance capacity problems.</p>
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.

UI Element	Description
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. This tree displays the hierarchy of Monitoring Tree Elements displayed in the Monitoring Tree that is shown in the SAP user interface with transaction RZ20. The information in the SiteScope browse tree may differ slightly from that in RZ20 depending on the authorization level of the user name you specified for this monitor.</p> <p>Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Tips

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Troubleshooting and Limitations

- The SAP CCMS 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.
- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries
- 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.

Chapter 73

SAP CCMS Alerts Monitor

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.

Note: The SAP CCMS Alerts monitor is an optional SiteScope monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. Contact your HP sales representative for more information.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP CCMS monitor.

Learn More

Supported Platforms/Versions

This monitor enables supports monitoring alerts for various components of your SAP R/3 4.6B, R/3 4.6C, R/3 4.7E, and SAP ECC5 and ECC6 landscape.

Tasks

How to Configure the SAP Alerts CCMS Monitor

1. Prerequisites

- The SAP Alerts CCMS monitor requires additional licensing to enable the monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- Before configuring the monitor, make sure you have the necessary setup requirements and user privileges to log on to the CCMS server and retrieve metrics.
 - The SAP Java Connector (SAP JCo 2.0.6 and later) component must 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).
 - The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and later only.
 - Consult your SAP documentation to determine if your R/3 landscape components requires additional software installed to run or work with CCMS.
 - You must have SAP authorization of the remote system user. For details on the minimum SAP permission required by SiteScope, see the sections on “AAAB - Cross-application Authorization Objects” and “BC_A - Basis: Administration” in [SAP RFC User privileges](#) in the SAP documentation (http://help.sap.com/saphelp_nw73/helpdata/de/49/bb35b8623a489aa63abd9f5ebf2448/content.htm).
 - 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 log on 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_ALLOne test to see if a user has such authorization is to try and issue transaction RZ20 in the SAP user interface and see if the CCMS monitor sets can be displayed.
 - The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries.

2. Download the SAP Java Connector

The SAP Java Connector (SAP JCo version 2.0.6 or later) component must be downloaded and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

- a. To download SAP Java Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>).

Note: You need a valid Service Marketplace login to access the SAP Web site

- b. After you log on, select **SAP NetWeaver > SAP NetWeaver in Detail > Application Platform > Connectivity > Connectors > SAP Java Connector**, and then click **Tools and Services**.

3. Enable the SAP CCMS Alerts monitor

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.

- a. Download the following files from the SAP support Web site (<http://www.service.sap.com/connectors>):

On a Windows environment:

File	Copy to...
sapjco.jar	<SiteScope root directory>\WEB-INF\lib
librfc32.dll	<SiteScope root directory>\bin
sapjcorfc.dll	Note: 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), you must overwrite them with these .dll files before copying them into the SiteScope directory.

On a UNIX environment:

File	Copy to...
sapjco.jar	<SiteScope root directory>/WEB-INF/lib Note: JCO native libraries must be copied to /usr/lib for 32-bit platforms and to /usr/lib64 for 64-bit platforms. To check that a JCO connector is installed correctly, run the following command: <pre>/opt/HP/SiteScope/java/bin/java -jar /opt/HP/SiteScope/WEB-INF/lib/sapjco.jar</pre>
librfccm.so libsapjcorfc.so	<ul style="list-style-type: none"> o For Sun installations: <SiteScope root directory>/java/lib/sparc o For Linux installations: /usr/lib for 32-bit platforms and /usr/lib64 for 64-bit platforms.

- b. Restart SiteScope.

4. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Note: Although you can change the run schedule for this monitor using the **Frequency** setting in Monitor Run Settings (the default is every 10 minutes), CCMS metrics are generally only updated once every 5 minutes.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

SAP CCMS Alerts Monitor Settings

User interface elements are described below:

UI Element	Description
Application server	Host name/IP address of the SAP server you want to monitor.
SAP client	Client to use for connecting to SAP.
System number	System number for the SAP server.
SAP router string	<p>Router address string if your connection is being made through a router (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>
Credentials	<p>Option for providing the user name and password to access the SAP CCMS metrics:</p> <ul style="list-style-type: none">• Use user name and password. Select this option to manually enter user credentials. Enter the user name and password to access the SAP server in the User name and Password box.• Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p>Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 74

SAP Java Web Application Server Monitor

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 monitor is an optional SiteScope monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. 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 in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP Java Web Application Server monitor.

Learn More

Supported Platforms/Versions

This monitor supports monitoring SAP Java Web Application Server 6.40, 7.00, and SAP Enterprise Portal 5.0, 6.0 and 7.0.

Tasks

How to Configure the SAP Java Web Application Server Monitor

1. Prerequisites

- This monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running.
- You must have SAP authorization of the remote system user. For details on the minimum SAP permission required by SiteScope, see the sections on “AAAB - Cross-application Authorization Objects” and “BC_A - Basis: Administration” in [SAP RFC User privileges](#) in the SAP documentation (http://help.sap.com/saphelp_nw73/helpdata/de/49/bb35b8623a489aa63abd9f5ebf2448/content.htm).
- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries
- The SAP Java Web Application Server monitor uses SAP JMX Connector libraries to connect to SAP J2EE cluster. Depending on your monitored environment, the JMX Connector files are available on the SAP Java Web Application server from `\usr\sap\<SID>\JC<InstanceNumber>\j2ee\admin\lib` or `\usr\sap\<SID>\DVEBMGS<InstanceNumber>\j2ee\admin\lib`.
 - i. Copy the following .jar files from the SAP Java Web Application server installation into the `<SiteScope root directory>\WEB-INF\lib` directory:
 - **admin.jar**
 - **com_sap_pj_jmx.jar**
 - **exception.jar**
 - **logging.jar**
 - **jmx.jar**
 - ii. Restart SiteScope
- To enable monitoring a SAP Java Web Application Server 6.40 or 7.00-7.02 server, you must install a patch (SAP Note 1740150) from the SAP portal ([https://websmp230.sap-ag.de/sap\(bD11biZjPTAwMQ==\)/bc/bsp/spn/sapnotes/index2.htm?numm=1740150](https://websmp230.sap-ag.de/sap(bD11biZjPTAwMQ==)/bc/bsp/spn/sapnotes/index2.htm?numm=1740150)). The SAP JMX Client jars should be taken from the patched SAP system.

For versions SAP NetWeaver 7.1.1 and higher, the following JMX client jars should be copied from `\usr\sap\130\DVEBMGS00\j2ee\j2eeclient` on the SAP Java Web Application server:

 - **sap.com~tc~exception~impl.jar**
 - **sap.com~tc~je~clientlib~impl.jar**
 - **sap.com~tc~je~leanClient.jar**
 - **sap.com~tc~logging~java~impl.jar**

- **tc~bl~base~client.jar**
 - **tc~bl~deploy~client.jar**
2. Enable monitoring the P4 port using a secure connection - optional
 - a. Copy the jar files from the **usr\sap\<INSTANCE_NAME>\SYS\global\security\lib\tools** directory on the SAP machine into the **<SiteScope root directory>\WEB-INF\lib** directory.
 - b. When setting the monitor properties (in the following step), configure the following:
 - **Port.** Enter the port number that allows P4 over SSL connections. For details on J2EE port requirements, see http://help.sap.com/saphelp_nw04/helpdata/en/a2/f9d7fed2adc340ab462ae159d19509/frameset.htm.
 - **Transport layer:** Select **SSL**.
 3. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

SAP Java Web Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
Application server	Address of the SAP Java Web Application Server you want to monitor.
Port	Number of the P4 port for the SAP Java Web Application Server you want to monitor. For details on J2EE port requirements, see http://help.sap.com/saphelp_nw04/helpdata/en/a2/f9d7fed2adc340ab462ae159d19509/frameset.htm . Default value: 50004
Transport layer	Select the option for monitoring the P4 port. <ul style="list-style-type: none"> • SSL. Select this option to monitor P4 using a secure SSL transport layer connection. • No underlying transport layer. Select this option to use a non-secure connection.
Credentials	Option for providing the user name and password to access the SAP server: <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password to access the SAP server in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. These counters are received dynamically from the JMX. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 75

SAP Performance Monitor

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 enables 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. The error and warning thresholds for the monitor can be set on SAP server and database performance statistics.

Note:

- The SAP Performance monitor is an optional SiteScope monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. 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 in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP Performance monitor.

Learn More

Supported Platforms/Versions

This monitor supports monitoring SAP Application Servers R/3 4.6B, R/3 4.6C, R/3 4.7E, SAP ECC5 and SAP ECC6.

Tasks

How to Configure the SAP Performance Monitor

1. Prerequisites

- You must have SAP authorization of the remote system user. For details on the minimum SAP permission required by SiteScope, see the sections on “AAAB - Cross-application Authorization Objects” and “BC_A - Basis: Administration” in [SAP RFC User privileges](http://help.sap.com/saphelp_nw73/helpdata/de/49/bb35b8623a489aa63abd9f5ebf2448/content.htm) in the SAP documentation (http://help.sap.com/saphelp_nw73/helpdata/de/49/bb35b8623a489aa63abd9f5ebf2448/content.htm).
- A SAP 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
- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries.

2. Download the SAP Java Connector

The SAP Java Connector (SAP JCo version 2.0.6 or later) component must be downloaded and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

- a. To download SAP Java Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>).

Note: You need a valid Service Marketplace login to access the SAP Web site

- b. After you log on, select **SAP NetWeaver > SAP NetWeaver in Detail > Application Platform > Connectivity > Connectors > SAP Java Connector**, and then click **Tools and Services**.

3. Enable the SAP Performance monitor

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.

- a. Download the following files from the SAP support Web site (<http://www.service.sap.com/connectors>):

On a Windows environment:

File	Copy to...
sapjco.jar	<SiteScope root directory>\WEB-INF\lib
librfc32.dll sapjcorfc.dll	<p><SiteScope root directory>\bin</p> <p>Note: 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), you must overwrite them with these .dll files before copying them into the SiteScope directory.</p>

On a UNIX environment:

File	Copy to...
sapjco.jar	<p><SiteScope root directory>/WEB-INF/lib</p> <p>Note: JCO native libraries must be copied to /usr/lib for 32-bit platforms and to /usr/lib64 for 64-bit platforms. To check that a JCO connector is installed correctly, run the following command:</p> <pre>/opt/HP/SiteScope/java/bin/java -jar /opt/HP/SiteScope/WEB-INF/lib/sapjco.jar</pre>
librfccm.so libsapjcorfc.so	<ul style="list-style-type: none"> ○ For Sun installations: <SiteScope root directory>/java/lib/sparc ○ For Linux installations: /usr/lib for 32-bit platforms and /usr/lib64 for 64-bit platforms.

b. Restart SiteScope.

4. **Configure the monitor properties**

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

SAP Performance Monitor Settings

User interface elements are described below:

UI Element	Description
Application server	Address of the SAP server you want to monitor.
SAP client	Client to use for connecting to SAP.
System number	System number for the SAP server.
SAP router string	<p>Router address string if your connection is being made through a router (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>
Credentials	<p>Option for providing the user name and password to access the SAP server:</p> <ul style="list-style-type: none">• Use user name and password. Select this option to manually enter user credentials. Enter the user name and password to access the SAP server in the User name and Password box.• Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p>Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 76

SAP Work Processes Monitor

The SAP Work Processes monitor enables 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.

Using the SAP Work Processes monitor, you can also enable reporting of the host topology to BSM. If enabled, BSM automatically populates the RTSM with CIs based on the monitored hardware in SiteScope.

Note: The SAP Work Processes monitor is an optional SiteScope monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. Contact your HP sales representative for more information.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP Work Processes monitor.

Learn More

This section contains the following topics:

- ["Understanding the SAP Work Processes Monitor" below](#)
- ["Supported Platforms/Versions" below](#)
- ["SAP Work Processes Topology" 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.

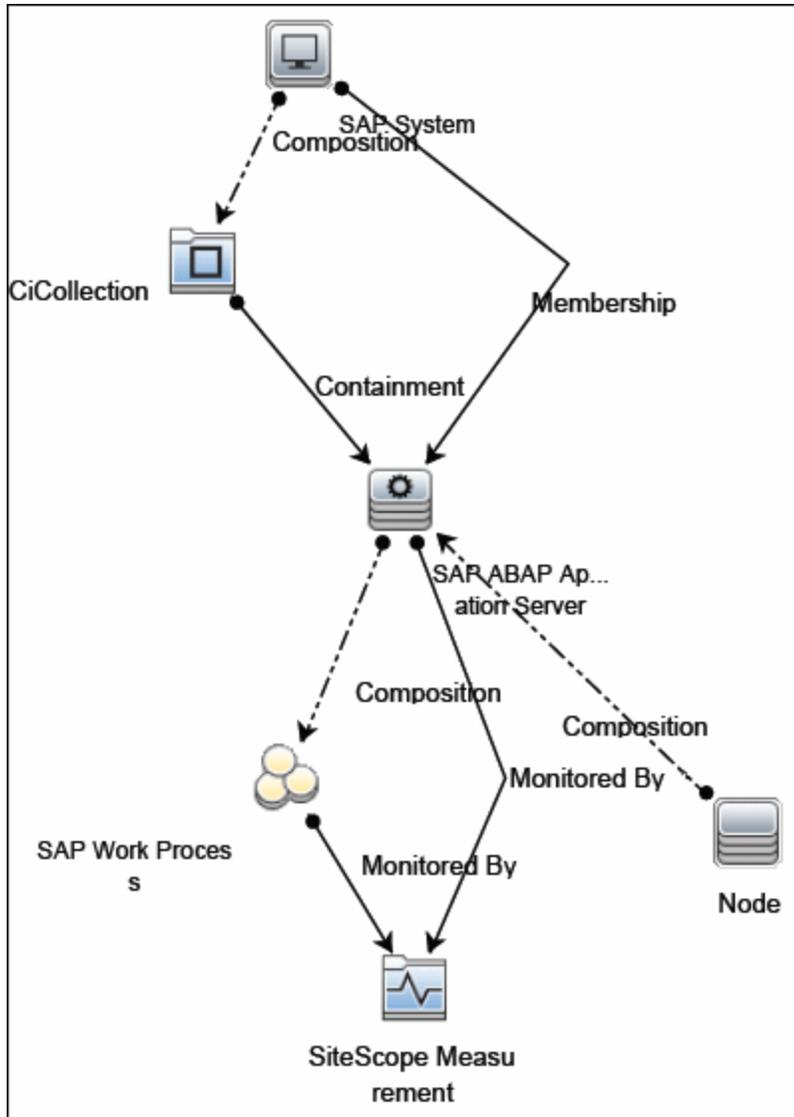
The dispatcher assigns tasks to the free work processes, making optimal use of system resources and balancing the system load. The dispatcher knows and distributes pending tasks according to the type of the defined processes. The difference among the various work processes affects only those tasks or special services that have been assigned to the work processes through the dispatching strategy.

Supported Platforms/Versions

This monitor supports monitoring SAP Application Servers R/3 4.6B, R/3 4.6C, R/3 4.7E, SAP ECC5 and SAP ECC6 servers.

SAP Work Processes Topology

The SAP Work Processes monitor can identify the work processes of the server being monitored. The monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM as SiteScope Measurement Groups and SiteScope Measurement CIs.

Note: This direct integration between SiteScope and BSM is available only when the Application Management for SAP license is installed.

For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

For information about the SAP topology, see SAP Systems View in the BSM User Guide in the BSM Help.

Tasks

How to Configure the SAP Work Processes Monitor

1. Prerequisites

- You must have SAP authorization of the remote system user. For details on the minimum SAP permission required by SiteScope, see the sections on “AAAB - Cross-application Authorization Objects” and “BC_A - Basis: Administration” in [SAP RFC User privileges](http://help.sap.com/saphelp_nw73/helpdata/de/49/bb35b8623a489aa63abd9f5ebf2448/content.htm) in the SAP documentation (http://help.sap.com/saphelp_nw73/helpdata/de/49/bb35b8623a489aa63abd9f5ebf2448/content.htm).
- A SAP 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
- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries.

2. Download the SAP Java Connector

The SAP Java Connector (SAP JCo version 2.0.6 or later) component must be downloaded and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

- a. To download SAP Java Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>).

Note: You need a valid Service Marketplace login to access the SAP Web site

- b. After you log on, select **SAP NetWeaver > SAP NetWeaver in Detail > Application Platform > Connectivity > Connectors > SAP Java Connector**, and then click **Tools and Services**.

3. Enable the SAP Performance monitor

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.

- a. Download the following files from the SAP support Web site (<http://www.service.sap.com/connectors>):

On a Windows environment:

File	Copy to...
sapjco.jar	<SiteScope root directory>\WEB-INF\lib
librfc32.dll sapjcorfc.dll	<p><SiteScope root directory>\bin</p> <p>Note: 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), you must overwrite them with these .dll files before copying them into the SiteScope directory.</p>

On a UNIX environment:

File	Copy to...
sapjco.jar	<p><SiteScope root directory>/WEB-INF/lib</p> <p>Note: JCO native libraries must be copied to /usr/lib for 32-bit platforms and to /usr/lib64 for 64-bit platforms. To check that a JCO connector is installed correctly, run the following command:</p> <pre>/opt/HP/SiteScope/java/bin/java -jar /opt/HP/SiteScope/WEB-INF/lib/sapjco.jar</pre>
librfccm.so lib- sapjcorfc.so	<ul style="list-style-type: none"> ○ For Sun installations: <SiteScope root directory>/java/lib/sparc ○ For Linux installations: /usr/lib for 32-bit platforms and /usr/lib64 for 64-bit platforms.

b. Restart SiteScope.

4. **Configure the monitor properties**

Configure the monitor properties as described in the UI Descriptions section below.

5. **Enable topology reporting - optional**

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "SAP Work Processes Topology" on page 550.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

SAP Work Processes Monitor Settings

User interface elements are described below:

UI Element	Description
Application server	Address of the SAP server you want to monitor.
SAP client	Client to use for connecting to SAP.
System number	System number for the SAP server.
SAP router string	<p>Router address string if your connection is being made through a router (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>
Credentials	<p>Option for providing the user name and password to access the SAP server:</p> <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password to access the SAP server in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p>Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 77

Script Monitor

This monitor enables you to integrate existing system management scripts into the SiteScope environment by running external commands and reporting the command result. It also enables you to parse and report a specific value from the command output.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Script monitor.

Learn More

This section includes:

- "Script Monitor Overview" below
- "Supported Platforms/Versions" below
- "Script Options" below
- "Status" on the next page
- "Caching Script Output" on page 559
- "Setting a Timeout Value for Script Execution" on page 559
- "Running Different Types of Scripts" on page 559

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 email or page you if this monitor was in error.

Symbolic links are now supported when executing scripts on remote UNIX servers. This support is enabled by setting the property `_scriptMonitorAllowSymbolicLink` to `true` (false by default) in the `master.config` file. When enabled, the symbolic link appears in the list of available scripts when configuring a Script monitor to monitor a UNIX remote.

Supported Platforms/Versions

- The Script monitor supports monitoring remote servers running on Windows platforms and on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see "How to Configure the HP NonStop Resources Monitor" on page 282.
- This monitor is also supported in SiteScopes that are running on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.

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 <code><SiteScope root directory>\scripts</code> directory.

Script Option	Description
Remote Script	<p>A remote script file (UNIX and Windows-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>Note:</p> <ul style="list-style-type: none"> On Window platforms, the path to the user home directory depends on the particular SSH server. For example if you install a Cygwin SSH server in <code>C:\Cygwin</code>, the default path to the home directory for the Administrator user will be <code>C:\Cygwin\home\Administrator</code>. For additional information, see the documentation for your SSH server. Only executable script files are displayed. <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	<p>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.</p>

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, or 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 (seconds)** setting in the Monitor Settings section. To configure multiple Script monitors to use the data in the cache, each monitor instance must be:

- Configured to use the same remote Server profile.
- Configured to use the same Script file.
- Have a **Cache life (seconds)** value greater than zero.

The **Cache life (seconds)** 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 (seconds)** 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.

For details on how to set a timeout value for script execution, see "[Script Monitor Settings](#)" on page 562.

Running Different Types of Scripts

You can run non-batch scripts, for example VBScript or Perl scripts, without wrapping them into a batch file.

Note: This is supported only on Windows machines where SiteScope Server is the target of the Script monitor.

- You can see scripts with any extensions by adding the **_scriptMonitorExtensions** property to 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 in the **master.config** file as follows: `_`

```
script-
```

```
Interpreters=pl=c:/perl/perl.exe;py=c:/python/python.exe;php=c:/php/  
php.exe
```

Tasks

How to Configure the Script Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Script Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server where the script you want to run is stored. Select a server from the server list (only those Windows and UNIX remote servers configured in SiteScope using SSH are displayed).</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Add Remote Server	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Script	<p>The script to run. SiteScope gets scripts from a scripts subdirectory in the home directory of the account SiteScope uses to access the remote server. For example, <code>home/sitescope/scripts</code>. On Windows, SiteScope gets scripts from the home directory on the remote machine (this depends on the SSH server configuration). For example, <code>C:\Documents and Settings\Administrator\Scripts</code> directory.</p> <p>When monitoring the SiteScope Server, 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 Remote script command file field 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 <code>test.sh</code> and save it in the <SiteScope root directory>\scripts.remote directory. Edit <code>test.sh</code> 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 <code>test.sh</code> as the USE COMMAND script to run.</p> <p>Note: The <code>diskSpace.bat</code> script accepts only 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, we recommend that you use the Disk Space monitor instead.</p>
Parameters	<p>Specifies any additional parameters to pass to the script. You can use a regular expression or use the attributes found in SiteScope alert templates to insert variables into the parameters box. For details, see SiteScope Alert Template and Event Properties Directory.</p> <p>Example: <code>s/\$month\$ \$day\$ \$year\$ /</code> passes the current month, day and year to the script.</p> <p>Syntax exceptions: SiteScope cannot pass the following characters to scripts: <code>` ; & </code></p>
Output encoding	<p>The encoding used on the server where SiteScope is running if the command output uses an encoding that is different than. This enables SiteScope to match and display the encoded file content correctly.</p> <p>Default value: windows-1252</p>

UI Element	Description
Match value labels	<p>Labels for the matched values found in the script output. The matched value labels are used as variables to access retained values from the match expression for use with the monitor threshold settings. These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.</p> <p>Example: Enter <code>Copyright_start, Copyright_end</code> to represent the copyright date range used in the Match expression field. After the monitor runs, these labels are displayed in the Condition list in Threshold Settings, enabling you to set status threshold settings (Error if, Warning if, and Good if) for the matched value.</p> <p>Note:</p> <ul style="list-style-type: none"> • Separate multiple labels with a comma (,). • You can set up to 10 labels.
Match expression	<p>Regular expression used to retrieve values from the script output. For example, the expression: <code>/(\d+)/</code> matches one or more digits returned by the script. Use parentheses to enable the monitor to retrieve these values as counters.</p> <p>By using the labels in Match value labels, these counters can be automatically assigned with a customized name and you can define thresholds for them. 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>Example: <code>/([UDTCP]{3,4})s*([\w\d\W]{5,35}\:\d+)s*([\w\d\W]{5,35}\:\d+)s*([A-Z]{5,35})s</code> could be used to match and retain values from the four columns of the following command output:</p> <pre>TCP planetcom:2664 COMSRVF01:2412 ESTABLISHED</pre> <p>Note:</p> <ul style="list-style-type: none"> • If this item is left blank, no value is retrieved from the script. • You can use up to 10 sets of parentheses to retain multiple values from the script output.
Open Tool	<p>Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.</p>

UI Element	Description
Remote script command file	<p>The script file that contains the commands that SiteScope should send to the remote machine if you USE COMMAND is selected as the Script option and a remote machine as the Server. 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. Enter 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>Default value: none</p> <p>Syntax 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>
Cache life (seconds)	<p>Uses 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"> Enter a time value (in seconds) greater than zero to have SiteScope cache the output of the script execution. 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. Enter a value of 0 (zero) to disable the cache function. This causes the monitor to run the script each time that it runs. <p>Default value: 0</p>
Measurement maximum (milliseconds)	<p>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>
Timeout (seconds)	<p>Amount of time, in seconds, to wait for the script to run successfully before timing out.</p> <p>Default value: -1 (no timeout)</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying a Script monitor from a template, the case of the remote script name must match that of the script in the scripts subdirectory. Otherwise, the selected script is shown as 'none'.
- The Script monitor **round trip time** counter includes SiteScope server loading time, such as time required for preparing the monitor run, the network transfer, and script execution. The **script execution time** counter shows the time spent for running the script (it is preferable to use this counter for script performance diagnostics than the **round trip time** counter).

Chapter 78

Service Monitor

The Service monitor verifies that specific services or processes are listed as running, and optionally, it can also check to see how much CPU and memory (Page File Bytes) a service or process is using. If a service or 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 service or process to help minimize the effect on other operations and downtime.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Service monitor.

Learn More

This section includes:

- "Service Monitor Overview" below
- "Supported Platforms/Versions" below
- "Status" below
- "Scheduling the Monitor" below
- "IPv6 Addressing Supported Protocols" on the next page

Service Monitor Overview

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.

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 if your monitor fails. For details on using a Script Alert, see Working with Script Alerts in the Using SiteScope Guide.

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows platforms, and also on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

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 good or error. An error status is returned if the service is not found.

Scheduling the 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 either server, managing a large number of remote connections

can result 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.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

Note: When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`

would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the Service Monitor

1. Prerequisites

SiteScopes running on Windows platforms need 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 Servers option in the remote server view.

For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **Services Tool** is available when configuring this monitor to view services running on the server where SiteScope is installed (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Services Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Service Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server where the service or process you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note: Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none">• Browse servers. Select a server from the drop-down list of servers in the local domain.• Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Service	<p>The service (or process in UNIX) that you want to monitor from the services list.</p> <p>To monitor a Windows process, select (Using Process Name) in the drop-down list and enter the name in the Process name box.</p> <p>Note: The CPU and memory (Page File Bytes) counters are relevant for processes and not for services, and it is displayed only if the selected service is by process name.</p>
Other service	<p>Name of the service you want to monitor (if it is not listed in the services list).</p> <p>Note: This field is available only when Unknown is selected in the Service box.</p>
Process name	<p>(For Windows only) Name of the process if you want to get information about the percentage of CPU and memory (Page File Bytes) being used by a specific process and/or the number of a specific type of process running. Use a string or a regular expression.</p> <p>Note:</p> <ul style="list-style-type: none"> • The name of the process must be as it appears in Windows Task Manager. • This field is available only when (using Process name) is selected in the Service box. <p>Example: explorer.exe</p>
Measure process memory use	<p>For UNIX only) SiteScope reports the amount of virtual memory being used by a specific process.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- In Threshold Settings, the CPU and memory (Page File Bytes) measurements are relevant only for processes and not for system services. If the selected service is a process name, CPU and memory (Page File Bytes) measurements are in the drop-down list. If the selected service is a system service, such as `Event Log`, CPU and memory (Page File Bytes) measurements are not listed.
- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- Added the ability to reduce Service monitor runtime by adding the `_serviceMonitorOptByServiceName=true` property to the `<SiteScope root directory>\groups\master.config` file. This enables the monitor to retrieve data for the service selected for monitoring only, instead of retrieving all services from the remote machine, and then sorting for the selected service.

Chapter 79

Siebel Application Server Monitor

The Siebel Application Server monitor uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel application servers.

Note:

- This monitor is an optional SiteScope monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. 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 in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Siebel Application Server monitor.

Learn More

This section includes:

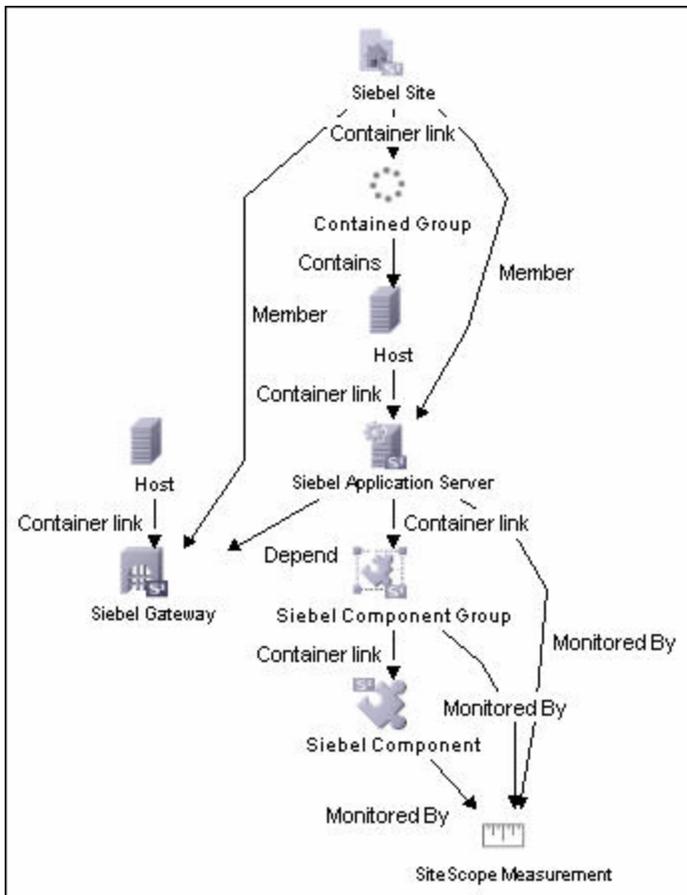
- "Supported Platforms/Versions" below
- "Siebel Application Server Topology" below

Supported Platforms/Versions

This monitor uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel 7.03, 7.04, 7.5.3, 7.7, 8.0, and 8.1 application servers.

Siebel Application Server Topology

The Siebel Application Server monitor can identify the topology of the Siebel Application Servers being monitored. The monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM as SiteScope Measurement Groups and SiteScope Measurement CIs.

Note: This direct integration between SiteScope and BSM is available only when the Application Management for Siebel license is installed.

Monitor Reference

Chapter 79: Siebel Application Server Monitor

For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

For information about the Siebel topology, see Siebel Views in the BSM User Guide in the BSM Help.

Tasks

How to Configure the Siebel Application Server Monitor

1. Prerequisites

The following are requirements for using the Siebel Application Server monitor:

- The Siebel Server Manager client must be installed only on the machine where SiteScope is running or that is accessible to the SiteScope. 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. This option is applicable only for UNIX remotes.
 - 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 (usually called **srvmgr** or **srvmgr.exe**).
- 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 this setting, open the **Preferences** context, select **Infrastructure Settings** Preferences, and expand the **General Settings** section.

- For SiteScope on Solaris/Linux: You must make sure that the Siebel Server Manager Client's libraries are available to the Client. 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.
```

2. **Configure the monitor properties**

Configure the monitor properties as described in the UI Descriptions section below.

3. **Enable topology reporting - optional**

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "Siebel Application Server Topology" on page 575.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Siebel Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
Siebel host name	<p>Siebel host name is required if you are doing either of the following:</p> <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. Enter the Host Server Name of the Siebel Remote definition (not the Title). This is the Windows Server Address box for Windows remote servers or Server Address box for UNIX remote servers. • Reporting monitor data to an installation of HP Business Service Management. 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 a BSM report. The box is optional only if the Script Server box is already specified to be the target Siebel server.
Application server	Siebel server name or address.
Gateway server	Gateway server name or address.
Enterprise server	Enterprise server name or address.
Credentials	<p>Siebel Server Manager client requires a user name and password. Option to use for providing credentials:</p> <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (selected by default). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.

UI Element	Description
<p>Script server</p>	<p>The remote Windows or UNIX machine where the Server Manager (srvmgr) script is installed. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>The method of connection is either SSH or Telnet (but not Microsoft NetBIOS). For NetBIOS, choose this server and map the drive.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
<p>Browse Servers</p>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> • Browse servers. Select a server from the drop-down list of servers visible in the local domain. • Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<p>Add Remote Server</p>	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
<p>Script path</p>	<p>Full path to the Siebel Server Manager executable directory relative to the machine chosen above.</p> <p>Example:E:\sea704\client\BIN</p>
<p>Counters</p>	<p>Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.</p>
<p>Get Counters</p>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p>Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

UI Element	Description
Siebel tasks time window (minutes)	<p>A time window in which tasks are monitored on the Siebel application server. This setting applies only to the "No. of Tasks in XXX" counters. This value tells SiteScope to count tasks that have started within the last N minutes only. It can be used, for instance, to make SiteScope monitor only newly occurring tasks.</p> <p>Example: 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: <code>time window = (current time - property value)</code>.</p> <p>Enter 0 to monitor every task on the Siebel application server, regardless of its start time.</p> <p>Default value: 60 minutes</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers**, **Add Remote Server**, and **Add Credentials** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 80

Siebel Log File Monitor

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 receive warnings before issues escalate into more serious problems.

Note: The Siebel Log File monitor is an optional SiteScope monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. Contact your HP sales representative for more information.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Siebel Log File monitor.

Learn More

This section includes:

- "Siebel Log File Monitor Overview" below
- "Supported Platforms/Versions" below

Siebel Log File Monitor Overview

The Siebel Log File monitor checks for log file entries added to a group of log files by looking for entries containing a specific event type or subtype.

Each time that SiteScope runs this monitor, it starts from the point in the file where it stopped reading last time it ran. This ensures that you are only notified of new entries and speeds the rate at which the monitor runs. While this behavior can be overridden, we do not recommend it, and this 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.

Supported Platforms/Versions

This monitor supports monitoring remote servers running on Siebel Application Server 7.03, 7.04, 7.5.3, 7.7, 8.0, and 8.1.

Tasks

How to Configure the Siebel Log File Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

This section includes:

- "Siebel Log File Monitor Settings" below
- "Settings Common to All Monitors"

Siebel Log File Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>The Siebel server where the log files you want to monitor are running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none"> • Browse servers. Select a server from the drop-down list of servers visible in the local domain. • Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note: To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
Add Remote Server	<p>Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Log file directory	<p>Path to the log directory you want to monitor.</p> <p>To monitor log files on a remote Windows 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 Windows server, you must select the java library and ssh1 options for that remote.</p>
File name (regular expr.)	<p>Log files that you want to monitor. You must use a regular expression to specify multiple files, and the regular expression string must be enclosed in forward slashes (for example, /<my reg exp>/). 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>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> <p>Default value: Fatal</p>
Event type	<p>Matching event type or subtype. The monitor reports how many log entries were found of the specified type.</p> <p>Default value: GenericLog</p>
Log-entry content match	<p>(Optional) 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>Always checks the contents of the whole file. If this option is not selected, SiteScope checks only newly-added records, starting at the time that the monitor was created (not when the file was created).</p> <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: Not selected</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

Chapter 81

Siebel Web Server Monitor

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:

- This monitor is an optional SiteScope monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. 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 in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Siebel Web Server monitor.

Learn More

This section includes:

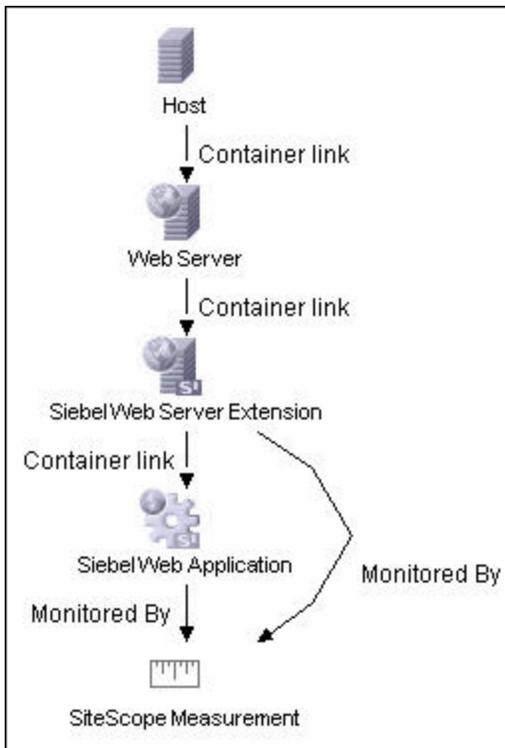
- "Supported Platforms/Versions" below
- "Siebel Web Server Topology" below

Supported Platforms/Versions

This monitor supports monitoring remote servers running on Siebel Application Server 7.03, 7.04, 7.5.3, 7.7, 8.0, and 8.1.

Siebel Web Server Topology

The Siebel Web Server monitor can identify the topology of the Siebel Web Server being monitored. The monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM as SiteScope Measurement Groups and SiteScope Measurement CIs.

Note: This direct integration between SiteScope and BSM is available only when the Application Management for Siebel license is installed.

For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

Monitor Reference

Chapter 81: Siebel Web Server Monitor

For information about the Siebel topology, see Siebel Views in the BSM User Guide in the BSM Help.

Tasks

How to Configure the Siebel Web Server Monitor

1. Prerequisites

The following are 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. Refer to the Siebel documentation for more information.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "[Siebel Web Server Topology](#)" on page 590.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

This section includes:

- "Siebel Web Server Monitor Settings" below
- "Settings Common to All Monitors"

Siebel Web Server Monitor Settings

User interface elements are described below:

UI Element	Description
Basic Settings	
Application URL	URL of the Web plug-in server stats page for the application you want to monitor. Example: <code>http://siebelsrv/service/_stats.swe</code> If the Siebel Web server is configured to support verbose mode, you can also use <code>http://siebelsrv/service/_stats.swe?verbose=high</code> to include information on Locks and Current Operations Processing for the Siebel server.
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.
Connection Settings (These settings are optional, unless the server requires authentication)	
Authorization user name	User name to access the Web server stats page.
Authorization password	Password for accessing the Web server stats page.
HTTP proxy	Proxy server and port to use if you are using a proxy to access the Siebel server. Example: <code>proxy.SiteScope.com:8080</code>
Proxy server user name	Proxy user name if the proxy server requires authorization.

UI Element	Description
Proxy server password	<p>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>
<p>HTML Form-Based Authentication (These settings are optional, unless the server requires authentication)</p>	
HTML form-based authentication required	<p>SiteScope submits HTML form-based authentication when accessing the Siebel Web server plug-in.</p>
Authorization form name	<p>Authentication form identifier within the Web page when using HTML Form-based Authentication. 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 user name form field	<p>User name that should be submitted to the access control system when using HTML Form-based Authentication. 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.</p>
Authorization password form field	<p>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.</p>
Authorization form button	<p>Identifier of the Submit button on the authentication form when using HTML Form-based Authentication.</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>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 82

SNMP Monitor

This monitor enables you to monitor devices that communicate with the SNMP protocol, such as firewalls, routers, and UPS systems.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SNMP monitor.

Learn More

This section includes:

- "SNMP Monitor Overview" below
- "Supported Platforms/Versions" below
- "IPv6 Addressing Supported Protocols" below

SNMP Monitor Overview

Many network devices support the SNMP protocol as a way of monitoring them. 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 (MIBs) 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 Object ID that maps to that value. The Object ID's may be available in the product documentation or in the form of a MIB file. 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.

Supported Platforms/Versions

This monitor supports monitoring agents of SNMP versions 1.0, 2.0, and 3.0 MD5 and SHA.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the SNMP Monitor

1. Prerequisites

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 (MIBs) and configured to read those MIBs.
- If SNMP version 3 is used, a valid user name and password might be required to access the SNMP device.
- 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. If you want the monitor to get you the next OID of the OID you entered, you can enter 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) (<http://h20230.www2.hp.com/selfsolve/documents>). To enter the knowledge base, you must log on with your HP Passport ID.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **SNMP Tool** is available when configuring this monitor to query a SNMP Management Information Base (MIB) and retrieve a set of OIDs (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Tool.

Related workflow

"How to Deploy a Monitor" in the Using SiteScope Guide

UI Descriptions

SNMP Monitor Settings

User interface elements are described below:

UI Element	Description
Basic SNMP Settings	
Host name	Host name or IP address of the SNMP device that you want to monitor (for example, <code>demo.thiscompany.com</code>).
Port	Port to use when requesting data from the SNMP agent. Default value: 161

UI Element	Description
Object ID	<p>Select the Object ID setting:</p> <ul style="list-style-type: none"> Commonly used values. Select the Object ID mnemonic from the drop-down list. (This is the default option with system.sysDescr set as the default value.) <p>Enter 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. The index value for Commonly used values is set to <code>ifSpecific.ifInOctets</code>. <p>Default value: 0</p> <ul style="list-style-type: none"> Other values. Enter the Object Identifier (OID) for the SNMP value you want to retrieve. The OID specifies which value should be retrieved from the device. <p>Example: 1.3.6.1.2.1.4.3</p> <p>Tip: 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 cannot be found.</p> <p>Note: SiteScope supports SNMP versions 1.0, 2.0, and 3.0.</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 enter 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>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>

UI Element	Description
Secondary object ID	<p>Secondary object ID and Secondary match content are used for creating a new Object ID and for getting data for it. The SNMP monitor gets data using the main Object ID, and the data that is matched by the Secondary match content {index corresponding to the group} is used in the Secondary object ID.</p> <p>Example: Secondary match content matches the first digit and can be used in the Secondary object ID using the next construction 1.3.6.5.{0}, or it can match the full Object ID and the Secondary object ID can be set using the next construction {0}.</p> <p>(To enable secondary object changes, you must add the property <code>_enableSecondSNMP=true</code> to the <code>master.config</code> file.)</p>
Secondary match content	<p>Sets up a secondary SNMP index. Match this item against the main SNMP value using a string, regular expression (see Regular Expressions Overview), or XML names (see Monitoring XML Documents Overview in the Using SiteScope Guide).</p> <p>Example: <code>/ (\d) /</code> gets the first digit and uses it in the secondary index.</p>
SNMP Connection Settings	
Timeout (seconds)	<p>Amount of time, in seconds, that SiteScope should wait for an SNMP request.</p> <p>Default value: 5 seconds</p>
Number of retries	<p>Number of SNMP request retries before SiteScope considers the monitor to have failed.</p> <p>Default value: 1</p>
Community	<p>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>Default value: public</p> <p>Note: The field is valid only for version 1 or 2 connections.</p>
SNMP version	<p>SNMP version used by the SNMP host you want to monitor. SiteScope supports SNMP version 1, version 2, and version 3.</p> <p>Default value: V1</p>

UI Element	Description
Authentication algorithm	Authentication algorithm used for SNMP V3. You can select MD5, SHA, or None. Note: This field is available only if SNMP V3 is selected.
User name	User name to be used for authentication if you are using SNMP version 3. Note: This field is available only if SNMP V3 is selected.
Password	Password to be used for authentication if you are using SNMP version 3. Note: This field is available only if SNMP V3 is selected.
Privacy algorithm	The privacy algorithm used for authentication for SNMP version 3 (DES, 128-Bit AES, 192-Bit AES, 256-Bit AES). Default value: DES Note: This field is available only if SNMP V3 is selected.
Privacy password	The privacy password used for authentication for SNMP version 3. Leave blank if you do not want privacy. Note: This field is available only if SNMP V3 is selected.
Context name	The context name of SNMP version 3. Note: This field is available only if SNMP V3 is selected.
Context engine ID	The context engine ID of SNMP version 3. Note: This field is available only if SNMP V3 is selected.
SNMP Data Manipulation Settings	
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 box. Default value: No scaling
Match content	Use to match against an SNMP value, using a string or a regular expression or XML names.
Open Tool	Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.
Units	Optional units string to append when displaying the value of this counter.
Measurement label	Optional text string to describe the measurement being made by the monitor.

UI Element	Description
Measure as delta	Reports the measurement as the difference between the current value and the previous value.
Measure as rate per second	Divides the measurement by the number of seconds since the last measurement.
Percentage base	Value to use for calculating the percentage base from the Commonly used values list or by typing a number or SNMP object ID in the Other values box. If entered, the measurement is divided by this value to calculate a percentage. Default value: No percentage base
Measure base as delta	Calculates 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	Maximum value for the Object ID. The maximum is calculated to create the gauge display (Optional).

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 83

SNMP by MIB Monitor

The SNMP by MIB monitor enables you to monitor objects on any SNMP agent.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SNMP by MIB monitor.

Learn More

This section includes:

- "SNMP by MIB Monitor Overview" below
- "IPv6 Addressing Supported Protocols" below

SNMP by MIB Monitor Overview

The SNMP by MIB monitor gathers information from a source, organizes it into a browsable tree structure, and enables 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 MIBs 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 SNMP version 1, 2, and 3 MD5.

The MIB files in **<SiteScope root directory>\templates.mib** are then used to create a browsable tree that contains names and descriptions of the objects found during a traversal. An object may or may not be displayed with a textual name and description, depending on the MIBs available in **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.

The error and warning thresholds for the monitor can be set on one or more different objects.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the SNMP by MIB Monitor

1. Add MIBs to the templates.mib directory

You can add to the MIBs of which SiteScope is aware by putting new MIB files in the **templates.mib** directory.

Note: Since 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.

- a. To check compilation of the new MIB, you can use the command line tool located in **<SiteScope root directory>\tools\SNMPMIBCompilation**. This tool enables you to check the new MIB compilation without having to restart SiteScope for every change you make in the MIB file. 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.
- b. 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.
- c. Restart SiteScope.
- d. Proceed to add a new SNMP by MIB monitor. Before adding the monitor, check that your new MIB files are listed in the **MIB file** drop-down box. If they are, then they were successfully compiled and you can 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, see ["Troubleshooting MIB Compilation" on page 610](#).

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **SNMP Browser Tool** is available when configuring this monitor to verify the connection properties of an SNMP agent and to gain more information about the MIBs which that agent implements (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Browser Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

SNMP by MIB Monitor Settings

User interface elements are described below:

UI Element	Description
SNMP Settings	
Server	Name of the server you want to monitor.
Port	Port to use when requesting data from the SNMP agent. Default value: 161
MIB File	<p>MIB file that contains the objects you want to monitor.</p> <p>If you select a specific MIB file, then only the objects described in that MIB file are displayed.</p> <p>If you select All MIBs, then all objects retrieved from the agent during a MIB traversal are displayed.</p> <p>If no MIB information is available for an object, it is still displayed but with no textual name or description.</p> <p>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.</p> Default value: All MIBs
Counter calculation mode	<p>Performs a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are:</p> <ul style="list-style-type: none">• Calculate delta. Calculates a simple delta of the current value from the previous value.• Calculate rate Calculates a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements.• Do not calculate. No calculation is performed. <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> Default value: Do not calculate

UI Element	Description
Starting OID	<p>Use 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 here.</p> <p>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 enter a different value.</p> <p>Default value: 1</p> <p>Note: This field is available in template mode only.</p>
SNMP Connection Settings	
Timeout (seconds)	<p>Amount of time, in seconds, that SiteScope should wait for an SNMP request.</p> <p>Default value: 5 seconds</p>
Retries	<p>Number of SNMP request retries before SiteScope considers the monitor to have failed.</p> <p>Default value: 1</p>
SNMP version	<p>Version of SNMP to use when connecting. SiteScope supports SNMP version 1, version 2, and version 3. Selecting V3 enables you to enter version 3 settings in the fields below.</p> <p>Default value: V1</p>
Authentication type	<p>Type of authentication to use for version 3 connections.</p> <p>Default value: MD5</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
User name	<p>User name for version 3 connections.</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
Authentication password	<p>Authentication password to use for version 3 connections.</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
Privacy type	<p>The privacy protocol used for authentication for SNMP version 3 (DES, 128-Bit AES, 192-Bit AES, 256-Bit AES). Leave blank if you do not want privacy.</p> <p>Default value: DES</p> <p>Note: This field is available only if SNMP V3 is selected.</p>

UI Element	Description
Privacy password	<p>Privacy password for version 3 connections. Leave blank if you do not want privacy.</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
Context name	<p>Context Name to use for this connection. This is applicable for SNMP V3 only.</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
Context engine ID	<p>Hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.</p> <p>Note: This field is available only if SNMP V3 is selected.</p>
SNMP Counters	
Counters	<p>Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p>Note:</p> <ul style="list-style-type: none"> • At first, only the MIB tree is loaded. You should choose the required MIB node you want to monitor, and right-click it to load counters from the remote device. • The counters displayed are those received during the timeout period, and may not include all the counters available on the server. Specifying a longer timeout in the Timeout (seconds) field in the SNMP Connection Settings panel may result in receiving more counters. • The total time for receiving the counters may be longer than the timeout specified, due to additional processing time not part of the request/response period. <p>Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Tips

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Troubleshooting MIB Compilation

If MIBs are not listed in the **MIB file** drop-down box after adding MIB files to the **templates.mib** directory, perform the following MIB Compilation troubleshooting steps:

1. Open **<SiteScope root directory>\logs\RunMonitor.log** and look for MIB compilation error messages close to 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.
2. Correct the errors found in **RunMonitor.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 **RunMonitor.log**. There is a lot of information about these errors on the Web.
3. After correcting the errors described in **RunMonitor.log**, restart SiteScope.
4. Follow the procedures in step 1 of "[How to Configure the SNMP by MIB Monitor](#)" on page 606 to verify that the new MIB files compiled correctly.

Chapter 84

SNMP Trap 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.

Note: To have SiteScope query a specific device for a specific value, use the SNMP monitor.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SNMP Trap monitor.

Learn More

This section includes:

- "Supported Platforms/Versions" below
- "IPv6 Addressing Supported Protocols" below

Supported Platforms/Versions

The monitor supports monitoring traps of SNMP versions 1, 2, and 3.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Tasks

How to Configure the SNMP Trap Monitor

1. Prerequisites

You 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.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **SNMP Trap Tool** is available when configuring this monitor to view SNMP Traps received by SiteScope's SNMP listener (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Trap Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

SNMP Trap Monitor Settings

User interface elements are described below:

UI Element	Description
<p>Content match</p>	<p>Text to look for in SNMP Traps. Regular expressions may also be used for pattern matching. By default, all SNMP traps received are matched.</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>
<p>Match value labels</p>	<p>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>

UI Element	Description
Run alerts	<p>Method for running alerts:</p> <ul style="list-style-type: none">• For each SNMP Trap matched. The monitor triggers alerts for every matching entry found. When the SNMP Trap monitor is run for each SNMP Trap received, 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.• Once, after all SNMP Traps have been checked. 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 Settings section. <p>Default value: For each SNMP Trap matched</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

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.

Chapter 85

Solaris Zones Monitor

The Solaris Zones monitor enables you to monitor the physical host, its zones, and their resource pools on Solaris servers.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Solaris Zones monitor.

Learn More

This section includes:

- ["Solaris Zones Topology" below](#)
- ["Virtualization Support" below](#)
- ["Solaris Zones Topology" below](#)

Solaris Zones Monitor Overview

Use the Solaris Zones monitor to show statistics on the physical host, its zones, and their resource pools on Solaris servers. This monitor can help you recognize problems in the Solaris system, and isolate them in the zone or resource pool level. The Solaris Zones monitor supports monitoring machines that are running on Solaris 10 update 7 (5/09) operating systems.

The Solaris Zones monitor queries the list of UNIX servers currently configured in the UNIX Remote Servers container. To monitor a remote Solaris Zones server, you must define a UNIX Remote connection profile for the server before you can add a Solaris Zones monitor for that server. For details, see Remote Servers Overview in the Using SiteScope Guide.

For details on how to analyze Solaris zones monitor results, see ["How to Analyze Solaris Zones Monitor Results – Use-Case Scenario"](#) on page 620.

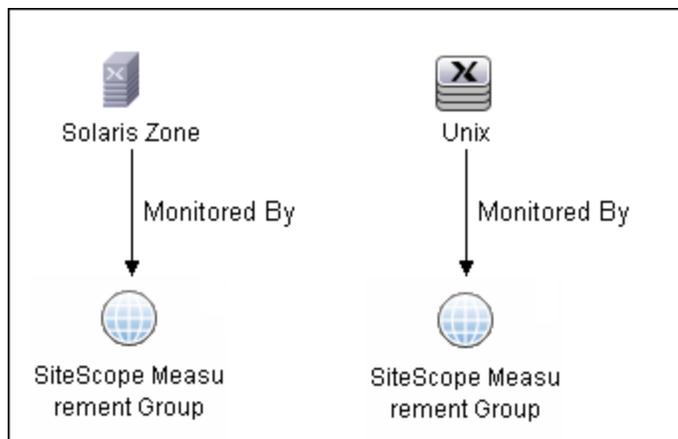
Virtualization Support

A Solaris zone is a virtualized operating system environment created within a single instance of the Solaris Operating System. It provides the required isolation and security to run multiple applications of the same operating system on the same server.

Note: Branded zones that are not of Solaris type are not supported.

Solaris Zones Topology

The Solaris Zones monitor can identify the topology of the Solaris system being monitored. If **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting), the monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM as SiteScope Measurement Groups CIs and the counters in it as SiteScope Measurement CIs. SiteScope Measurement CIs that refer to the physical host or global zone are linked to a UNIX host CI that represents the machine. SiteScope Measurement CIs that refer to a non-global zone are linked to a UNIX host CI that represents the zone. SiteScope can also report other measurements that are not connected to the host CIs. These can include pool measurements and counters in error.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

Tasks

This section includes:

- "How to Configure the Solaris Zones Monitor" below
- "How to Analyze Solaris Zones Monitor Results – Use-Case Scenario" below

How to Configure the Solaris Zones Monitor

1. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

2. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "Solaris Zones Topology" on page 618.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

How to Analyze Solaris Zones Monitor Results – Use-Case Scenario

This use-case scenario describes how the Solaris Zones monitor can be used to diagnose problems on the physical host, and in the zone and resource pool level.

- **Background**

Bob, the SiteScope administrator for ABC Company, configures the Solaris Zones monitor to monitor the company's Solaris system that comprises of four zones, two CPUs, and 4GB RAM.

- **High CPU load in zone1**

Bob notices that the physical host counters show CPU consumption of 51%, of which, according to `zone1` counters, `zone1` uses 50% of the machine's total CPU (no resource pools are used, so both CPUs can be used by each zone).

Now that Bob knows that the problem is with `zone1`, he can further investigate this zone.

- **High CPU load and memory consumption**

The Solaris Zones monitor's physical host counters show that there is high CPU and memory consumption and excessive paging. After examining the counters results for each of the four zones, Bob discovers that `zone2` consumes 2 GB of virtual memory.

Now that Bob knows that the problem is with `zone2`, he can further investigate this zone.

- **High CPU load in a resource pool**

In this scenario, `zone1` and `zone2` use `ResourcePool1` that contains one CPU, while all the other zones use the default pool that has the other CPU. Bob is alerted by the Solaris Zones monitor to the following:

- High CPU usage (100%) in `ResourcePool1`.
- The physical host counters in the Solaris Zones show CPU consumption of 51%.

- `zone1` consumes 49-50% of the total machine CPU, while `zone2` consumes only 0.4% (both of these zones use `ResourcePool1`).

Bob realizes that there is a problem with the existing resource allocation. Possible actions include:

- Assigning more CPU to `zone1`.
- Associating `zone2` to the default pool to reduce the effect of poor performance from `zone1`.
- Stopping `zone1` until the reason for the high CPU usage is found.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Solaris Zones Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of server that you want to monitor. Select a server from the server list (only the UNIX remote servers that have been configured in SiteScope are displayed), or use the Add Remote Servers button to add a Solaris server.</p> <p>Note when working in template mode:</p> <ul style="list-style-type: none">You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.There is a Server to get measurements from box with the list of UNIX servers from which you can select the server from which to get measurements.
Add Remote Server	<p>Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
Counters	<p>Displays the server performance counters you want to check with this monitor. You can select counters on the physical host, its zones, and the resource pools used by the host. Use the Get Counters button to select counters.</p> <p>Note: When configuring this monitor in template mode, you can use regular expressions to define counters.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Tips

- The monitor collects measurements for the zones that are in **Running** state only.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Notes and Limitations

- The monitor collects measurements for counters of running zones only. If a zone that was running is stopped or deleted, when the monitor next runs, the counters of this zone that were selected show *n/a* and the state string indicates that the zone is not running.
- When defining a Solaris remote server (by selecting Sun Solaris as the operating system), it does not necessarily mean that you can run special zone commands. To verify that zones are supported, run the **zoneadm** command, and check the output list contains the word **global** (this is the default zone that exists in any machine that supports zones). If it does not, the operating system does not support zones.
- A Solaris Zones monitor should be defined on a Solaris machine that supports Solaris Zones. The remote server should be defined on the machine itself (the global zone), and not on one of the machine's non-global zones. If the monitor is defined on a remote server that does not support zones, SiteScope identifies it by the output of the **zoneadm list** command. The output on operating systems that support zones always includes the global zone. If the global zone is not part of the command output (where the command is not supported), SiteScope displays the following error message: "The operating system does not support Solaris Zones".

Note: If the server goes down while running the **zoneadm** command, all the zones go down with it, and the server might be identified as a version that does not support zones.

- Some of the commands use **zlogin** to resolve the zone's data. Since this command can be used only by the global administrator operating in the global zone, you need to define your remote server with the global administrator user when selecting the zone's counters.
- While pool counters show all pools displayed by the **poolstat** command (including temporary pools), the **%usageOfPoolCpu** counter refers only to the pool defined for the zone in the **zonecfg** command, and does not include temporary dynamic pools. Where temporary pools are used, for example, by defining a **dedicated-cpu** resource for the zone, this counter does not reflect the real state.
- The **%usageOfPoolCpu** counter also takes account of the size of the pools, and assumes that pool size does not change during the monitor run.
- All counters that refer to pools, including all counters under the **Resource Pool** category and the **%usageOfPoolCpu** counter, show *n/a* if the pool facility is not active.
- Processes in the global zone can be bound to a pool used by another zone through a project. In this situation, the **%usageOfPoolCpu** counter (which takes into account only the pool configured to the zone in **zonecfg**), does not reflect the CPU usage out of all CPU power allocated to this zone's processes, since the potential CPU power available for the zone comes

not only from its pool, but also from the other pools that its processes use.

- The **mbSize** zone counter has the same value in the SIZE and SWAP columns in the **prstat -Z** command output. In some versions of Solaris 10, the column is called SIZE and refers to the total address space size of all processes. In some later versions, the column is called SWAP and refers to the total swap (virtual memory) reserved by the zone's processes.
- If you create a Solaris Zones monitor and click **Save** (instead of **Verify & Save**), only a partial topology is reported to BSM. This topology includes the CIs of the measurements and measurement groups and the host CI of the machine itself (if some of its measurements were selected). The topology does not include the host CIs that represent the zones, since when saving only, no connection is made to the remote server to collect data that it has not already been collected (such as the zone's names in the network). These missing CIs are reported either:
 - If you make a change to the monitor, and click **Verify & Save**.
 - According to the **Topology resolving frequency (minutes)** value that is defined in **Preferences > Infrastructure Preferences > General Settings**. This is the amount of time, in minutes, to wait between checking the topology of the server being monitored (the default time is 120 minutes). If this time is exceeded during a monitor run, the monitor connects to the server to collect topology data (the zone's names in the network). If the data has changed or has not yet been reported, the monitor is put in the queue for reporting data. Since the queue is checked every hour, the monitor reports the topology again after a maximum of three hours since the time that the topology changed.

Chapter 86

SunONE Web Server Monitor

This monitor enables you to monitor the availability of SunONE or iPlanet 6.x and 7.0 servers using the stats-xml performance metrics file (iwsstats.xml or nesstats.xml) facility.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SunONE Web Server monitor.

Learn More

SunONE Web Server Monitor Overview

Use the SunONE Web Server monitor to monitor performance metrics reported in the stats-xml file of SunONE or iPlanet 6.x servers. 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.

You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SunONE server you are running. Error and warning thresholds for the monitor can be set on one or more SunONE server performance statistics or HTTP response codes.

Tasks

How to Configure the SunONE Web Server Monitor

1. Prerequisites

Before you can use the SunONE Web 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 take effect.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

SunONE Web Server Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Stats-XML URL	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	User name of the SunONE server you want to monitor.
Authorization password	Password of the SunONE server you want to monitor.
HTTP proxy	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the server.
Proxy server user name	Proxy server user name if the proxy server requires a name and password to access the server. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Proxy server password	Proxy server password if the proxy server requires a name and password to access the server.
Timeout (seconds)	Amount of time, in seconds, to 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. Default value: 60 seconds 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 time to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.
Counter Settings	
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.

UI Element	Description
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 87

Sybase Monitor

The Sybase monitor enables you to monitor the availability and performance statistics of a Sybase Server. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning.

Create a separate monitor instance for each Sybase server in your environment. The error and warning thresholds for the monitor can be set on one or more Sybase server performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Sybase monitor.

Learn More

Supported Platforms/Versions

- This monitor supports monitoring the server performance data for Sybase 11.0, 11.5, 11.92, 12.x, and 15.5 database servers.
- This monitor is supported in SiteScopes that are running on Windows versions only.
- This monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.

Tasks

How to Configure the Sybase Monitor

1. Prerequisites

- Before you can use the Sybase monitor, you have to configure the Sybase server environment. The Sybase monitor connects to the Sybase Adaptive Server Enterprise (ASE) server by using the ASE Monitor Server and retrieves metrics from the server using Sybase-provided libraries. When connecting to the monitored server, you connect to the ASE Monitor Server, not the Sybase server. The ASE Monitor Server is an application that runs on the same machine as Sybase server and retrieves performance information from the Sybase server. The ASE 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 ASE Monitor Server for that server would be `back-endddb_ms`.
- Make sure that your ASE Monitor Server has all EBF updates and works correctly. To download the updates, log on to the Sybase web site, and in the **Support** menu, select **EBFs/Update > EBFs/Maintenance > Adaptive Server Enterprise**. (A Sybase account is required to access this page.)
- You also have to install the Sybase Central client on the machine where SiteScope is running to connect to the ASE 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. Copy the content of the `sql.ini` file located in **<System Root>\SYBASE\INI** on the Sybase server into the `sql.ini` file on the SiteScope server. You can use the `dsedit` tool in the Sybase client console to test connectivity with the ASE Monitor Server.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Sybase Monitor Settings

User interface elements are described below:

UI Element	Description
Server	Name of the server you want to monitor. Usually it is the name of the server followed by <code>_MS</code> .
User name	User name to access the Sybase database.
Password	Password of the user name to access the Sybase database.
Counters	Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 88

Syslog Monitor

Use this monitor to check for specific entries added to a log file on a UNIX or Linux environment by looking for entries containing a text phrase or a regular expression.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Syslog monitor.

Learn More

This section includes:

- ["Syslog Monitor Overview" below](#)
- ["Support for IPv6" below](#)

Syslog Monitor Overview

The Syslog monitor is used for monitoring Syslog processes and messages from UNIX and Linux remote servers. It watches for specific entries containing a text phrase or a regular expression in log files that were determined in the **syslog.conf** (**rsyslog.conf**) file. All UNIX and Linux systems supported by SiteScope are POSIX-compliant (partially or fully), and all of them use syslog for logging various system events.

You can use the monitor 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 641](#).

Support for IPv6

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the SSH protocol is supported.

For details on using IPv6, see [Support for IP Version 6 in Using SiteScope](#).

Tasks

This section includes:

- "How to Configure the Syslog Monitor" below
- "Customizing Syslog Content Matches and Monitor Alerts" below

How to Configure the Syslog Monitor

1. Prerequisites

The following configuration requirements must be performed or verified before the Syslog monitor can be used:

- The remote server should be created with credentials that grant read access on the monitored file.
- The **rsyslog.conf** file on the remote machine must be backward compatible with the **syslog.conf** file.
- The **syslog.conf** (**rsyslog.conf**) file must exist and be accessible under credentials used for connecting to the remote server, or under which SiteScope is running (if monitoring a local file).
- The path to **syslog.conf** (**rsyslog.conf**) can be determined for each operating system in the **<SiteScope root directory>\templates.os** folder in the syslog section.
- SiteScope is unable to execute a command with more than 80 characters on a remote UNIX server via a Telnet connection (the "unable to read log file" message is displayed in the monitor summary). To avoid this issue, increase the COLUMNS variable in the UNIX shell script that customized the shell environment (for bash this is `.bashrc`).

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Customizing Syslog Content Matches and Monitor Alerts

You can create a Syslog monitor that triggers customized alerts for content matches according to the threshold status of the monitor.

To configure the Syslog monitor with custom matches and alerts:

1. In the Syslog Monitor Settings, configure the following settings:
 - **Run alerts:** Select the **For each log entry matched** option.
 - **Process match** and **Message match:** Enter the text to look for in the log entries. For example, to find text entries `redflag` and `disaster` in the log file, enter `(redflag|disaster)/`. The test string from both of these fields is combined in one regular expression, which is displayed in the **Regular expression preview** box. You can determine how the strings are combined in the **_sysLogMatchRegExp** property in the **<SiteScope root directory>\master.config** file.
2. Configure error, warning, and good alerts for the Syslog 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,

Monitor Reference

Chapter 88: Syslog Monitor

the error alert is triggered. For details on configuring alerts, see [How to Configure an Alert in the Using SiteScope Guide](#).

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Syslog Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Server	<p>Server where the file you want to monitor is located. Select a server from the server list (only UNIX remote servers that have been configured in SiteScope and the local SiteScope machine are displayed), or click Add Remote Server to add a new UNIX server.</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p>
Log file path	<p>Path to the log file from which you want to extract data. Lists log files from syslog.conf with information of messages stored in that log.</p> <p>Examples:</p> <ul style="list-style-type: none">• /var/log/messages (*.info;mail.none;authpriv.none;cron.none)• /var/log/secure (authpriv.*)• /var/log/maillog (mail.*)
Add Remote Server	<p>Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
Run alerts	<p>Method for running alerts for this monitor.</p> <ul style="list-style-type: none"> • For each log entry matched. The monitor triggers alerts according to thresholds applied to each matching entry found. Since status can change according to thresholds for each matched entry, each alert action could be triggered many times within a monitor run. Syslog can write repetitive entries as "last message repeated N times" instead of writing identical messages to the log file (this does not work for Server-side processing). <p>Example: If you want to send a warning alert on matched text value "power off" and an error alert if more than one server is turned off, set the following thresholds:</p> <ul style="list-style-type: none"> ▪ <code>Error if matchCount > 1</code> ▪ <code>Warning if value == 'power off'</code> <p>To send an error alert if only one threshold is matched, set <code>Error if value == 'power off'</code>.</p> <p>For details on how to create a Syslog monitor that triggers customized alerts for content matches, see "Customizing Syslog Content Matches and Monitor Alerts" on page 638.</p> <ul style="list-style-type: none"> • Once, after all log entries have been checked. 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>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>
Process match	<p>Expression describing the process to match in the log entries. You can also use a regular expression in this entry to match text patterns. The message entered here is displayed in the Regular expression preview box</p> <p>Note: If you enter more than 10 values for process or match messages, when you create a report by clicking the monitor title, the report includes only the first 10 values.</p>

UI Element	Description
Open Tool	Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.
Message match	<p>Expression describing the message to match in the log entries. You can also use a regular expression in this entry to match text patterns. The message entered here is displayed in the Regular expression preview box.</p> <p>Note:</p> <ul style="list-style-type: none"> • The search is case sensitive. • If you enter more than 10 values for process or match messages, when you create a report by clicking the monitor title, the report includes only the first 10 values.
Regular expression preview	<p>Displays a preview of the regular expression text match to run which includes the text from the Process match and Message match boxes above.</p> <p>The Syslog monitor process and message 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.</p>
Advanced Settings	
Log file encoding	<p>If the log file content to be monitored uses an encoding that is different than the encoding used on the server where SiteScope is running, select 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>Default value: windows-1252</p>
Match value labels	<p>Use to enter 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 (,).</p> <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> <p>Note: If you enter more than four match value labels, when you create a report by clicking the monitor title, the report includes only the first four values.</p>

UI Element	Description
<p>Server-side processing</p>	<p>Processes log file data on the server-side. Benefits include low memory usage and low CPU utilization on the SiteScope server, and faster monitor run. Server-side processing does however cause high CPU utilization on the remote server when processing the file.</p> <p>Default value: Not selected (we recommend using this option only if SiteScope performance is affected by large amounts of data being appended to the target log file between monitor runs, and the Syslog monitor is performing badly in regular mode).</p> <p>Note:</p> <ul style="list-style-type: none"> • The encoding for the remote server must be Unicode, or match the encoding of the log file (if the remote file is in Unicode charset). • To enable server-side processing to work correctly when monitoring on a Solaris server, open the remote server settings for the monitored host (Remote Servers > UNIX Remote Servers > Main Settings), and enter a path to the bash interpreter in the Initialize shell environment field.
<p>No error if file not found</p>	<p>Monitor remains in Good status if the file is not found. The monitor status remains Good regardless of the monitor threshold configuration.</p> <p>Default value: Not selected</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- When monitoring a log file on a FreeBSD remote server, make sure the correct path to the "cat" command is used in **<SiteScope root directory>\templates.os/FreeBSD.config**, since the command was moved in the latest FreeBSD versions.
- SiteScope is unable to execute a command with more than 80 characters on a remote UNIX server via a Telnet connection (the "unable to read log file" message is displayed in the Syslog monitor summary). To avoid this issue, increase the COLUMNS variable in the UNIX shell script that is used to customize the shell environment (for bash this is .bashrc).
- When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the **Browse Servers** and **Add Remote Server** buttons are not displayed.

Chapter 89

Tuxedo Monitor

Use the Tuxedo monitor to monitor the server performance data for Tuxedo servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning.

Create a separate monitor instance for each Tuxedo server in your environment. The error and warning thresholds for the monitor can be set on one or more Tuxedo monitor performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Tuxedo monitor.

Learn More

Supported Platforms/Versions

- This monitor supports monitoring server performance data for Oracle Tuxedo 6.5, 7.1, 8.0, 8.1, 9.0, and 9.1 servers.
- This monitor is supported in SiteScopes that are running on Windows versions only. However, this monitor can monitor remote servers running on any platform/operating system.
- This monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.

Tasks

How to Configure the Tuxedo Monitor

1. Prerequisites

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.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Tuxedo Monitor Settings

User interface elements are described below:

UI Element	Description
Basic Tuxedo Settings	
Server	Name or IP address of the server. The address should match that dedicated to the Tuxedo Workstation component (the WSL process). On UNIX servers, enter the full path of the applicable server.
Port	Port number for the Tuxedo server. The port number should match the port dedicated to the Tuxedo Workstation component (the WSL process).
User name	User name if required to access the Tuxedo server.
Password	Password if required to access the Tuxedo server.
Advanced Tuxedo Settings	
Client name	Optional client name for the Tuxedo server.
Connection data	Any extra or optional connection data to be used for connecting to the Tuxedo server. In some cases, this may be a hexadecimal number.
Tuxedo Counters	
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 90

UDDI Monitor

Use the UDDI monitor to check the availability and round-trip response time of the UDDI 2.0 server. Each time that the monitor is run, SiteScope checks if the UDDI Server can find a business entity. The administrator of the UDDI server can limit or disable this monitor.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the UDDI monitor.

Tasks

How to Configure the UDDI Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

UDDI Monitor Settings

User interface elements are described below:

UI Element	Description
Inquiry URL	UDDI server inquiry URL. Example: <code>http://uddi.company.com/inquiry/</code>
Business name	Business entity to search for in the UDDI server.
Maximum number of businesses	Maximum number of business entities to receive from the UDDI server (1–200). Default value: 10

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 91

UNIX Resources Monitor

The UNIX Resources monitor enables you to monitor multiple system statistics on a single UNIX system.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the UNIX Resources monitor.

Learn More

This section includes:

- "UNIX Resources Monitor Overview" below
- "Supported Versions" below
- "IPv6 Addressing Supported Protocols" below
- "Server-Centric Report" on the next page

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 enables you to monitor the remote server for loading, performance, and availability at a basic system level. Create a separate UNIX Resources monitor instance for each UNIX server in your environment. The error and warning thresholds for the monitor can be set on one or more server system statistics.

The UNIX Resources monitor queries the list of UNIX servers currently configured in the UNIX Remote Servers container.

Supported Versions

This monitor supports monitoring UNIX remote servers running on:

- Solaris 2.7, 2.8, 2.9, 5.10, 7, 8, 9, 10, 10u8-11
- Red Hat Linux 7.x, 8.x, 9.x, and Red Hat Linux AS/ES Linux 3.x, 4.x, 5.2, 5.4, 5.5, 5.8, 6.0, 6.1
- HP-UX 11iv1 (B.11.11) on HP 9000 series:
 - HP-UX B.11.11 U 9000/800 4030070275 unlimited-user license
 - HP-UX B.11.31 U ia64 4005705783 unlimited-user license
 - HP-UX 11i v3
- AIX 5.2, 5.3, 6.1, 7.0

Note: The UNIX Resources monitor does not support monitoring remote servers running on HP NonStop operating systems. You should use the "HP NonStop Resources Monitor" on page 280 instead.

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SSH protocol only.

Note: SSH is supported only when SiteScope is installed on UNIX machines.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Server-Centric Report

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 the SiteScope Dashboard. For details, see Server-Centric Report in the Using SiteScope Guide.

Tasks

How to Configure the UNIX Resources Monitor

1. Prerequisites

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 Remote Servers Overview in the Using SiteScope Guide.

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

UNIX Resources Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server that you want to monitor. Select a server from the server list (only those UNIX remote servers that have been configured in SiteScope are displayed), or click the Add Remote Servers button to add a UNIX server.</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p>
Server to get measurements from	(Available in template mode only) Name of any SiteScope remote server from which you want to get counters.
Add Remote Server	Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.
Available Counters	<p>Displays the available measurements for this monitor.</p> <p>For each measurement, select the Object, Instances and Counters you want to check with the UNIX Resources monitor, and click the Add Selected Counters  button. The selected measurements are moved to the Selected Counters list.</p> <p>Note: The Disk Stat counter is available only when monitoring remote servers running on Linux version 2.4. This is because the <code>/proc/stat</code> command, which retrieves relevant disk stat information, is available for this version only.</p>
Selected Counters	<p>Displays the measurements currently selected for this monitor, and the total number of selected counters.</p> <p>To remove measurements selected for monitoring, select the required measurements, and click the Remove Selected Counters  button. The measurements are moved to the Available Counters list.</p>
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 Server-Centric Report in the Using SiteScope Guide.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- When configuring this monitor in template mode, you can use regular expressions to define counters.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 92

URL Monitor

This monitor provides 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the URL monitor.

Learn More

This section includes:

- "URL Monitor Overview" below
- "Supported Platforms/Versions" below
- "What to Monitor" below
- "Status" on the next page
- "Scheduling the Monitor" on the next page
- "Support for IPv6 Addresses" on page 662
- "SSL Connectivity" on page 662

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 HTTP Settings pane.

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 enables you to verify that the contents of the page are correct.

Supported Platforms/Versions

The URL monitor supports monitoring HTTP versions 1.0 and 1.1.

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 use 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.

Status

Each time the URL monitor runs, it returns a reading and a 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, email 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 in the SiteScope Dashboard. 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 good.

Scheduling the 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.

Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP and HTTPS protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

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 either:

- Selecting the **Accept untrusted certificates for HTTPS** option in the Authentication Settings section of the Monitor Settings panel as described in "URL Monitor" on page 659.
- Importing the server certificate. For details on how to perform this task, see "How to configure the URL monitor" on the next page.

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol\Client	Java	WinInet
SSLv2	x	x
SSLv3	x	√
TLSv1	√	√

Tasks

This section includes:

- ["How to configure the URL monitor" below](#)
- ["How to manually import server certificates " below](#)

How to configure the URL monitor

1. Prerequisites

The user name and password specified in the **Credentials** section (in **Authentication Settings**) must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.

2. Import the server certificates (if the Web Server is configured to use SSL encryption)

If the Web server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate. Use one of the following methods for importing server certificates:

- Import the server certificates using SiteScope Certificate Management. For details, see [How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide](#).
- Import the server certificates manually. For details, see ["How to manually import server certificates " below](#).

3. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip:

- The **Get URL Tool** is available when configuring this monitor to request a URL from a server, print the returned data, and test network routing (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see [URL Tool in the Using SiteScope Guide](#).
- You can use the **URL Sequence Tool** to get on the spot data for the URL and to view the HTML received from the HTTP request.

How to manually import server certificates

Instead of using Certificate Management, you can manually import certificates using the keytool method, if preferred. Certificates imported this way can still be managed using Certificate Management. For details on Certificate Management, see [Certificate Management in the Using SiteScope Guide](#).

1. Check the certificates already in the keystore, from the **<SiteScope root directory>\javalib\security** directory, by entering:

```
../../bin/keytool -list -keystore cacerts
```

2. Import the certificate, into **<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 **cacerts** file.

Note: The default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Therefore, you should create a copy of the **cacerts** file with a different name before SiteScope is upgraded or re-installed so that the file is not overwritten when new certificates are imported.

3. In SiteScope, select **Preferences > Certificate Management**, and click the **Reload Certificate List** button to reload the keystore certificates from the **cacerts** file. This enables you to manually reload keystore changes without having to restart SiteScope.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

URL Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
URL	<p>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>Text string to match in the returned page or frameset.</p> <p>If the text is not contained in the page, the monitor displays the message <code>content match error</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.</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 <code>i</code> 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>Note: The search is case sensitive.</p>
Open Tool	<p>Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.</p>

UI Element	Description
Match content for error	<p>Text string to check for in the returned page or frameset. 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: <code>< B> Error < /B> Message</code></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 indicating case-insensitive matching.</p> <p>Example: <code>/href=Doc\d+\.html/</code> or <code>/href=doc\d+\.html/i</code></p> <p>Note:</p> <ul style="list-style-type: none">• The search is case sensitive.• You can click the Open Tool button to use the Regular Expression Test tool to check your regular expressions. For details, see Regular Expression Tool in the Using SiteScope Guide.
Show detailed measurement	<p>Records a detailed breakdown of the process times involved in retrieving the requested URL.</p> <p>These measurements 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.
Timeout (seconds)	<p>Amount of time, in seconds, to 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 selected the Retrieve images or Retrieve frames option, SiteScope waits for these items to be retrieved before considering the page to be fully downloaded.</p> <p>Default value: 60 seconds</p>
Retries	<p>Number of times (between 0-10) that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request is a recoverable error.</p> <p>Default value: 0</p>

UI Element	Description
HTTP Settings	
Request headers	<p>Header request lines sent by the HTTP client to the server. Headers should be linebreak separated. The standard list of HTTP1.1 request headers can be found in http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.</p> <p>Note: Although this field is optional, some Web pages behave unexpectedly when the request header is missing (such as performing endless redirects, providing wrong content, and so forth).</p>
URL content encoding	<p>SiteScope retrieves the correct encoding from the server response. The default value appearing here should not be edited.</p> <p>Default value: Retrieve encoding from server response</p>
POST data	<p>If the URL is for a POST request, enter the post variables, one per line as <code>name=value</code> 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 <code>Set-cookie: cookieName=cookieValue</code>.</p> <p>To change the content type of a post, use the format <code>Content-Type: application/my-format</code>.</p> <p>To substitute values in the POST data, add a line to the master.config file, such as:</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>
POST data encoding	<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 <code>urlencoded</code> then encode, otherwise do not encode. • Force URL encoding. Always encode the post data. • Do not force URL encoding. Do not encode the POST data.

UI Element	Description
<p>Check for content changes</p>	<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 goes 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: No content checking</p>
<p>Error if redirected</p>	<p>Generates an error (and notifies you) if a URL is redirected.</p> <p>Default value: Not selected</p>
<p>HTTP version</p>	<p>HTTP version for SiteScope to use for style request headers (HTTP version 1.1 or 1.0).</p> <p>Default value: 1.1</p>
<p>Retrieve images</p>	<p>The status and response time statistics include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by <code>IMG</code>, <code>BODY</code> (from the background property), and <code>INPUT TYPE=IMAGE</code> 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> <p>Default value: Not selected</p>

UI Element	Description
Retrieve frames	<p>Retrieves the frames references in a frameset and counts their retrieval time in the total time to download this page. Frames include those referenced by <code>FRAME</code> and <code>IFRAME</code> 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> <p>Default value: Not selected</p>
Use WinInet	<p>WinInet is used as an alternative HTTP client for this monitor.</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>Default value: Not selected</p>
Proxy Settings	
HTTP proxy	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URL.
Proxy server user name	<p>Proxy server user name if the proxy server requires a user name to access the URL.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Proxy server password	<p>Proxy serverpassword if the proxy server requires a user name to access the URL.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Proxy NTLM V2	Select if the proxy requires authentication using NTLM version 2.
Authentication Settings	

UI Element	Description
Credentials	<p>Option to use for authorizing credentials if the URL specified requires a name and password for access:</p> <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password to access the URL in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password for the URL (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Pre-emptive authorization	<p>Option for sending authorization credentials if SiteScope requests the target URL:</p> <ul style="list-style-type: none"> • Use global preference. Select to have SiteScope use the setting specified in the Pre-emptive 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. <p>Note: If the URL does not require a user name and password, this option may cause the URL to fail.</p> <ul style="list-style-type: none"> • Authenticate if requested. Select to send the user name and password on the second request if the server requests a user name and password. <p>Note: If the URL does not require a user name and password, this option may be used.</p> <p>All options use the User name and Password entered for this monitor instance. If these are not specified for the individual monitor, the Default authentication user name and Default authentication password specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p>Note: Pre-emptive authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
Client side certificate	<p>The certificate file, if you need to use a client side certificate to access the target URL. Normally, this is a <code>.pfx</code> (<code>.p12</code>) type certificate, which usually requires a password. You enter the password for the certificate in the Client side certificate password box.</p> <p>Note: Client side certificate files must be copied into the <code><SiteScope root directory>\templates.certificates</code> directory.</p>
Client side certificate password	<p>Password if you are using a client side certificate and that certificate requires a password.</p>

UI Element	Description
Authorization NTLM domain	Domain for NT LAN Manager (NTLM) authorization if required to access the URL.
Accept untrusted certificates 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" on page 662 .
Accept invalid certificates for HTTPS	Select 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.
NTLM V2	Select if the URL you are accessing requires authentication using NTLM version 2.

For information on configuring setting panels that are common to all monitors, see [Common Monitor Settings](#) in the [Using SiteScope Guide](#).

Tips/Troubleshooting

General Notes/Limitations

- While the **round trip time** performance counter is measured in milliseconds in the Threshold Settings, it is displayed in seconds in the SiteScope Dashboard.
- When SiteScope is connected to BSM, not all monitor metrics are reported to BSM. If a URL monitor gets its status from a metric that is not reported to BSM and a metric that is reported to BSM (for example, **roundtrip time**) does not have any threshold set in SiteScope, then no monitor status is reported to BSM.
- When setting thresholds for the URL monitor, the **status** condition relates only to HTTP status codes (such as 200, 302, and 404) in the page itself, whereas **overall status** relates to HTTP status codes in the page and in components of the page such as images or frames (provided **Retrieve images** and **Retrieve frames** are selected in the monitor settings).
- When using several URL load threads, the total duration time might be less than the combined total of the DNS lookup, connection, server response, and download time. In this case, total duration time is the duration between the start and end of all threads, whereas DNS lookup, connection, response, and download time is the sum of the corresponding value of each thread. You can set the required count of URL load threads in the **_urlLoadThreads** property in `<SiteScope root directory>\groups\master.config`.

Chapter 93

URL Content Monitor

The URL Content monitor is a specialized variation of the "URL Monitor" on page 659 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the URL Content monitor.

Learn More

This section includes:

- "URL Content Monitor Overview" below
- "Supported Platforms/Versions" below
- "Status" below
- "Support for IPv6 Addresses" on the next page
- "SSL Connectivity" on the next page

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.

Supported Platforms/Versions

The URL Content monitor supports monitoring HTTP versions 1.0 and 1.1.

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 displayed as `good`, `warning`, or `error` in the SiteScope Dashboard dependent on the results of the retrieval, content match, and the error or warning status criteria that you select.

Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP and HTTPS protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

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 either:

- Selecting the **Accept untrusted certificates for HTTPS** option in the Authentication Settings section of the Monitor Settings panel as described in "URL Content Monitor Settings" on page 678.
- Importing the server certificate. For details on how to perform this task, see "How to Configure the URL Content Monitor" on the next page.

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol\Client	Java	WinNet
SSLv2	x	x
SSLv3	x	√
TLSv1	√	√

Tasks

This section includes:

- "How to Configure the URL Content Monitor" below
- "How to Manually Import Server Certificates" below

How to Configure the URL Content Monitor

1. Prerequisites

The user name and password specified in the **Credentials** section (in **Authentication Settings**) must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.

2. Import the server certificates (if the Web Server is configured to use SSL encryption)

If the Web server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate. Use one of the following methods for importing server certificates:

- Import the server certificates using SiteScope Certificate Management. For details, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
- Import the server certificates manually. For details, see "How to Manually Import Server Certificates" below.

3. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **URL Tool** is available when configuring this monitor to request a URL from a server, print the returned data, and test network routing (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see URL Tool in the Using SiteScope Guide.

How to Manually Import Server Certificates

Instead of using Certificate Management, you can import certificates manually using the keytool method, if preferred. Certificates imported this way can still be managed using Certificate Management. For details on Certificate Management, see Certificate Management Overview in the Using SiteScope Guide.

1. Check the certificates already in the keystore, from the **<SiteScope root directory>\javalib\security** directory, by entering:

```
../../../../bin/keytool -list -keystore cacerts
```

2. Import the certificate, into **<SiteScope root directory>\javalib\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 **cacerts** file.

Note: The default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Therefore, you should create a copy of the **cacerts** file with a different name before SiteScope is upgraded or re-installed so that the file is not overwritten when new certificates are imported.

3. In SiteScope, select **Preferences > Certificate Management**, and click the **Reload Certificate List** button to reload the keystore certificates from the **cacerts** file. This enables you to manually reload keystore changes without having to restart SiteScope.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

URL Content Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
URL	<p>URL that you want to monitor.</p> <p>Example:<code>http://demo.thiscompany.com</code></p> <p>If you are monitoring a secure URL, the URL must reflect the correct transfer protocol. The URL starts with <code>https://</code> and the connection is made using SSL.</p> <p>Example:<code>https://demo.thiscompany.com</code></p>
Match content	<p>Expression describing the values to match in the returned page. If the expression is not contained in the page, the monitor displays the message <code>no match on content</code>. A regular expression is used to define the values to match.</p> <p>Use parentheses to enable the monitor to retrieve these values as counters. By using the labels, these counters can be automatically assigned with a customized name and you can define thresholds for them. You can use up to 10 sets of parentheses.</p> <p>Example: The expression <code>/Copyright (\d*)-(\d*)/</code> would match two values, 1996 and 1998, from a page that contained the string <code>Copyright 1996-1998</code>. The returned values (1996 and 1998) could be used when setting Error if or Warning if thresholds.</p>
Open Tool	<p>Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.</p>

UI Element	Description
<p>Match content labels</p>	<p>Labels for the matched values found in the content. The matched value labels are used as variables to access retained values from the content match expression for use with the monitor threshold settings. These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.</p> <p>Example: Type <code>Copyright_start</code>, <code>Copyright_end</code> to represent the copyright date range used in the Match content field. After the monitor runs, these labels are displayed in the Condition list in Threshold Settings, enabling you to set status threshold settings (Error if, Warning if, and Good if) for the matched value. SiteScope also sends the label name of content matches to Generic Data integrations, Diagnostics integrations, and OM metrics integrations.</p> <p>Note:</p> <ul style="list-style-type: none"> • Separate multiple labels with a comma (,). • You can set up to 10 labels.
<p>Match content for error</p>	<p>Text string to check for in the returned page. If the text is contained in the page, the monitor displays <code>content error found</code>. 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: <code>< B> Error < /B> Message</code></p> <p>You can 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 there is no case sensitive matching. Click the Open Tool button to use the Regular Expression Test tool to check your regular expressions. For details, see Regular Expression Tool in the Using SiteScope Guide.</p> <p>Example: <code>/href=Doc\d+\.html/ or /href=doc\d+\.html/i</code></p> <p>Note: The search is case sensitive.</p>
<p>Show detailed measurement</p>	<p>SiteScope records 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.

UI Element	Description
Timeout (seconds)	<p>Amount of time, in seconds, to 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.</p> <p>If you have selected the Retrieve frames or Retrieve images option, SiteScope waits for these items to be retrieved before considering the page to be fully downloaded.</p> <p>Default value: 60 seconds</p>
Retries	<p>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> <p>Default value: 0</p>
HTTP Settings	
Request headers	<p>Header request lines sent by the HTTP client to the server. Headers should be separated by a linebreak. The standard list of HTTP1.1 request headers can be found in http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.</p> <p>Note: Although this field is optional, some Web pages behave unexpectedly when the request header is missing (such as performing endless redirects, providing wrong content, and so forth).</p>
URL content encoding	<p>SiteScope retrieves the correct encoding from the server response. The default value appearing here should not be edited.</p> <p>Default value: Retrieve encoding from server response</p>
POST data	<p>If the URL is for a POST request, enter the post variables, one per line as <code>name=value</code> 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>

UI Element	Description
POST data encoding	<p>Determines if the POST data is to be 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. • Do not force URL encoding. Do not encode the POST data. <p>Default value: Use content type</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.</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: No content checking</p>
HTTP version	<p>HTTP version for SiteScope to use for style request headers (HTTP version 1.0 or 1.1).</p> <p>Default value: 1.1</p>

UI Element	Description
<p>Retrieve images</p>	<p>The status and response time statistics include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by <code>IMG</code>, <code>BODY</code> (from the background property), and <code>INPUT TYPE=IMAGE</code> 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>
<p>Retrieve frames</p>	<p>Retrieves the frames references in a frameset and counts their retrieval time in the total time to download this page. Frames include those referenced by <code>FRAME</code> and <code>IFRAME</code> 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>
<p>Error if redirected</p>	<p>SiteScope notifies you if a URL is redirected.</p>
<p>Use WinInet</p>	<p>WinInet is used as an alternative HTTP client for this monitor.</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>Note: This field is available on Windows versions of SiteScope only.</p>
<p>Authentication Settings</p>	

UI Element	Description
Credentials	<p>Option to use for authorizing credentials if the URL specified requires a name and password for access:</p> <ul style="list-style-type: none"> • Use use name and password. Select this option to manually enter user credentials. Enter the user name and password to access the URL in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password for the URL. Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see <i>How to Configure Credential Preferences</i> in the <i>Using SiteScope Guide</i>.
Pre-emptive authorization	<p>Option for sending authorization credentials 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 Pre-emptive 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. <p>Note: If the URL does not require a user name and password, this option may cause the URL to fail.</p> <ul style="list-style-type: none"> • Authenticate if requested. Select to send the user name and password on the second request if the server requests a user name and password. <p>Note: If the URL does not require a user name and password, this option may be used.</p> <p>All options use the User name and Password entered for this monitor instance. If these are not specified for the individual monitor, the Default authentication user name and Default authentication password specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p>Note: Pre-emptive 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 certificates 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" on page 675.</p>
Accept invalid certificates for HTTPS	<p>Select 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>

UI Element	Description
Client side certificates	<p>Certificate file if you need to use a client side certificate to access the target URL. 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 certificates password	Password for a client side certificate if required.
Authorization NTLM domain	Domain for NT LAN Manager (NTLM) authorization if required to access the URL.
NTLM V2	Select if the URL you are accessing requires authentication using NTLM version 2.
Proxy Settings	
HTTP proxy	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URL.
Proxy server user name	<p>Proxy server user name if required to access the URL.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Proxy server password	<p>Proxy server password if required to access the URL.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Proxy NTLM V2	Proxy requires authentication using NTLM version 2.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- You can use the URL Sequence Tool to get on the spot data for the URL and to view the HTML received from the HTTP request.
- When using several URL load threads, the total duration time might be less than the combined total of the DNS lookup, connection, server response, and download time. In this case, total duration time is the duration between the start and end of all threads, whereas DNS lookup, connection, response, and download time is the sum of the corresponding value of each thread. You can set the required count of URL load threads in the `_urlLoadThreads` property in `<SiteScope root directory>\groups\master.config`.

Chapter 94

URL List Monitor

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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the URL List monitor.

Learn More

This section includes:

- ["URL List Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Scheduling the Monitor" below](#)
- ["Support for IPv6 Addresses" on the next page](#)
- ["SSL Connectivity" on the next page](#)

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" on page 315](#)) or other Web transaction processes (see ["URL Sequence Monitor" on page 695](#)).

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.

Supported Platforms/Versions

The URL List monitor supports monitoring HTTP versions 1.0 and 1.1.

Scheduling the Monitor

This is 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.

The error log marks this as a "skip". If this happens 10 times, SiteScope restarts itself, and SiteScope Health shows an error status. There are several things you can do to try to resolve this issue:

- Schedule the monitor to run less frequently. If this conflicts with some other objective, use the other options.

- Split the URLs that you want to check into more than one list, and add additional monitors to monitor each list.
- 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.

Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP and HTTPS protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

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 importing the server certificate. For details on how to perform this task, see ["How to Configure the URL List Monitor" on the next page](#).

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol\Client	Java	WinInet
SSLv2	x	x
SSLv3	x	√
TLSv1	√	√

Tasks

This section includes:

- "How to Configure the URL List Monitor" below
- "How to import Server Certificates manually"

How to Configure the URL List Monitor

1. Prerequisites

The user name and password specified in the **Credentials** section (in **Authentication Settings**) must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.

2. Import the server certificates (if the Web Server is configured to use SSL encryption)

If the Web server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate. Use one of the following methods for importing server certificates:

- Import the server certificates using SiteScope Certificate Management. For details, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
- Import the server certificates manually. For details, see "How to Manually Import Server Certificates" below.

3. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

How to Manually Import Server Certificates

Instead of using Certificate Management, you can manually import certificates using the `keytool` method, if preferred. Certificates imported this way can still be managed using Certificate Management. For details on Certificate Management, see Certificate Management in the Using SiteScope Guide.

1. Check the certificates already in the keystore, from the **<SiteScope root directory>\javalib\security** directory, by entering:

```
../../bin/keytool -list -keystore cacerts
```

2. Import the certificate, into **<SiteScope root directory>\javalib\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 `cacerts` file.

Note: The default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Therefore, you should create a copy of the **cacerts** file with a different name before SiteScope is upgraded or re-installed so that the file is not overwritten when new certificates are imported.

3. In SiteScope, select **Preferences > Certificate Management**, and click the **Reload Certificate List** button to reload the keystore certificates from the **cacerts** file. This enables you to manually reload keystore changes without having to restart SiteScope.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

URL List Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
URL list file	<p>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. If the URLs are stored in a map format, each URL must be in the format:</p> <pre><URL ID>;<host>;<port>;<secure> or <nonsecure>;<page></pre> <p>Examples:</p> <pre>http://www.website.com/index.html http://www.website.com/main/customer/order.html http://www.website.net/default.htm http://www.Webpages.com/tech/support/ws/intro.html</pre>
Log file	<p>Path for the log file for this monitor. For each URL checked, an entry is added to this log file.</p> <p>If this item is blank, a log is not created.</p>
Error log file	<p>Path for the error log file for this monitor. For each error retrieving a URL, an entry is added to this log file.</p> <p>If this item is blank, a log is not created.</p>
Specific server	<p>Server name of URLs to check in the URL list. If the URLs are stored in a map format (see URL list file box for details), this item is used to check a subset of the URLs from the list.</p> <p>Default value: All URLs that are in the list are checked.</p> <p>Note:If you modify the value in the this box, you must also change the value in the URL list file box for SiteScope to implement the change.</p>
Pause (milliseconds)	<p>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.</p> <p>Default value: 1000 milliseconds</p>
Threads	<p>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.</p> <p>Default value: 4</p>

UI Element	Description
Timeout (seconds)	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. Default value: 60 seconds
Retries	Number of times you want SiteScope to try to reach URLs that are returning an error. Default value: 0
HTTP Settings	
Request headers	Header request lines sent by the HTTP client to the server. Headers should be separated by a linebreak. The standard list of HTTP1.1 request headers can be found in http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14 . Note: Although this field is optional, some Web pages behave unexpectedly when the request header is missing (such as performing endless redirects, providing wrong content, and so forth).
Use WinInet	WinInet is used as an alternative HTTP client for this monitor. Select this option to use WinInet instead of Apache when: <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. Default value: Not selected
Proxy Settings	
HTTP proxy	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URLs in the list.
Proxy server user name	Proxy server user name if the required to access the URL. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Proxy server password	Proxy server password if the required to access the URL. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Authentication Settings	

UI Element	Description
Credentials	<p data-bbox="483 268 1383 331">Option to use for authorizing credentials if the URLs in the list require a user name and password for access:</p> <ul data-bbox="492 352 1375 680" style="list-style-type: none"><li data-bbox="492 352 1375 457">• Use user name and password. Select this option to manually enter user credentials. Enter the user name and password to access the URLs in the User name and Password box.<li data-bbox="492 478 1375 680">• Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password for the URLs (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- You can use the URL Sequence Tool to get on the spot data for the URL and to view the HTML received from the HTTP request.
- When using several URL load threads, the total duration time might be less than the combined total of the DNS lookup, connection, server response, and download time. In this case, total duration time is the duration between the start and end of all threads, whereas DNS lookup, connection, response, and download time is the sum of the corresponding value of each thread. You can set the required count of URL load threads in the `_urlLoadThreads` property in `<SiteScope root directory>\groups\master.config`.

Chapter 95

URL Sequence Monitor

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 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 are not familiar with your application. By using this monitor to perform sequence testing, you can verify that users are able to successfully complete transactions.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **URL Sequence** monitor.

Learn More

This section includes:

- ["URL Sequence Monitor Overview" below](#)
- ["Working with the URL Sequence Monitor" below](#)
- ["Defining Sequence Steps" on the next page](#)
- ["URL Sequences and Dynamic Content" on page 699](#)
- ["Retaining and Passing Values Between Sequence Steps" on page 701](#)
- ["Sharing Cookies Between Monitor Runs and Configured Monitors" on page 702](#)
- ["Support for IPv6 Addresses" on page 703](#)
- ["SSL Connectivity" on page 703](#)

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 URL Sequence monitor supports monitoring HTTP versions 1.0 and 1.1.

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, you can define up to twenty sequence steps. For each step you may specify a content match to search for, enter 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 the SiteScope Dashboard.

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 forty 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 create the monitor.
- You can set thresholds for individual steps or for the whole 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 can be displayed in the following step by clicking the **Show Source** button. 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 707 and Client-side Programs help page.
- You should consider using the VuGen script rather than the URL Sequence monitor in the following circumstances:
 - Where Javascripts are embedded in the HTML being monitored (if they play an important role in the HTML). This is because Javascripts are not supported by the URL monitor.
 - If you experience problems when monitoring HTMLs over the SSL protocol, and these problems persist after you have verified that all monitor settings are correct.

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 enter 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 enables 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.
Selecting a Form button	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. The listings are in the following format: { [formNumber] FormName } ButtonName Example: The <code>Search</code> button on a company's search page might be listed as: { [1]http://www.CompanyName.com/bin/search}search
Selecting a Frame within a frameset	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.
Following a META REFRESH redirection	If the page for this step of the sequence is controlled by a <code><META HTTP-EQUIV="Refresh" CONTENT="timedelay; URL=filename.htm"></code> 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.

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.

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, JSP, 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 box.

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

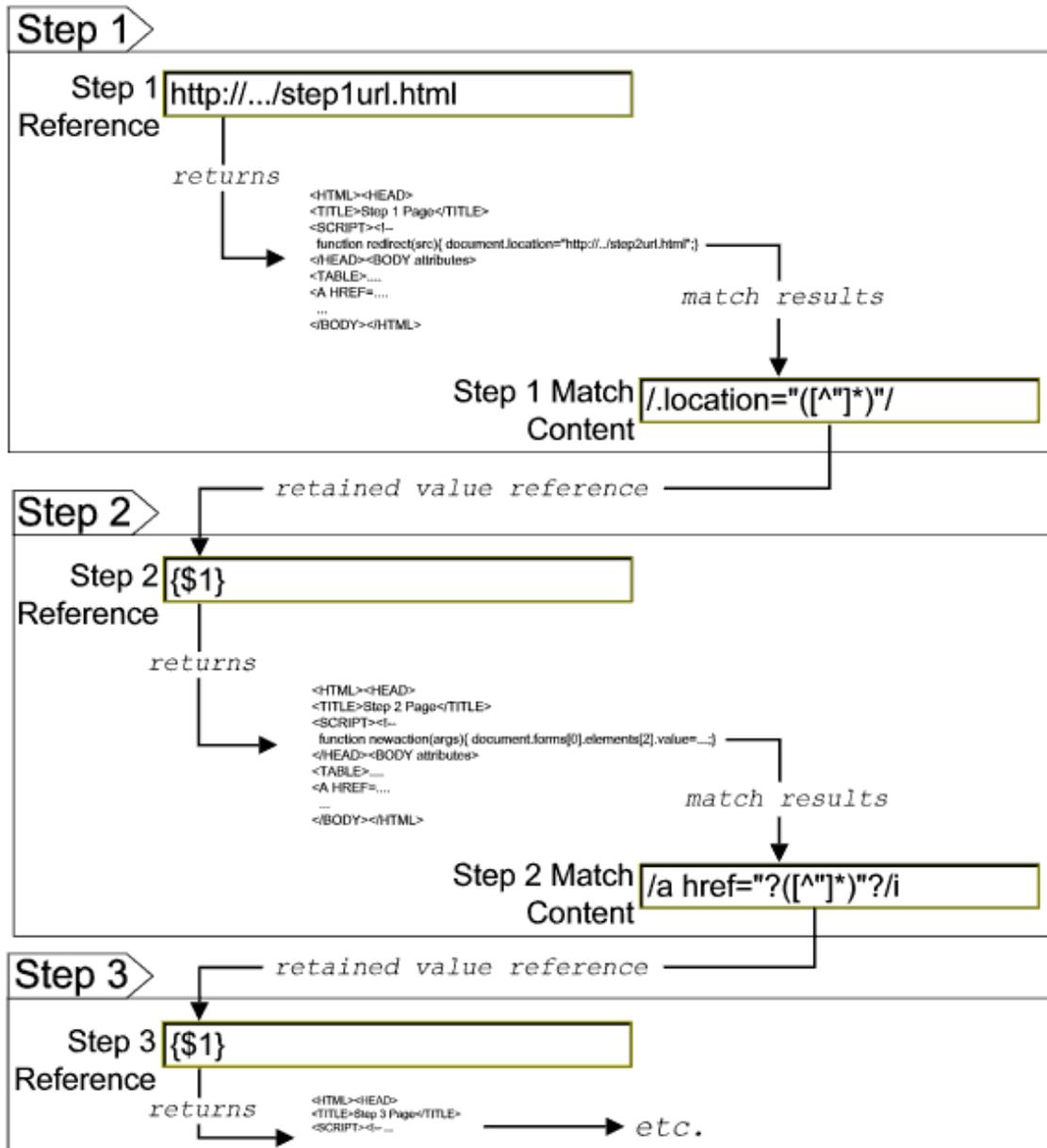
There are several ways to make a SiteScope URL Sequence monitor perform actions controlled by client-side programs and other dynamic content. Several of these workarounds are presented below. The workarounds generally require knowledge of the principles of Web page construction, CGI programming, Perl-style Regular Expressions Overview, 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 HTTP Settings section of the URL Sequence Step dialog box. 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><A HREF=...</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>

Dynamic Content	SiteScope Workaround
<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 <code>NAME=VALUE</code> pairs for the subject sequence step. This is done in the POST data box in the HTTP Settings section of the URL Sequence Step dialog box. This requires familiarity with the script, the form structure, and CGI request headers.</p>
<p>A script dynamically sets the ACTION attribute of an HTML <code><FORM></code> tag.</p>	<p>Manually enter the ACTION URL for the next sequence step. This is done in the URL box in the Reference Settings section of the URL Sequence Step dialog box. This requires familiarity with the script.</p>
<p>A script dynamically sets the METHOD attribute of an HTML <code><FORM></code> tag.</p>	<p>Manually enter the POST or GET data for the next sequence step. For POST methods, enter the data in the POST data box in the HTTP Settings section of the URL Sequence Step dialog box. For GET methods, enter the ACTION URL plus the <code>&NAME=VALUE</code> pairs in the URL box in the Reference Settings section of the URL Sequence Step dialog box. This requires familiarity with the script, the form structure, and CGI request headers.</p>

The figure below illustrates several of the principles of constructing a URL Sequence monitor using regular expressions. The regular expression 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 uses only 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)[\M-\=]*?(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 on' 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.

Note:

- Configure the monitor designated to save cookies to run at a frequency that is not less than the time frame of the session to make sure 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 make sure 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 assure that the monitor saving cookies runs first.

Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP and HTTPS protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

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 either:

- Selecting the **Accept untrusted certificates for HTTPS** option in the Authentication Settings section of the Monitor Settings panel as described in "[URL Sequence Monitor](#)" on page 695.
- Importing the server certificate. For details on how to perform this task, see "[How to Configure the URL Sequence Monitor](#)" on the next page.

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol\Client	Java	Wininet
SSLv2	x	x
SSLv3	x	√
TLSv1	√	√

Tasks

This section includes:

- "How to Configure the URL Sequence Monitor" below
- "How to import Server Certificates manually"

How to Configure the URL Sequence Monitor

1. Prerequisites

The user name and password specified in the URL Sequence Step dialog box must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.

2. Import the server certificates (if the Web Server is configured to use SSL encryption)

If the Web server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate. Use one of the following methods for importing server certificates:

- Import the server certificates using SiteScope Certificate Management. For details, see [How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide](#).
- Import the server certificates manually. For details, see ["How to Manually Import Server Certificates"](#) on page 706.

3. Add a URL Sequence monitor

Add the URL Sequence monitor to a monitor group container and enter a name for the monitor instance in the General Settings panel.

For details on the General Settings panel, see [General Settings in the Using SiteScope Guide](#).

4. Start a new URL sequence

Configure the first URL in the sequence in the URL Sequence Step dialog box. The URL sequence must begin with an initial URL.

- a. In the Step Settings panel of the New URL Sequence Monitor dialog box, click the **New Step** button.
- b. In the URL Sequence Step dialog box, enter the initial URL address in the Reference Settings section. 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. Configure the other sequence step settings as necessary and click **OK**. Generally, the URL is sufficient for the first step of most URL sequences.
- d. In the Step Settings panel, click the **Test Steps** button to run all the defined steps in the URL Sequence and display the results of the collected data. For details on the URL Sequence test, see ["URL Sequence Steps Results Dialog Box"](#) on page 716.

For details on the URL Sequence Step dialog box, see "URL Sequence Step Dialog Box" on page 711.

5. Define additional sequence steps

Configure the individual steps for the URL sequence in the URL Sequence Step dialog box.

- a. In the URL Sequence Step Settings panel of the New URL Sequence Monitor dialog box, click the **New Step** button.
- b. Use the options in the Reference Settings section to select how SiteScope progresses from one step of a URL sequence to the next. The options are:
 - o **URL**. To go to a URL manually.
 - o **Link**. To follow a hyperlink.
 - o **Form**. To select a form button.
 - o **Frame**. To select a frame within a frameset.
 - o **Refresh**. To follow a meta refresh redirection.

For details on the reference types, see "Defining Sequence Steps" on page 697.

- c. Configure the other sequence step settings as necessary and click **OK**. For user interface details, see "URL Sequence Step Dialog Box" on page 711.

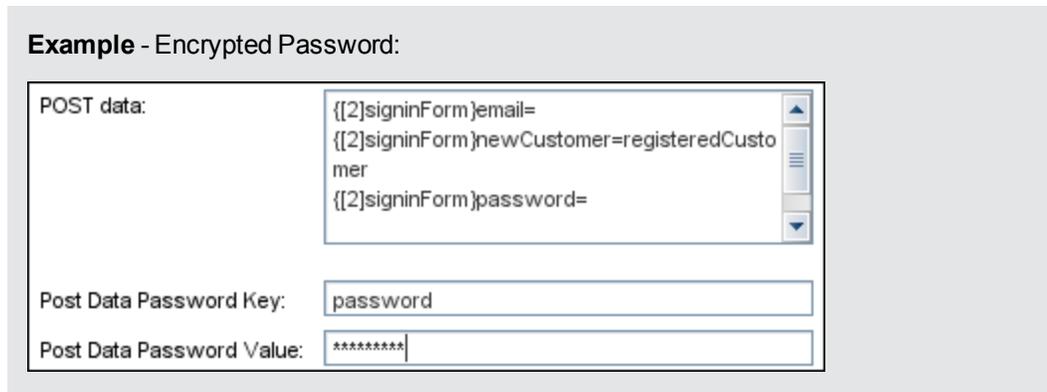
6. Enter an encrypted or unencrypted password (if required)

You can give an encrypted or unencrypted password to the URL monitor in the URL Sequence Step dialog box.

- To give an unencrypted password, enter the password in the **password=** line in the **POST data** text box. The password you enter 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. Enter the password itself in the **Post data password value** text box. The password is encrypted.

Example - Unencrypted Password:

The screenshot shows a dialog box with a 'POST data:' label on the left and a text area on the right. The text area contains three lines of data: `{{2}signInForm}email=`, `{{2}signInForm}newCustomer=registeredCusto`, and `mer` followed by `{{2}signInForm}password=mypassword`. Below the text area are two input fields: 'Post Data Password Key:' and 'Post Data Password Value:'.



7. Configure other settings for the monitor

Configure the monitor properties as described in the UI Descriptions section below.

How to Manually Import Server Certificates

Instead of using Certificate Management, you can manually import certificates using the `keytool` method, if preferred. Certificates imported this way can still be managed using Certificate Management. For details on Certificate Management, see Certificate Management in the Using SiteScope Guide.

1. Check the certificates already in the keystore, from the **<SiteScope root directory>\javallib\security** directory, by entering:

```
../../../../bin/keytool -list -keystore cacerts
```

2. Import the certificate, into **<SiteScope root directory>\javallib\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 **cacerts** file.

Note: The default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Therefore, you should create a copy of the **cacerts** file with a different name before SiteScope is upgraded or re-installed so that the file is not overwritten when new certificates are imported.

3. In SiteScope, select **Preferences > Certificate Management**, and click the **Reload Certificate List** button to reload the keystore certificates from the **cacerts** file. This enables you to manually reload keystore changes without having to restart SiteScope.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

This section includes:

- "Step Settings" below
- "URL Sequence Monitor Settings" below
- "URL Sequence Step Dialog Box" on page 711
- "URL Sequence Steps Results Dialog Box" on page 716

Step Settings

User interface elements are described below:

UI Element	Description
	New Step. Opens the URL Sequence Step dialog box enabling you to define the URL sequence steps. For user interface details, see "URL Sequence Step Dialog Box" on page 711.
	Edit Step. Opens the URL Sequence Step dialog box enabling you to edit the properties of an existing URL sequence step. For user interface details, see "URL Sequence Step Dialog Box" on page 711.
	Delete Last Step. Deletes the last step in the URL sequence.
	Select All. Selects all listed URL sequence steps.
	Clear Selection. Clears the selection.
	Test Steps. Runs the defined steps in the URL Sequence, and display the results of the collected data. The response embeds a copy of the HTML received from the HTTP request. For details, see "URL Sequence Steps Results Dialog Box" on page 716.
Step	The step number in the URL sequence.
Reference Type	URL of the sequence step.
Title	Name of this step within the sequence monitor.

URL Sequence Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	

UI Element	Description
Timeout (seconds)	<p>Amount of time, in seconds, to 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.</p> <p>Default value: 60 seconds</p>
Timeout for each step	<p>Uses 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.</p> <p>Default value: Not selected</p>
Retries	<p>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> <p>Default value: 0</p>
If error, resume at step	<p>Specifies 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>
Run resume step and remaining steps	<p>If the If error, resume at step option is selected and run, selection of this option causes SiteScope to run that step and continue running the other, subsequent steps until it reaches the end of the sequence.</p> <p>Default value: Not selected</p>
Show detailed measurements	<p>SiteScope records 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. <p>Default value: Not selected</p>
HTTP Settings	

UI Element	Description
Request headers	<p>Header request lines sent by the HTTP client to the server. Headers should be separated by a linebreak. The standard list of HTTP1.1 request headers can be found in http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.</p> <p>Note: Although this field is optional, some Web pages behave unexpectedly when the request header is missing (such as performing endless redirects, providing wrong content, and so forth).</p>
HTTP version	<p>HTTP version for SiteScope to use. Some systems may not be designed to accept HTTP 1.1 requests headers. If this is the case, select HTTP 1.0.</p> <p>Default value: HTTP version 1.1</p>
Retrieve images	<p>Status and response time statistics include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by <code>IMG</code>, <code>BODY</code> (from the background property), and <code>INPUT TYPE=IMAGE</code> 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> <p>Default value: Not selected</p>
Retrieve frames	<p>SiteScope retrieves the frames references in a frameset and counts their retrieval time in the total time to download this page. Frames include those referenced by <code>FRAME</code> and <code>IFRAME</code> 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> <p>Default value: Not selected</p>

UI Element	Description
Use WinInet	<p>WinInet is used as an alternative HTTP client for this monitor.</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>Default value: Not selected (Apache is used)</p>
Proxy Settings	
HTTP proxy	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URLs in the sequence.
Proxy server user name	<p>Proxy server user name if required to access the URLs in the sequence.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Proxy server password	<p>Proxy server password if required to access the URLs in the sequence.</p> <p>Note: Your proxy server must support Proxy-Authenticate for these options to function.</p>
Proxy NTLM V2	Select if the proxy server requires authentication using NTLM version 2.
Authentication Settings	
NTLM V2	<p>Select if the URL you are accessing requires authentication using NTLM version 2.</p> <p>Default value: Not selected</p>
Accept untrusted certificates 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" on page 703.</p> <p>Default value: Not selected</p>
Accept invalid certificates for HTTPS	<p>Select 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> <p>Default value: Not selected</p>

UI Element	Description
Use cookie persistency	<p>Shares cookies between monitor runs and between configured monitors. For details, see "Sharing Cookies Between Monitor Runs and Configured Monitors" on page 702.</p> <p>Default value: Not selected</p>
Load cookies from persistency	<p>Loads all relevant cookies from the persistency file and adds them to the list of cookies to be sent to the server. Cookies are loaded at the beginning of the monitor run.</p> <p>Default value: Not selected</p>
Save cookies to persistency	<p>Saves 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.</p> <p>Default value: Not selected</p>
Cookie persistency file path	<p>Path and name of the cookie persistency file.</p>

URL Sequence Step Dialog Box

This dialog box displays the settings used for each individual sequence step in the URL Sequence Step Settings panel of the New URL Sequence Monitor 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.

To access: Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **URL Sequence** monitor. In the **Step Settings** panel, click the **New Step** or **Edit Step** button.

User interface elements are described below:

UI Element	Description
Reference Settings	

UI 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 697.</p> <ul style="list-style-type: none"> • URL. Go to a particular URL directly. Enter 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 be that the page uses a client-side program. In this case, you may have to specify the URL manually. • Form. Enter 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 699. • 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.
Main Settings	
Step title	Enter the text for the title of this step within the sequence monitor. The title is only displayed in the URL Sequence Steps Settings panel.

UI Element	Description
Match content	<p>Enter 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 <code>content match error</code>.</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: <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 <code>i</code> after the trailing slash indicating case-insensitive matching. Example: <code>/href=Doc\d+\.html/ or /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>. 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>
Match content for error	<p>Enter 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>
Delay (seconds)	<p>Enter how long SiteScope should wait before executing the next step of the sequence.</p> <p>Default value: 0 seconds</p>
Authentication Settings	
User name	<p>If the URL specified for this step requires a name and password for access, enter the user name. Alternately, you can leave this entry blank and enter 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	<p>If the URL specified for this step requires a name and password for access, enter the password. Alternately, you can leave this entry blank and enter 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>

UI Element	Description
Pre-emptive authorization	<p>Select when the authorization credentials should be sent if SiteScope requests the target URL.</p> <ul style="list-style-type: none"> • Use global preference (default value). Select to have SiteScope use the settings specified in the Pre-emptive authorization field in the General Settings 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. <p>Note: If the URL does not require a user name and password, this option may cause the URL to fail.</p> <ul style="list-style-type: none"> • Authenticate if requested. Select to send the user name and password on the second request if the server requests a user name and password. <p>Note: If the URL does not require a user name and password, this option may be used.</p> <p>All options use the authorization User name and Password entered for this monitor instance. If these are not specified for the individual monitor, the Default authentication user name and Default authentication password specified in the General Settings of the General Preferences page are used, if they have been specified.</p> <p>Note: Pre-emptive authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
Client side certificate	<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 root>\templates.certificates directory. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You enter the password for the certificate in the Client side certificate password box.</p> <p>Default value: none</p>
Client side certificate password	<p>If you are using a client side certificate and that certificate requires a password, enter the password.</p>
Authorization NTLM domain	<p>Enter the domain for Windows NT LAN Manager (NTLM) authorization if it is required to access the URL in this step.</p>
HTTP Settings	
URL content encoding	<p>SiteScope retrieves the correct encoding from the server response. The default value appearing here should not be edited.</p> <p>Default value: Retrieve encoding from server response</p>

UI 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), enter 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>Enter 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>Enter 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, <code>gmail.com</code> sends. The site <code>gmail.com</code> 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 <code>gmail.com</code> is <code>Passwd</code>. The Post Data Password Value is the password that you provide.</p> <p>For details on how to enter an encrypted or unencrypted password, see "How to Configure the URL Sequence Monitor" on page 704.</p>
POST Data encoding	<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. • Do not force URL encoding. Do not encode the post data.
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>

UI Element	Description
Show HTML	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.

URL Sequence Steps Results Dialog Box

This dialog box displays the collected data from running all the URL steps defined in the Step Settings panel. This includes the status of the overall sequence, the response time for each step and the content match for each step in the sequence (if applicable). A copy of the HTML page returned at each step of the sequence is also displayed, so that a more graphical view of the sequence can be viewed.

To access:

1. Select the **Monitors** context.
2. In the monitor tree, right-click a group, select **New > Monitor**, and select the **URL Sequence** monitor.
3. In the **Step Settings** panel, configure the individual steps for the URL sequence, and then click the **Test Steps**  button to view the test results.
4. In the URL Sequence Steps Results dialog box, use the step hyperlinks at the top to navigate to any step in the sequence.

User interface elements are described below:

UI Element	Description
<Step # link>	Links to the relevant step in the results.
Save to file	Opens the Save dialog box, enabling you to save the sequence steps results to an HTML file.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- When using the URL Sequence monitor with WinInet, if you encounter error 12057 (which indicates that revocation cannot be checked because the revocation server is offline), you should either:
 - Avoid using WinInet, or
 - In Internet Explorer, select **Tools > Internet Options > Advanced > Security**, and switch off **Check for server certificate revocation**.
- You can run all the steps defined in the URL sequence by clicking the **Test Steps** button in the Step Settings panel or the **Tools** button in the SiteScope Dashboard. This displays the collected data from each step, and embeds a copy of the HTML page returned. For details, see "[Step Settings](#)" on page 707.
- If a step fails, an error message is displayed and the sequence steps report is not generated.
- When using several URL load threads, the total duration time might be less than the combined total of the DNS lookup, connection, server response, and download time. In this case, total duration time is the duration between the start and end of all threads, whereas DNS lookup, connection, response, and download time is the sum of the corresponding value of each thread. You can set the required count of URL load threads in the `_urlLoadThreads` property in `<SiteScope root directory>\groups\master.config`.

Chapter 96

VMware Datastore Monitor

Use the VMware Datastore monitor to monitor the state of VMware Datastores and Virtual Disks (connectivity, capacity, free space, and snapshot size).

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **VMware Datastore** monitor.

Learn More

This section includes:

- "VMware Datastore Monitor Overview" below
- "Supported Versions" below
- "Dynamic Monitoring Mechanism" below
- "SSL Connectivity" on the next page
- "Connection Pool Settings" on the next page
- "VMware Datastore Monitor Topology" on page 721
- "System Tuning for Loaded Environments" on page 722

VMware Datastore Monitor Overview

SiteScope simplifies the monitoring of virtual storages changes in dynamic, virtualized environments by automatically changing the SiteScope configuration according to changes in the virtual environment. The VMware Datastore monitor is dynamically updated over time by adding or removing counters and thresholds as datastores and virtual disks are added or removed from the VMware Datacenters. This enables you to configure the monitor once, and leave it to automatically discover changes in the environment and update itself.

During initial monitor creation, the monitor uses the connection URL configured to access the VMware datacenters in the vCenter and dynamically discover the exists datastores and virtual disks. You can select from these performance counters to determine which measurements SiteScope should retrieve for reporting datastore status.

For details describing all the available counters, refer to the VMware documentation available at <http://www.vmware.com/support/developer/vc-sdk/visdk25pubs/ReferenceGuide/>.

Supported Versions

This monitor supports monitoring remote servers running on VMware vCenter Server 4.0, 4.1, 5.0, 5.1.

Note: Monitoring VMware ESX(i) is not supported when Lockdown mode is enabled.

Dynamic Monitoring Mechanism

To enable the monitor to dynamically update counters and thresholds, select the counter patterns you want to monitor using a regular expression. For example, if you enter the pattern `/.*/.*/accessible/`, the monitor retrieves the accessible counter for all datastores.

Note: SiteScope uses Perl regular expressions for pattern matching. Accordingly, you should use Perl regular expressions to specify patterns for VMware Datastore monitor counters. For example, if you enter `/usage.*/` or `usage`, any counters with usage in their name match this pattern and are added to the counters list.

You also set the frequency of the dynamic update mechanism at the monitor level. This is the frequency that SiteScope uses to update the counters retrieved from the server. This enables running the update mechanism at a frequency that is appropriate for the monitor type.

During each update, the monitor connects to the VMware datastore and dynamically updates:

- The status of each counter that matches the pattern defined by the regular expression. If there are no available counters on the server, or no counters that match the monitor patterns, the monitor is not updated and it displays the previous counters set.
- Thresholds for the selected counters (every time counters are added or removed as a result of environment changes, the appropriate threshold is added or removed from the monitor).

In this way, the monitor automatically configures itself with counters on the relevant dynamic environment components. Counters that are no longer available on the VMware vCenter are automatically removed from SiteScope and no errors are logged.

Note: When you define static counters (with no regular expression), these counters are never removed from the monitor, even if they are no longer available on the server.

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. For details on how to perform this task, see ["How to import the VMware Server Certificates" on page 725](#).

Connection Pool Settings

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. The connection pool is a set of pools per key. A key is the combination of a vCenter, and a user (the connection cannot be shared between different users due to different permissions)

If all VM monitors are configured with the same vCenter URL and user, one connection pool is created. For two vCenters and two different users for every vCenter, four connection pools are created.

The connection pool configures itself over time to ensure that only working connections stay in the pool. It does this by running an additional thread at the rate of the connection timeout multiplied by two; if the connection timeout is 30 minutes, it will run once every hour and evict idle connections from the pool. Connections that are idle for more than half a minute before the connection timeout are eligible for eviction.

For example, if the connection timeout is 30 minutes, the thread will evict connections that were idle for more than 29.5 minutes, but less than 30 minutes (to avoid a connection timeout). The connections that were idle more than 30 minutes are evicted by the timeout process. As a result, only working connections stay in the pool.

You can configure the following connection pool properties in the **<SiteScope root directory>\groups\master.config** file:

- **_vmWareConnectionPoolMaxIdlePervCenterKey.** The maximum number of idle connections in the pool. The default value is 60.
- **_vmWareConnectionPoolMaxSizePervCenterKey.** The maximum number of active connections in the pool. The default value is 60.

Note: If a SiteScope is registered to BSM, it uses more connections to retrieve properties relevant for topology reporting. Therefore, you should increase the maximum number of idle and active connection properties to enable SiteScope to perform well.

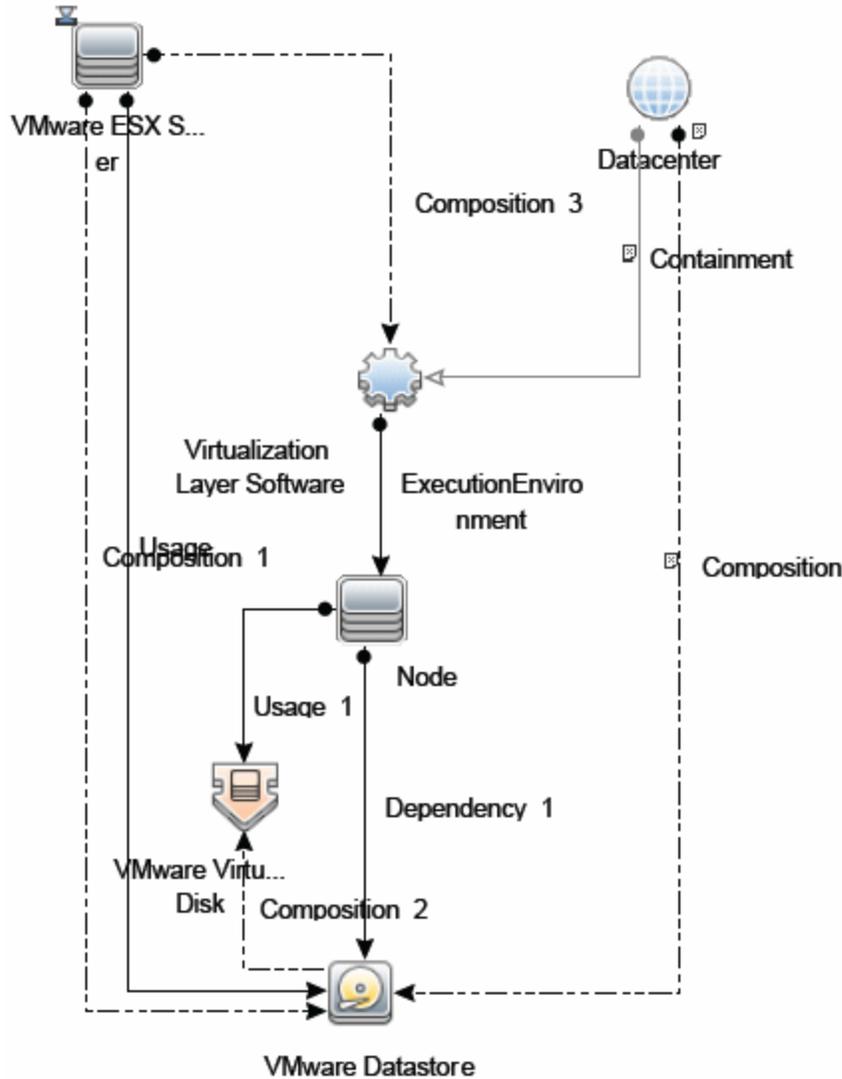
- **_vmWareConnectionPoolMaxTotal.** Maximum size of total connections for all keys. This is the total number of connections used in all the defined SiteScope vCenters. The default value is 1500.

Tip: We recommend setting the maximum size of total connections to the number of configured VM monitors in SiteScope, and let the internal connection pool mechanism optimize itself.

- **_vmWareConnectionTimeOut.** Connection timeout in minutes. The default value is 30 minutes.

VMware Datastore Monitor Topology

The VMware Datastore monitor can identify the topology of the VMware servers being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

System Tuning for Loaded Environments

SiteScope installed on a 64-bit environment supports configurations with up to 2000 VMware datastore monitors running concurrently. This loaded system can be integrated with BSM and OM metrics.

To support loaded environments, the following system tuning is required:

- SiteScope sizing is required to increase JVM heap size, desktop heap size, and the number of file handles. You can use the SiteScope Configuration Tool to size SiteScope. For details, see Using the SiteScope Configuration Tool in the HP SiteScope Deployment Guide.
- Add the `_runGCPPeriod=1200000` property to the `<SiteScope root directory>\groups\master.config` file. This means that SiteScope initiates

running the garbage collector every 20 minutes (1200000 milliseconds) for better performance.

- Tune the following vCenter connections parameters in the **<SiteScope root directory>\groups\master.config** file, as required:
 - **_vmWareConnectionPoolMaxIdlePervCenterKey=**
 - **_vmWareConnectionPoolMaxSizePervCenterKey=**
 - **_vmWareConnectionPoolMaxTotal=**
 - **_vmWareConnectionTimeOut=**
- Increase the number of dynamic monitors handles in **Preferences > Infrastructure Preferences > Dynamic Monitoring Settings**:
 - **Dynamic monitoring core thread pool size: 50**
 - **Dynamic monitoring maximum thread pool size: 70**

Tasks

This section includes:

- "How to Configure the VMware Datastore Monitor" below
- "How to import the VMware Server Certificates" on the next page

How to Configure the VMware Datastore Monitor

1. Prerequisites

The following are the requirements for monitoring VMware-based servers:

- The monitored vCenter server must be directly accessible by the SiteScope server (no proxy involved).
- The vCenter server provides connection either by http or by https (depending on the vCenter server configuration). If https is used, server certificate must be imported to the SiteScope. For task details, see "How to import the VMware Server Certificates" on the next page.

2. Configure the monitor properties

- a. Configure the monitor properties as described in the UI Descriptions section below.
- b. Click the **Get Counter** button, and select the counters you want to monitor from the Select Counters Form. The counters are added to the Preview tree in the **Patterns & Counters** section.
- c. For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
 - Clicking the **Add New Counter**  button to add an empty line to the table, and creating a pattern format using a regular expression.

Tip:

- (1). The pattern should always start and end with the forward slash ("/") character.
- (2). [and] characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character).
- (3). Use ".*" to describe any character any number of times.

For example, if you enter the pattern `/.*/.*/accessible/`, the monitor retrieves the accessible counter for all datastores .

- Selecting a static counter, and editing the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.
- d. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counters Preview tree.
 - e. Set the frequency for updating counters from the server, and then click **Verify & Save** or **Save** to save your settings. If you use only static counters, they are not affected by the

frequency for updating counters, since the dynamic framework does not run.

- f. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

3. **Enable topology reporting - optional**

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting).

For user interface details, see BSM Integration Data and Topology Settings in the Using SiteScope Guide.

4. **Configure the connection pool mechanism - optional**

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. We recommend setting the maximum size of total connections (the `_vmWareConnectionPoolMaxTotal` property in the `master.config` file) to the number of configured VM monitors in SiteScope, and letting the internal connection pool mechanism optimize itself.

For details, see "Connection Pool Settings" on page 720.

5. **Results**

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the vCenter service and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:

- The SiteScope **Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

For additional troubleshooting suggestions, see "Tips/Troubleshooting" on page 730.

How to import the VMware Server Certificates

If the VMware server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate.

You can import the certificates either:

- Using Certificate Management in the SiteScope Preferences. For task details, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
- Manually using the keytool method (see procedure below for details).

To import server certificates manually:

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 **cacerts** file.

Note: The default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Therefore, you should create a copy of the **cacerts** file with a different name before SiteScope is upgraded or re-installed so that the file is not overwritten when new certificates are imported.

3. In SiteScope, select **Preferences > Certificate Management**, and click the **Reload Certificate List** button to reload the keystore certificates from the **cacerts** file. This enables you to manually reload keystore changes without having to restart SiteScope.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

VMware Datastore Monitor Settings

User interface elements are described below:

UI Element	Description
URL	<p>URL of the VMware vCenter on the datastores that you want to monitor.</p> <p>The format of the URL is: <code><protocol>://<server_name>/sdk</code> where <code><protocol></code> is either <code>http</code> or <code>https</code>, and <code><server_name></code> is the name of the datastore server. You can import the server certificates directly from the monitor using SiteScope's Certificate Management (click the Import Certificates icon), instead of importing certificates manually.</p> <p>Note: If you get 'Error Code: 31008. Error getting counters' when SSL is used, navigate to Preferences > Infrastructure Preferences > General Settings, and select Accept untrusted SSL certificates.</p>
Credentials	<p>User name and password required to access the VMware datastore. Select the option to use for providing credentials:</p> <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
VM Disk Timeout (seconds)	<p>Amount of time, in seconds, to wait for the datastore to find its virtual disks before timing out.</p> <p>Default value: 1</p>

UI Element	Description
Patterns & Counters	<p>Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.</p> <p>Click the Add New Counter  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the Delete Counter  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the View Matches for Selected Pattern Counter  button to display counters that match the selected patterns.</p> <p>Note: SiteScope uses Perl regular expressions for pattern matching. Accordingly, you should use Perl regular expressions to specify patterns for VMware Datastore monitor counters. For example, if you enter <code>/cpu.*/</code> or <code>cpu</code>, any counters with <code>cpu</code> in their name match this pattern and are added to the counters list.</p>
Get Counters	<p>Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.</p>
Counters Preview	<p>Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.</p>
Frequency of updating counters from server	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p>Default value: 15 minutes</p> <p>Note:</p> <ul style="list-style-type: none"> • The update frequency cannot be less than the monitor run frequency in Monitor Run Settings. • When configuring this setting in a template, the variable value can only be in time units of seconds. • Static counters are never deleted.
Continue displaying counters that no longer exist after update	<p>Counters that no longer exist after running the update mechanism to retrieve counters from the VMware server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful if a server goes down or for keeping track of what counters were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings.</p> <p>Default value: Selected</p>

Monitor Reference

Chapter 96: VMware Datastore Monitor

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section describes troubleshooting and limitations for the VMware Datastore monitor.

- "Maximum Number of Counters That Can be Saved" below
- "Troubleshooting Logs" below

Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the `_browsableContentMaxCounters` parameter in the `master.config` file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns are limited by the `_maxCountersForRegexMatch` parameter in the `master.config` file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The `_maxCountersForRegexMatch` parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both `_browsableContentMaxCounters` and `_maxCountersForRegexMatch` parameters in the `master.config` file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

Troubleshooting Logs

- Check for dynamic framework errors in:
 - `<SiteScope root directory>\logs\dynamic_monitoring_changes.log`. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
 - `<SiteScope root directory>\logs\dynamic_monitoring.log`. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).
- Check for VMware monitor errors in:
 - `<SiteScope root directory>\logs\RunMonitor.log`. Contains information about specific monitor runs and actions related to managing monitors.
 - `<SiteScope root directory>\logs\vmware_connections.log`. This log provides information about the connection pool against the vCenter (get/return connection).
- Copy the following sections from the `log4j.properties.debug` file in the `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava` folder to the `log4j.properties` file, and change the log level to DEBUG.

```
#####  
# Dynamic Monitoring
```

```
#####
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
false
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG,
dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFile
Appender
log4j.appender.dynamic.monitoring.appender.File=./${log.file.path}/dynamic_
monitoring.log
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.Pattern
Layout
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p -
%m%n

# Dynamic monitors changes category
log4j.category.DynamicMonitoringChanges=INFO,
dynamic.monitoring.changes.appender
log4j.additivity.DynamicMonitoringChanges=false

# VMware Connection Pool
#####
log4j.category.VMwareConnectionPool=${monitor.loglevel}, vmware.connection.pool.appender
log4j.additivity.VMwareConnectionPool=false
log4j.appender.vmware.connection.pool.appender=org.apache.log4j.RollingFileAppender
log4j.appender.vmware.connection.pool.appender.File=./${log.file.path}/vmware_
connections.log
log4j.appender.vmware.connection.pool.appender.MaxFileSize=${def.file.max.size}
log4j.appender.vmware.connection.pool.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.vmware.connection.pool.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.vmware.connection.pool.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-
5p - %m%n
```

Chapter 97

VMware Host Monitors

Enables you to monitor CPU, Memory, Network, State and storage-related counters of the VMware host server and its guest virtual machines, as described in "VMware Host Monitor Overview" on the next page.

Note: VMware Host monitors are optional SiteScope monitors that require additional licensing to enable them in the SiteScope interface. Contact your HP sales representative for more information.

Tip: You can view a guided and narrated demonstration for the VMware Host monitors on the HP Videos channel on YouTube: <http://www.youtube.com/watch?v=A7Tzb-lb168&feature=plcp>.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the required VMware Host monitor.

Learn More

This section includes:

- "VMware Host Monitor Overview" below
- "Supported Versions" on the next page
- "VMware Performance Monitor or VMware Host Monitor?" on the next page
- "Dynamic Monitoring Mechanism" on page 735
- "Calculated (Smart) Counters" on page 736
- "SSL Connectivity" on page 737
- "Connection Pool Settings" on page 737
- "VMotion Support" on page 738
- "VMware Host Monitors" on the previous page
- "System Tuning for Loaded Environments" on page 740
- "Metrics Integration Support" on page 740

VMware Host Monitor Overview

Virtualization is one of the most important technologies in IT infrastructures that creates new complexities when it comes to managing the virtualization environment. Virtual Machines (VMs) and their host VMware ESX Servers need performance and availability monitoring.

SiteScope simplifies the monitoring of virtual infrastructure changes in dynamic, virtualized environments by automatically changing the SiteScope configuration according to changes in the virtual environment. VMware Host monitors are dynamically updated over time by adding or removing counters and thresholds as virtual machines are added or removed from the VMware Host. This enables you to configure the monitor one time, and leave it to automatically discover changes in the environment and update itself. The update is not only as a result of VMotion, but also when a new CPU, disk, or other resource is added or removed from the host server or guest VM.

Use the VMware Host monitors to monitor performance related resources (CPU, memory, network, state, and storage) on the host server and its guest VMs. The VMware Host CPU and VMware Host Memory monitors also include "smart" configuration counters that provide resource optimization recommendations to help you analyze and solve problems in dynamic virtual infrastructures and maximize resource usage. For details, see "[Calculated \(Smart\) Counters](#)" on [page 736](#).

During initial monitor creation, the monitors use the connection URL configured to access the vCenter or physical host URL 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/support/developer/vc-sdk/visdk25pubs/ReferenceGuide/>.

Tip: We recommend adding VMware Host monitors by deploying the VMware Host solution

template instead of creating the monitors manually. The template has a predefined monitor set with optimized settings based on VMware best practices for troubleshooting the ESX/Host server; it monitors only the relevant components (counter patterns) in dynamic environments, and provides the minimum data required for troubleshooting problems in the monitored infrastructure. For details, see VMware Capacity Management Solution Templates in the Using SiteScope Guide.

Supported Versions

This monitor supports monitoring remote servers running on:

- VMware VirtualCenter 2.x
- VMware ESX 3.x, 4.0, 4.1
- VMware ESXi 3.5, 4.0, 5.0, 5.1
- VMware ESX 2.5 using VirtualCenter 2.x
- VMware ESX 3.x using VirtualCenter 3.x
- VMware vCenter Server 4.0, 4.1, 5.0, 5.1

Note: Monitoring VMware ESX(i) is not supported when Lockdown mode is enabled.

VMware Performance Monitor or VMware Host Monitor?

	VMware Performance Monitor	VMware Host Monitors
Type of user	VM user/owner	Virtualization administrator
Requirements	<ul style="list-style-type: none"> • Measure performance and availability of a particular VM or set of VMs. • Display SiteScope and BSM reports and BSM topology for this VM. <p>Usually, VM users/owners are not interested on which host the VM runs or other issues.</p>	<ul style="list-style-type: none"> • Manage a virtualization environment or vCenter and provide VM services to other users. • Measure the availability and performance of vCenter resources (physical host machines). <p>Usually, virtualization administrators are not interested in specific VMs (only if this machine causes performance issues to the host).</p>
Recommended Use	Monitoring one or a set of VMs	Deploy using VM Host solution template

	VMware Performance Monitor	VMware Host Monitors
Benefits	Measures the data every monitor run regardless of whether the VM has migrated.	<ul style="list-style-type: none"> Enables the administrator to make most efficient use of host resources (create maximum VMs and serve more users). Provides notifications of availability and performance problems on the host (that might be caused by specific VM or VMs). The monitor is dynamically updated (see "Dynamic Monitoring Mechanism" below). Smart counters provide useful information for configuring the VM on the host to help maximize resource usage. For details, see "Calculated (Smart) Counters" on the next page.
Data in SiteScope and BSM Reports	Provides user with SiteScope and BSM reports with continuous data and topology that match the changes (the same VM connects to the relevant host).	<ul style="list-style-type: none"> Enables the administrator to check host information only (the data is continuous). The topology matches VM migration for the monitored hosts. Does not provide continuous data on the VM (every time a VM migrates from host to host, its ID changes in SiteScope and BSM reports). However, VM data does not interest the administrator.

Dynamic Monitoring Mechanism

To enable the monitor to dynamically update counters and thresholds, select the counter patterns you want to monitor using a regular expression. For example, if you enter the pattern `./*/VirtualMachine/./*/cpu/usage.average\[\]/`, the monitor retrieves the `usage.average[]` counter for all VMs.

Note: SiteScope uses Perl regular expressions for pattern matching. For example, if you enter `/cpu.*/` or `cpu`, any counters with `cpu` in their name match this pattern and are added to the counters list.

You also set the frequency of the dynamic update mechanism at the monitor level. This is the frequency that SiteScope uses to update the counters retrieved from the server. This enables running the update mechanism at a frequency that is appropriate for the monitor type.

During each update, the monitor connects to the vCenter/Host server and dynamically updates:

- The status of each counter that matches the pattern defined by the regular expression. If there are no available counters on the server, or no counters that match the monitor patterns, the

monitor is not updated and it displays the previous counters set.

- Thresholds for the selected counters (every time counters are added or removed as a result of environment changes, the appropriate threshold is added or removed from the monitor).

In this way, the monitor automatically configures itself with counters on the relevant dynamic environment components. If **Continue displaying counters that no longer exist after update** is selected in VMware Host Monitor Settings, the counters that no longer exist on the VMware host server after running the update mechanism are still displayed in the monitor (they are displayed as **n/a**). This is useful if a server goes down or for keeping track of what counters were previously being monitored. If this setting is cleared, counters that are no longer available are automatically removed from SiteScope and no errors are logged.

Note: When you define static counters (with no regular expression), these counters are never removed from the monitor, even if they are no longer available on the server.

Calculated (Smart) Counters

The VMware Host CPU and VMware Host Memory monitors also have a set of counters that provide information on the configured resources and the resources that are actually used. This information helps you to use host resources more efficiently by configuring VMs on the host to maximize VM resource usage.

Note:

- If calculated counter values are unavailable, this means the values are not defined in vCenter (for example, a reservation or limit is not defined for the VM).
- Calculated counters are not available in monitors deployed by the solution template.

These counters provide the following information:

Monitor	Counter Name	Description
VMware Host CPU	usageToReservationRelation	Measures the relation between CPU usage and CPU reserved on the VM. If the counter value is < 1 over time, the VM is not using the reserved CPU and the vCenter administrator should consider reducing the reservation.
	usageToLimitRelation	Measures the relation between CPU usage and the CPU limit on the VM. If the counter value is ≥ 1 (or close to 1) over time, the vCenter administrator should consider increasing the CPU limit for the VM.

Monitor	Counter Name	Description
VMware Host Memory	usageToReservationRelation	Measures the relation between memory usage and memory reserved on the VM. If the counter value is < 1 over time, the VM is not using the reserved memory and the vCenter administrator should consider reducing the reservation.
	usageToLimitRelation	Measures the relation between memory usage and memory limit on the VM. If the counter value is ≥ 1 (or close to 1) over time, the vCenter administrator should consider increasing the memory limit for the VM.
	usageOfESXMemory	Measures ESX host memory usage for every VM. This is useful for VMs that always run on the same ESX host (when there are no clusters or Distributed Resource Scheduler (DRS)).
	missingBalloonSizeTillTarget	Measures the difference between the target balloon set for the VM (by the VMkernel) and the actual balloon size. If the counter value is < 1 over time, the VM uses more balloon size than was set as the target, and the vCenter administrator should consider increasing the target balloon size.

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. For details on how to perform this task, see "How to import the VMware Server Certificates" on page 744.

Connection Pool Settings

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. The connection pool is a set of pools per key. A key is the combination of a vCenter or host URL, and a user (the connection cannot be shared between different users due to different permissions).

If all VM monitors are configured with the same vCenter URL and user, one connection pool is created. For two vCenters and two different users for every vCenter, four connection pools are created.

The connection pool configures itself over time to ensure that only working connections stay in the pool. It does this by running an additional thread at the rate of the connection timeout multiplied by two; if the connection timeout is 30 minutes, it will run once every hour and evict idle connections from the pool. Connections that are idle for more than half a minute before the connection timeout are eligible for eviction.

For example, if the connection timeout is 30 minutes, the thread will evict connections that were idle for more than 29.5 minutes, but less than 30 minutes (to avoid a connection timeout). The

connections that were idle more than 30 minutes are evicted by the timeout process. As a result, only working connections stay in the pool.

You can configure the following connection pool properties in the **<SiteScope root directory>\groups\master.config** file:

- **_vmWareConnectionPoolMaxIdlePervCenterKey.** The maximum number of idle connections in the pool. The default value is 60.
- **_vmWareConnectionPoolMaxSizePervCenterKey.** The maximum number of active connections in the pool. The default value is 60.

Note: If a SiteScope is registered to BSM, it uses more connections to retrieve properties relevant for topology reporting. Therefore, you should increase the maximum number of idle and active connection properties to enable SiteScope to perform well.

- **_vmWareConnectionPoolMaxTotal.** Maximum size of total connections for all keys. This is the total number of connections used in all the defined SiteScope vCenters. The default value is 1500.

Tip: We recommend setting the maximum size of total connections to the number of configured VM monitors in SiteScope, and let the internal connection pool mechanism optimize itself.

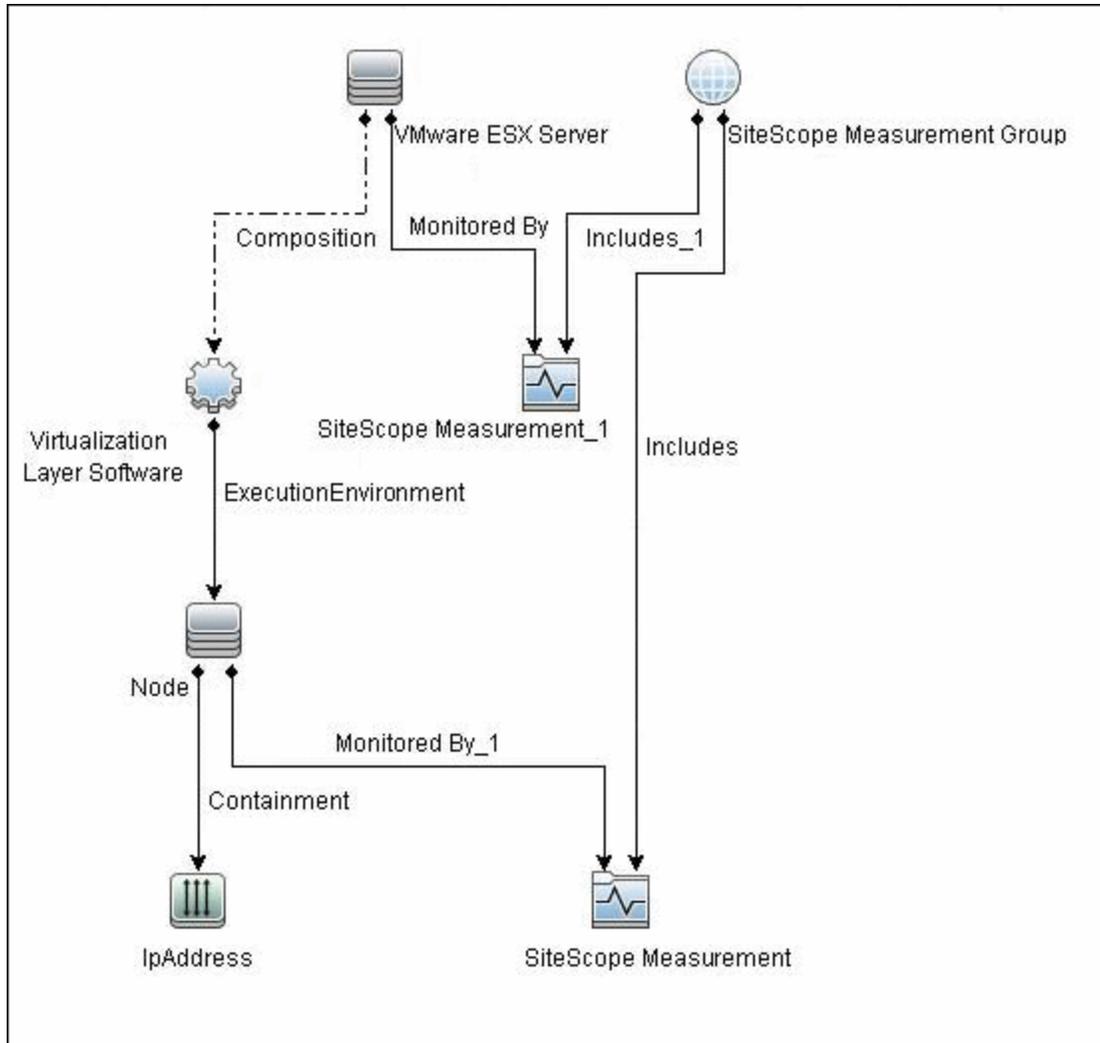
- **_vmWareConnectionTimeOut.** Connection timeout in minutes. The default value is 30 minutes.

VMotion Support

VMware's VMotion technology enables the transparent migration of running virtual machines between physical hosts in a virtual infrastructure cluster. It enables you to move an entire running virtual machine instantaneously from one server to another with continuous service availability and zero downtime. This process can be done both manually and automatically as part of cluster load balancing.

VMware Host Monitor Topology

The VMware Host monitors can identify the topology of the VMware servers being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

The VMware Host monitor reports the Node CI for the virtual machine (VM) and the VMware ESX Server CI (ESX), and reports the connection between the VM and ESX. If there is counter defined on the VM, the related ESX is also reported.

Note:

- When deleting a monitor or making configuration changes, links between previously reported VMs and ESXs are not deleted. This means that if a monitor was deleted and relevant VMs were subsequently migrated, the newly-created monitor contains the old link to the previous ESX Server and a link to the current ESX Server (reported on monitor creation).
- To enable the monitor to report the correct topology to BSM 9.0x, follow the "[VMware Host Monitors](#)" on page 732 procedure in Troubleshooting and Limitations below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

System Tuning for Loaded Environments

SiteScope installed on a 64-bit environment supports configurations with up to 2150 VMware Host monitors running concurrently. This loaded system can be integrated with BSM and OM metrics.

To support loaded environments, the following system tuning is required:

- SiteScope sizing is required to increase JVM heap size, desktop heap size, and the number of file handles. You can use the SiteScope Configuration Tool to size SiteScope. For details, see Using the SiteScope Configuration Tool in the HP SiteScope Deployment Guide.
- Add the **_runGCPeriod=1200000** property to the **<SiteScope root directory>\groups\master.config** file. This means that SiteScope initiates running the garbage collector every 20 minutes (1200000 milliseconds) for better performance.
- Tune the following vCenter/ESX connections parameters in the **<SiteScope root directory>\groups\master.config** file, as required:
 - **_vmWareConnectionPoolMaxIdlePervCenterKey=**
 - **_vmWareConnectionPoolMaxSizePervCenterKey=**
 - **_vmWareConnectionPoolMaxTotal=**
 - **_vmWareConnectionTimeOut=**
- Increase the number of dynamic monitors handles in **Preferences > Infrastructure Preferences > Dynamic Monitoring Settings**:
 - **Dynamic monitoring core thread pool size: 50**
 - **Dynamic monitoring maximum thread pool size: 70**

Metrics Integration Support

SiteScope uses the HP Operations agent to make metrics data from VMware Host monitors available to HP Performance Manager in HPOM and to PMi in BSM.

The reported metrics are associated with the relevant ESX host or VM resource. The target is the counter target (not the monitor target).

Monitor Type	Reports Metrics For	Reports Metrics to the Following Tables
VMware Host	ESX	VMware Host CPU, Memory, Storage, State, Network, System tables
	VM	VMware VM CPU, Memory, Storage, State, Network, System tables

Note:

- The first time you start monitoring a new VM or ESX host, it takes more time to get the data and to view it in the HP Operations agent.
- To support motion and changes in the vCenter, such as change of IP or host name, you can change the interval for updating the data saved to the cache in the **Frequency of VM**

configuration retrieval from vCenter (hours) field in **Preferences > Infrastructure Preferences > Monitor Settings**. By default, data is updated every 4 hours. You can also configure this by modifying the `_vmwareRetrieveConfFrequencyHours` property in the `<SiteScope root directory>\groups\master.config` file.

Tasks

This section includes:

- "How to Configure the VMware Host Monitor" below
- "How to import the VMware Server Certificates" on page 744

How to Configure the VMware Host Monitor

1. Prerequisites

- The VMware Host monitors are optional SiteScope monitors that require additional licensing to enable the monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- The following are the requirements for monitoring VMware-based servers:
 - The monitored vCenter or ESX server must be directly accessible by the SiteScope server (no proxy involved).
 - The vCenter or ESX server provides a connection either by http or by https (depending on the vCenter or host server configuration). If https is used, server certificate must be imported to the SiteScope.

2. Import the server certificates (if the Web Server is configured to use SSL encryption)

If the Web server has an `https://` prefix, it is a secure, encrypted connection. You can use one of the following methods for importing server certificates, or disable the requirement of having to import untrusted or invalid SSL certificates.

- Import the server certificates either:
 - Directly from the monitor using SiteScope's Certificate Management. In the monitor settings panel, click the **Import Certificates**  icon (next to the **vCenter URL/Host URL** box) to open the Import Certificates dialog box, and select the server certificates to import. For details, see step 2 of How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
 - Manually import the server certificates. For details, see "How to import the VMware Server Certificates" on page 744.
- To use the monitor without having to import or check untrusted or invalid SSL certificates, set the `_vmWareConnectionAcceptAllUntrustedCerts` property to `=true` in the **master.config** file, and restart SiteScope. You must add this property when upgrading from older versions of SiteScope.

3. Configure the monitor properties

For each VMware host, you can:

- Create the monitor by deploying the VMware Host solution template (recommended). The template contains a predefined monitor set with optimized settings that allow you to monitor only the relevant components. For solution template details, see VMware Capacity Management Solution Templates in the Using SiteScope Guide.

- Create the monitor manually (for task details on creating a monitor, see [How to Deploy a Monitor in the Using SiteScope Guide](#)), and then configure the settings as specified in the step below.

To create the monitor manually:

- a. In the VMware Host Monitor Settings panel, enter the required vCenter or Host settings.
For monitor user interface details, see ["VMware Host Monitor Settings" on page 746](#).
- b. Click the **Get Counter** button, and select the counters you want to monitor from the Select Counters Form. The counters are added to the Preview tree in the **Patterns & Counters** section.
- c. For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
 - Clicking the **Add New Counter**  button to add an empty line to the table, and creating a pattern format using a regular expression.
 - The pattern should always start and end with the forward slash ("/") character.
 - [and] characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character).
 - Use ".*" to describe any character any number of times.

For example, `./*/VirtualMachine./*/cpu/usage.average\[\]/` displays `usage.average[]` counter for all VMs.

 - Selecting a static counter, and editing the counter to create a pattern format using a regular expression. For details on using regular expressions, see [Regular Expressions Overview](#).

Note: For details on the maximum number of counters that can be selected from the browsable tree and the maximum number of counters that can match the selected counter patterns when creating and updating dynamic monitors, see ["Troubleshooting and Limitations" on page 749](#). If the maximum number of counters that can be deployed is exceeded, an error is written to the **RunMonitor.log**.
- d. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counters Preview tree.
- e. Set the frequency for updating counters from the server, and then click **Verify & Save** or **Save** to save your settings. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- f. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.
For threshold user interface details, see [Threshold Settings in the Using SiteScope Guide](#).

Note: When configuring threshold settings for VMware Host monitors:

- The monitor **always(default)** counter configured in the **Good if** section of the monitor's properties means that the state of the monitor is good, unless one of the thresholds of any of the other counters is breached.
- The **countersinError** counter configured in the **Error if** section of the monitor's properties means that the state of the monitor is error if one of the other counters is unavailable.

4. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "VMware Host Monitor Topology" on page 738.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

5. Configure the connection pool mechanism - optional

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. We recommend setting the maximum size of total connections (the `_vmWareConnectionPoolMaxTotal` property in **Preferences > Infrastructure Preferences > Custom Settings** to the number of configured VM monitors in SiteScope, and letting the internal connection pool mechanism optimize itself.

For details, see "Connection Pool Settings" on page 737.

6. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the vCenter/Host service and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:

- The **SiteScope Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

If counters are in error, try to isolate and troubleshoot the problem using the SiteScope VMware Host Best Practices document, which is available from **<SiteScope root directory>\sisdocs\pdfs\SiteScope_VMware_Host_Best_Practices.pdf**.

For additional troubleshooting suggestions, see "Troubleshooting and Limitations" on page 749.

How to import the VMware Server Certificates

If the VMware server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate.

You can import the certificates either:

- Manually using the keytool method (see procedure below for details).
- Directly from the monitor using SiteScope's Certificate Management. Click the **Import Certificates**  icon in the monitor settings panel to open the Import Certificates dialog box, and select the server certificates to import. For task details, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.

To import server certificates manually:

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 **cacerts** file.

Note: The default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Therefore, you should create a copy of the **cacerts** file with a different name before SiteScope is upgraded or re-installed so that the file is not overwritten when new certificates are imported.

3. In SiteScope, select **Preferences > Certificate Management**, and click the **Reload Certificate List** button to reload the keystore certificates from the **cacerts** file. This enables you to manually reload keystore changes without having to restart SiteScope.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

VMware Host Monitor Settings

User interface elements are described below:

UI Element	Description
Connect by: vCenter	<p>Select this option when connecting using a vCenter, and enter the following settings:</p> <ul style="list-style-type: none">• vCenter URL. URL of the VMware vCenter infrastructure for the server you want to monitor. The format of the URL is: <protocol>://<server_name>/sdk where <protocol> is either http or https, and <server_name> is the name of the vCenter server. You can import the server certificates directly from the monitor using SiteScope's Certificate Management (click the Import Certificates icon), instead of importing certificates manually. <p>Note: If you get 'Error Code: 31008. Error getting counters' when SSL is used, navigate to Preferences > Infrastructure Preferences > General Settings, and select Accept untrusted SSL certificates.</p> <ul style="list-style-type: none">• Host name. Name of the ESX/ESXi host server you want to monitor.
Connect by: Host	<p>Select this option when connecting directly using a host server, and enter the URL (host name, not IP address) of the VMware ESX host server you want to monitor in the Host URL box.</p> <p>You can import the server certificates directly from the monitor using SiteScope's Certificate Management (click the Import Certificates icon), instead of importing certificates manually.</p>
Credentials	<p>User name and password required to access the VMware Web service or host server. Select the option to use for providing credentials:</p> <ul style="list-style-type: none">• Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box.• Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Host to take counters from	<p>When working in template mode, enter the name of the VMware host server from which to take counters.</p> <p>Note: This is available in Template mode only.</p>

UI Element	Description
<p>Patterns & Counters</p>	<p>Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.</p> <p>Click the Add New Counter  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the Delete Counter  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the View Matches for Selected Pattern  button to display counters that match the selected patterns.</p> <p>Note: SiteScope uses Perl regular expressions for pattern matching. For example, if you enter <code>/cpu.* /</code> or <code>cpu</code>, any counters with <code>cpu</code> in their name match this pattern and are added to the counters list.</p>
<p>Get Counters</p>	<p>Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.</p>
<p>Counters Preview</p>	<p>Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.</p>
<p>Frequency of updating counters from server</p>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p>Default value: 15 minutes</p> <p>Note:</p> <ul style="list-style-type: none"> • The update frequency cannot be less than the monitor run frequency in Monitor Run Settings. • When configuring this setting in a template, the variable value can only be in time units of seconds. • Static counters are never deleted.
<p>Continue displaying counters that no longer exist after update</p>	<p>Counters that no longer exist after running the update mechanism to retrieve counters from the VMware host server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful if a server goes down or for keeping track of what counters were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings.</p> <p>Default value: Selected</p>

For information on configuring setting panels that are common to all monitors, see Common

Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section includes:

- ["General Notes/Tips" below](#)
- ["Troubleshooting and Limitations" below](#)
- ["Troubleshooting Logs" on page 751](#)

General Notes/Tips

- SiteScope supports configurations with up to 2150 VMware Host monitors.
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).

Troubleshooting and Limitations

This section describes troubleshooting and limitations for VMware Host monitors.

- ["Maximum Number of Counters That Can be Saved" below](#)
- ["Incorrect ESX version displayed by the VMware Host State monitor" on the next page](#)
- ["Inaccurate Performance Analysis Using Perfmon to Monitor CPU on VMware " on the next page](#)
- ["Enable reporting Virtualization Layer Software CI when SiteScope is integrated with BSM 9.0x" on the next page](#)

Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the `_browsableContentMaxCounters` parameter in the `master.config` file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the `_maxCountersForRegexMatch` parameter in the `master.config` file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The `_maxCountersForRegexMatch` parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both `_browsableContentMaxCounters` and `_`

maxCountersForRegexMatch parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

Incorrect ESX version displayed by the VMware Host State monitor

The incorrect ESX version is returned by the vCenter and displayed by the VMware Host State monitor. When the VMware Host State monitor monitors ESX directly (not via vCenter), the ESX version is correct.

Inaccurate Performance Analysis Using Perfmon to Monitor CPU on VMware

Problem: SiteScope uses Perfmon to connect to the operating system of the VMware virtual machine and query it for CPU usage of the virtual host. When used over a period of time to monitor CPU on VMware, Perfmon provides inaccurate performance analysis.

Solution: VMware resolved this issue by integrating virtual machine performance counters such as CPU and memory into Perfmon for Microsoft Windows guest operating systems when VMware Tools is installed.

- For vSphere v4.0, install the latest version of VMware Tools from vSphere v4.0. When running the Windows perfmon utility, use the new counter groups, VM Processor and VM Memory, to see real CPU utilization.
- For VMs running on ESX/ESXi v3.5, contact VMware alliances for a standalone version of this Perfmon integration tool.

Use the VMware Host monitors to monitor the new counters groups to get accurate CPU utilization and memory data.

Enable reporting Virtualization Layer Software CI when SiteScope is integrated with BSM 9.0x

1. Update topology scripts.
 - a. In BSM 9.0x, select **Admin > RTSM Administration > Package Manager**, and export the **sitescope** package to a local directory. When the export process is complete, make a back up of the **sitescope.zip** file that is downloaded.
 - b. Extract the contents of **sitescope.zip** to a separate directory.
 - c. Extract the contents of **<SiteScope root directory>\conf\integration\bsm\BSM_90_VMWareHostMonitors.zip** to the **\discoveryScripts** folder of the directory used in the previous step (overwrite the existing script files).

Note: Make sure **sitescope.zip** consists only of the modified files under the **\discoveryScripts** folder.

- d. Archive the extracted structure. Make sure that the directory structure is the same as in the original file.
 - e. In BSM 9.0x, select **Admin > RTSM Administration > Package Manager**, and deploy the updated archive back to the server.
2. Update Indicator Assignments.

Perform the following steps for each of the 5 new monitors listed in the table below.

- a. In BSM, select **Admin > System Availability Management > Metrics and Indicators**, and click the **Select Monitor** button, and then click the **New Monitor** button.
- b. In the Add New Monitor dialog box, enter the display name, monitor class name, and category.

Monitor display name/Monitor topaz name	Monitor class name	Category
VMware Host CPU Monitor	VMwareHostCPUMonitor	Virtualization
VMware Host Memory Monitor	VMwareHostMemoryMonitor	Virtualization
VMware Host Network Monitor	VMwareHostNetworkMonitor	Virtualization
VMware Host State Monitor	VMwareHostStateMonitor	Virtualization
VMware Host Storage Monitor	VMwareHostStorageMonitor	Virtualization

- c. Import the **vmware host assignments.xml** file into the monitor indicator assignments.
- d. Restart the SiteScope integrated with the BSM 9.0x server.

Troubleshooting Logs

- Check for dynamic framework errors in:
 - **<SiteScope root directory>\logs\dynamic_monitoring_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
 - **<SiteScope root directory>\logs\dynamic_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).
- Check for VMware monitor errors in:
 - **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.
 - **<SiteScope root directory>\logs\vmware_connections.log**. This log provides information about the connection pool against the ESX/vCenter (get/return connection).
- Copy the following sections from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####
# Dynamic Monitoring
#####
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
false
```

```
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG,
dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFile
Appender
log4j.appender.dynamic.monitoring.appender.File=../${log.file.path}/dynamic_
monitoring.log
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.Pattern
Layout
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p -
%m%n

# Dynamic monitors changes category
log4j.category.DynamicMonitoringChanges=INFO,
dynamic.monitoring.changes.appender
log4j.additivity.DynamicMonitoringChanges=false

# VMware Connection Pool
#####
log4j.category.VMwareConnectionPool=${monitor.loglevel}, vmware.connection.pool.appender
log4j.additivity.VMwareConnectionPool=false
log4j.appender.vmware.connection.pool.appender=org.apache.log4j.RollingFileAppender
log4j.appender.vmware.connection.pool.appender.File=../${log.file.path}/vmware_
connections.log
log4j.appender.vmware.connection.pool.appender.MaxFileSize=${def.file.max.size}
log4j.appender.vmware.connection.pool.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.vmware.connection.pool.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.vmware.connection.pool.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p
- %m%n
```

Chapter 98

VMware Performance Monitor

This monitor enables you to monitor performance statistics of the VMware infrastructure for various server applications.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the VMware Performance monitor.

Learn More

This section includes:

- "VMware Performance Monitor Overview" below
- "Supported Versions" below
- "VMware Performance Monitor or VMware Host Monitor?" on the next page
- "SSL Connectivity" on page 756
- "VMotion Support" on page 756
- "VMware Performance Topology" on page 756
- "System Tuning for Loaded Environments" on page 760
- "Metrics Integration Support" on page 760

VMware Performance Monitor Overview

Use the VMware Performance monitor to monitor VMware-based servers. VMware supplies much of the virtualization software available for x86-compatible computers. The VMware Performance monitor supports monitoring:

- ESX host, VM, and resource pool monitoring (it is not recommended to monitor more than one VM and ESX on a single monitor).
- 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>

Tip: To benefit from performance improvements made to this monitor, configure the filter options (**Get real-time data only**, **Get VMs and Hosts in powered on state only**, **Virtual machine**, and **Host**) according to the recommendations in "How to Configure the VMware Performance Monitor" on page 764. For best practices details, see "Best Practices for Configuring the VMware Performance Monitor" on page 762.

Supported Versions

This monitor supports monitoring remote servers running on:

- VMware VirtualCenter 2.x
- VMware ESX 3.x, 4.0, 4.1
- VMware ESXi 3.5, 4.0, 5.0, 5.1
- VMware ESX 2.5 using VirtualCenter 2.x

- VMware ESX 3.x using VirtualCenter 3.x
- VMware vCenter Server 4.0, 4.1, 5.0, 5.1

Note: Monitoring VMware ESX(i) is not supported when Lockdown mode is enabled.

VMware Performance Monitor or VMware Host Monitor?

	VMware Performance Monitor	VMware Host Monitors
Type of user	VM user/owner	Virtualization administrator
Requirements	<ul style="list-style-type: none"> • Measure performance and availability of a particular VM or set of VMs. • Display SiteScope and BSM reports and BSM topology for this VM. <p>Usually, VM users/owners are not interested on which host the VM runs or other issues.</p>	<ul style="list-style-type: none"> • Manage a virtualization environment or vCenter and provide VM services to other users. • Measure the availability and performance of vCenter resources (physical host machines). <p>Usually, virtualization administrators are not interested in specific VMs (only if this machine causes performance issues to the host).</p>
Recommended Use	Monitoring one or a set of VMs	Deploy using VM Host solution template
Benefits	Measures the data every monitor run regardless of whether the VM has migrated.	<ul style="list-style-type: none"> • Enables the administrator to make most efficient use of host resources (create maximum VMs and serve more users). • Provides notifications of availability and performance problems on the host (that might be caused by specific VM or VMs). • The monitor is dynamically updated (see "Dynamic Monitoring Mechanism" on page 735). • Smart counters provide useful information for configuring the VM on the host to help maximize resource usage. For details, see "Calculated (Smart) Counters" on page 736.

	VMware Performance Monitor	VMware Host Monitors
<p>Data in SiteScope and BSM Reports</p>	<p>Provides user with SiteScope and BSM reports with continuous data and topology that match the changes (the same VM connects to the relevant host).</p>	<ul style="list-style-type: none"> • Enables the administrator to check host information only (the data is continuous). The topology matches VM migration for the monitored hosts. • Does not provide continuous data on the VM (every time a VM migrates from host to host, its ID changes in SiteScope and BSM reports). However, VM data does not interest the administrator.

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. For details on how to perform this task, see "How to import the VMware Server Certificates" on page 765.

VMotion Support

VMware's VMotion technology enables transparent migration of running virtual machines between physical hosts in a virtual infrastructure cluster. It enables you to move an entire running virtual machine instantaneously from one server to another with continuous service availability and zero downtime. This process can be done both manually and automatically as part of cluster load balancing.

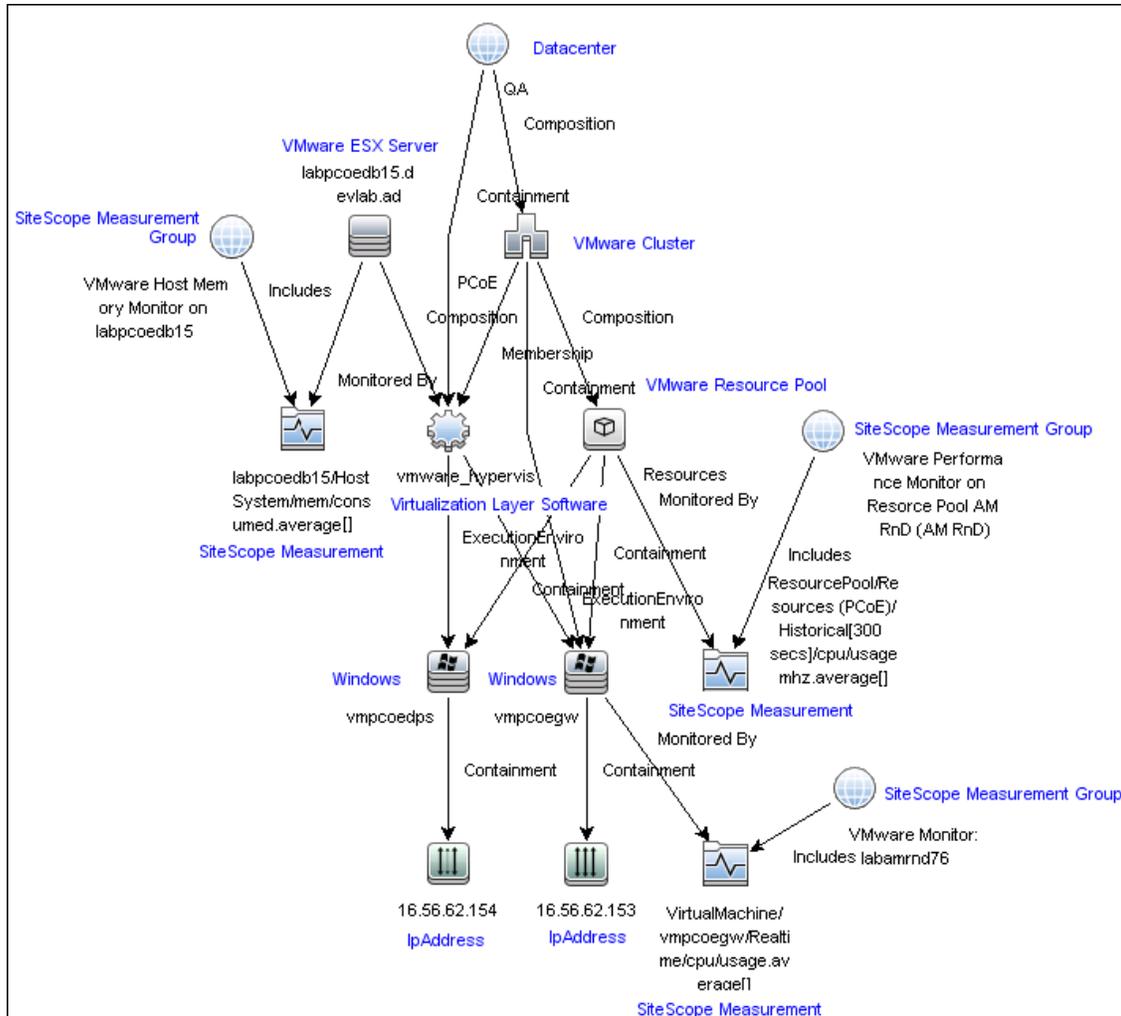
The VMware Performance monitor is browsable, and the counters tree is designed so that virtual machine nodes are not children of physical host nodes. This means that the structure of the tree does not change during migration and if counters from a virtual machine are selected for this monitor, they do not change as a result of VMotion. This is regardless of where the virtual machine belonged at any particular moment.

You can set the interval for checking topology changes on the server in **HP Integration Settings > BSM Integration Data and Topology Settings**. Each time the monitor is run or updated, if the specified time since the last such server check has passed, the monitor checks the target server to see if migration of the monitored VMs has occurred.

VMware Performance Topology

The VMware Performance monitor can identify the topology of the VMware servers being monitored. The monitor creates the following topology in BSM's RTSM.

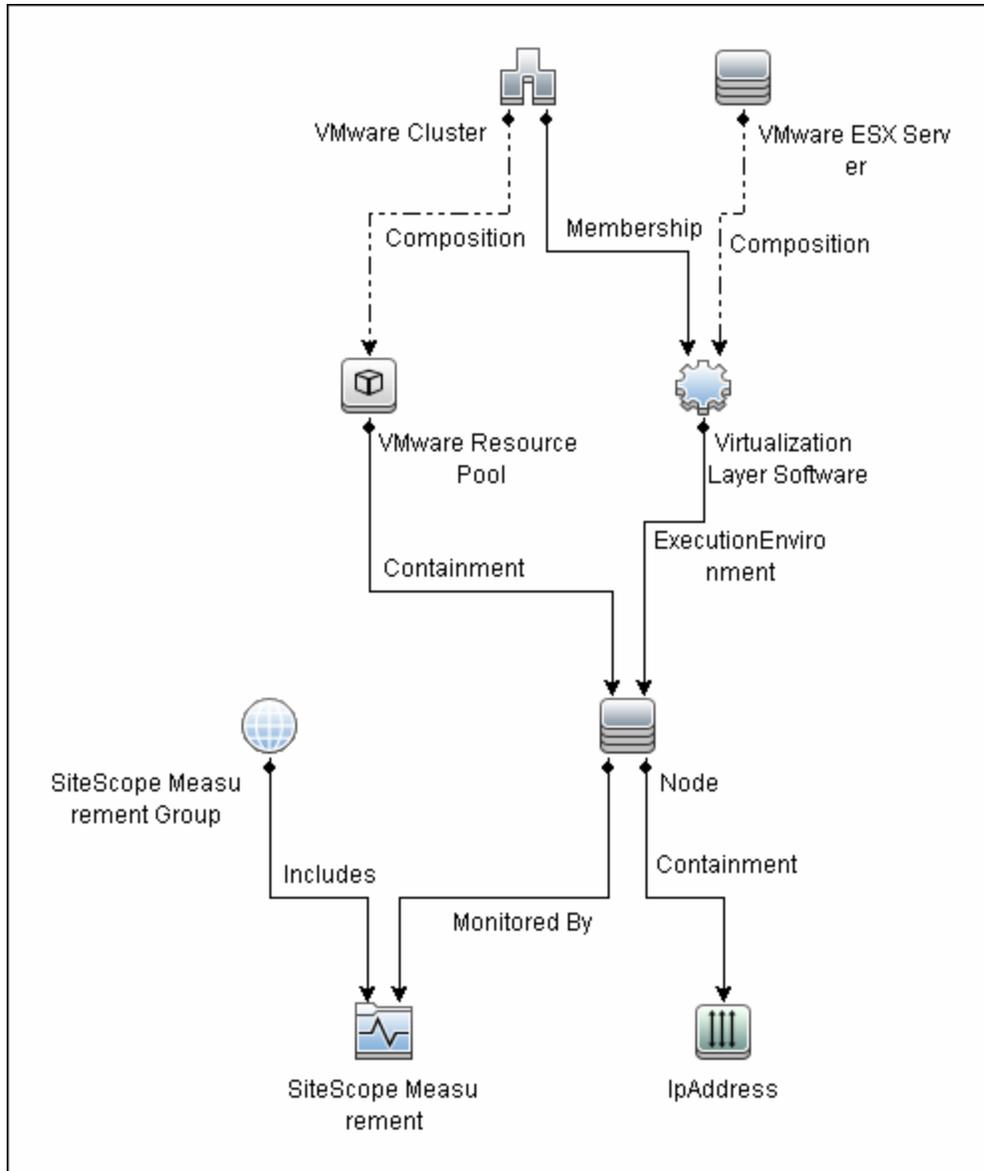
The VMware Performance monitor reports the Node CI for the virtual machine (VM) and the VMware ESX Server CI (ESX), and reports the connection between the VM and ESX. If there is counter defined on the VM, the related ESX and resource pool are also reported.



Note: When deleting a monitor or making configuration changes, links between previously reported VMs and ESXs are not deleted. This means that if a monitor was deleted and relevant VMs were subsequently migrated, the newly-created monitor contains the old link to the previous ESX Server and a link to the current ESX Server (reported on monitor creation).

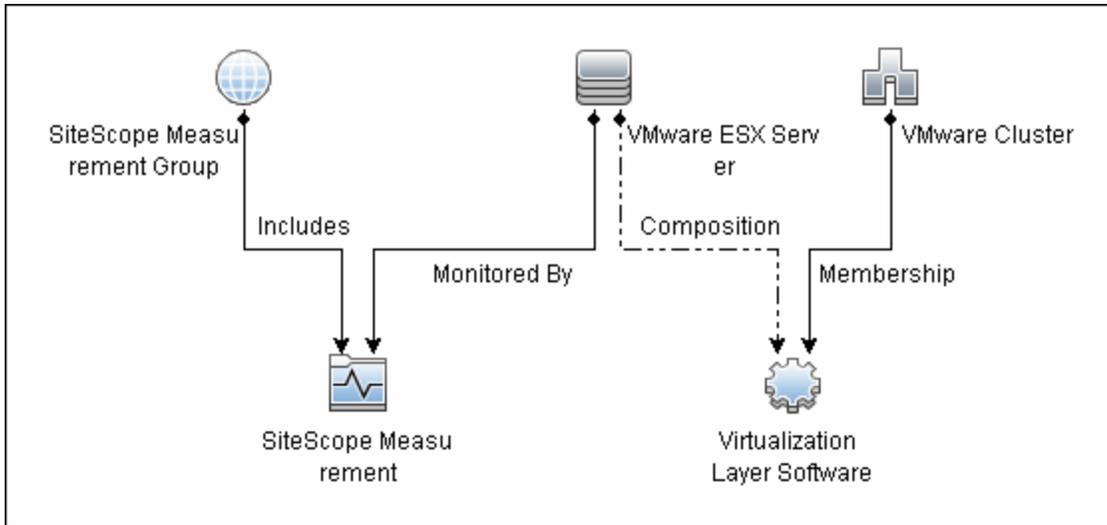
Cluster to Virtual Machine

The VMware Performance monitor reports topology for the VMware Cluster to the VM.



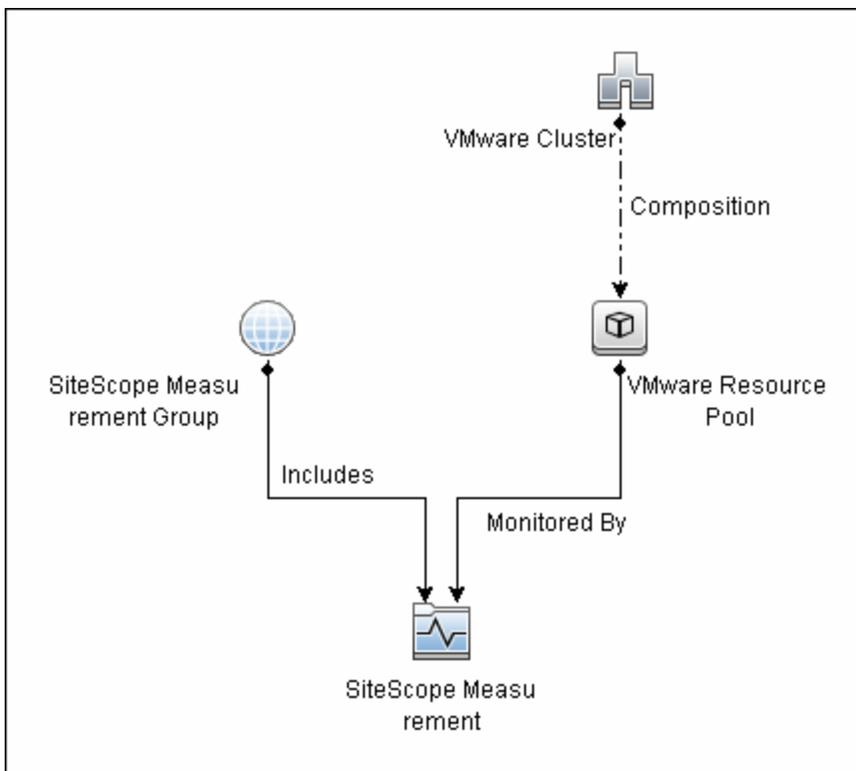
Cluster to ESX Server

The VMware Performance monitor reports topology for the VMware Cluster to the ESX Server.



Cluster to Resource Pool

The VMware Performance monitor reports topology for the VMware Cluster to the VMware Resource Pool.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

System Tuning for Loaded Environments

SiteScope installed on a 64-bit environment supports configurations with up to 2150 VMware Performance monitors running concurrently. This loaded system can be integrated with BSM and OM metrics.

To support loaded environments, the following system tuning is required:

- SiteScope sizing is required to increase JVM heap size, desktop heap size, and the number of file handles. You can use the SiteScope Configuration Tool to size SiteScope. For details, see Using the SiteScope Configuration Tool in the HP SiteScope Deployment Guide.
- Add the **_runGCPeriod=1200000** property to the **<SiteScope root directory>\groups\master.config** file. This means that SiteScope initiates running the garbage collector every 20 minutes (1200000 milliseconds) for better performance.
- Tune the following vCenter/ESX connections parameters in the **<SiteScope root directory>\groups\master.config** file, as required:
 - **_vmWareConnectionPoolMaxIdlePervCenterKey=**
 - **_vmWareConnectionPoolMaxSizePervCenterKey=**
 - **_vmWareConnectionPoolMaxTotal=**
 - **_vmWareConnectionTimeOut=**
- Increase the number of dynamic monitors handles in **Preferences > Infrastructure Preferences > Dynamic Monitoring Settings**:
 - **Dynamic monitoring core thread pool size: 50**
 - **Dynamic monitoring maximum thread pool size: 70**

Metrics Integration Support

SiteScope uses the HP Operations agent to make metrics data from the VMware Performance monitor available to HP Performance Manager in HPOM and to Performance Graphing in BSM.

The reported metrics are associated with the relevant resource: ESX host, VM, or Resource Pool. The target is the counter target (not the monitor target).

Monitor Type	Reports Metrics For	Reports Metrics to the Following Tables
VMware Performance	ESX	VMware Host CPU, Memory, Storage, State, Network, System tables
	VM	VMware VM CPU, Memory, Storage, State, Network, System tables
	Resource Pool	VMware Resource Pool table

Note:

- The first time you start monitoring a new VM or ESX host, it takes more time to get the data and to view it in the HP Operations agent.

- The VMware Performance monitor supports the following metrics types only: CPU, disk, memory (mem), network (net), state and sys (system). All other metrics types are currently not supported, including general metrics such as `usageToPresevationRelation` and `usageToLimitRelation` metrics.
- By default, the VMware Performance monitor sends each metric to a specific table with its ESX host server, VM, or resource pool target, according to its data type. To revert back to the old behavior where the monitor sends all metrics to one table, clear the **Report VMware Performance monitor metrics to OA metrics classes** check box in **Preferences > Infrastructure Preferences > Monitor Settings**. You can also modify this setting in the `<SiteScope root directory>\groups\master.config` file by changing the `_omReportNewVmwareMetricClasses` property value to `=false`.
- To support motion and changes in the vCenter, such as change of IP or host name, you can change the interval for updating the data saved to the cache in the **Frequency of VM configuration retrieval from vCenter (hours)** field in **Preferences > Infrastructure Preferences > Monitor Settings**. By default, data is updated every 4 hours. You can also configure this by modifying the `_vmwareRetrieveConfFrequencyHours` property in the `<SiteScope root directory>\groups\master.config` file.

Best Practices

Best Practices for Configuring the VMware Performance Monitor

To benefit from performance improvements made to the VMware Performance monitor, you should configure the monitor filtering options and the connection pool settings according to the best practices below.

This section includes:

- "Filtering Options" below
- "Connection Pool Settings" below

Filtering Options

To reduce monitor load on the VMware Performance monitor, it is important to use the appropriate filtering settings when configuring the monitor settings. If filtering options are not used, the monitor is placed under enormous load as it creates an XML file with all the counters retrieved. This causes performance problems each time monitor properties are opened, since the monitor attempts to display a large number of counters and create a heavy cache file.

When configuring the monitor, you should:

- Enter a virtual machine and host name in the **Virtual machine** and **Host** fields. If these fields are not filled, the monitor attempts to retrieve counters for all VMs, hosts, and resource pools defined in the vCenter. For example, if a vCenter has 800 VMs and 100 hosts, the monitor will try to get 80 counters per VM and 90 counters per host (this is the average number - the actual number depends on the configuration of the VM or host and may be even higher). In total: $(800 \text{ VMs} \times 80 \text{ counters}) + (100 \text{ Hosts} \times 90 \text{ counters}) = 73,000 \text{ counters}$.
- Make sure that the **Get real-time data only** option is selected (it is selected by default) so that historical data is not included. The number of counters above represents real-time data only. This number could be much higher, depending on your configuration, if historical data is not excluded.
- To avoid retrieving historical data from powered off VMs and hosts, make sure that the **Get VMs and Hosts in powered on state only** option is selected (it is selected by default).

For details on configuring filtering options, see "[How to Configure the VMware Performance Monitor](#)" on page 764.

Connection Pool Settings

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. The connection pool is a set of pools per key. A key is the combination of a vCenter or host URL, and a user (the connection cannot be shared between different users due to different permissions).

If all VMware Performance monitors are configured with the same vCenter URL and user, one connection pool is created. For two vCenters and two different users for every vCenter, four connection pools are created.

The connection pool configures itself over time to ensure that only working connections stay in the pool. It does this by running an additional thread at the rate of the connection timeout multiplied by

two; if the connection timeout is 30 minutes, it will run once every hour and evict idle connections from the pool. Connections that are idle for more than half a minute before the connection timeout are eligible for eviction.

For example, if the connection timeout is 30 minutes, the thread will evict connections that were idle for more than 29.5 minutes, but less than 30 minutes (to avoid a connection timeout). As a result, only working connections stay in the pool.

You can configure the following connection pool properties in **<SiteScope root directory>\groups\master.config**:

- **_vmWareConnectionPoolMaxIdlePervCenterKey**. The maximum number of idle connections in the pool. The default value is 60.
- **_vmWareConnectionPoolMaxSizePervCenterKey**. The maximum number of active connections in the pool. The default value is 60.

Note: If a SiteScope is registered to BSM, it uses more connections to retrieve properties relevant for topology reporting. Therefore, you should increase the maximum number of idle and active connection properties to enable SiteScope to perform well.

- **_vmWareConnectionPoolMaxTotal**. Maximum size of total connections for all keys. This is the total number of connections used in all the defined SiteScope vCenters. The default value is 1500.

Tip: We recommend setting the maximum size of total connections to the number of configured VM monitors in SiteScope, and let the internal connection pool mechanism optimize itself.

- **_vmWareConnectionTimeOut**. Connection timeout in minutes. The default value is 30 minutes.

Tasks

This section includes:

- "How to Configure the VMware Performance Monitor" below
- "How to import the VMware Server Certificates" on the next page

How to Configure the VMware Performance Monitor

1. Prerequisites

The following are the requirements for monitoring VMware-based servers:

- The monitored vCenter or ESX server must be directly accessible by the SiteScope server (no proxy involved).
- The vCenter server or ESX server provides connection either by http or by https (depending on the vCenter/host server configuration). If https is used, server certificate must be imported to the SiteScope.

2. Import the server certificates (if the Web Server is configured to use SSL encryption)

If the Web server has an `https://` prefix, it is a secure, encrypted connection. You can use one of the following methods for importing server certificates, or disable the requirement of having to import untrusted or invalid SSL certificates.

- Import the server certificates either:
 - Using Certificate Management in SiteScope (avoids having to restart SiteScope). For details, see step 2 of How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
 - Manually import the server certificates. For details, see "How to import the VMware Server Certificates" on the next page.
- To use the monitor without having to import or check untrusted or invalid SSL certificates, set the `_vmWareConnectionAcceptAllUntrustedCerts` property to `=true` in the `master.config` file, and restart SiteScope. You must add this property when upgrading from older versions of SiteScope.

3. Configure the monitor properties

To benefit from performance improvements made to this monitor, configure the monitor according to the recommendations below. For best practices details, see "Best Practices for Configuring the VMware Performance Monitor" on page 762.

- a. Create a separate monitor for each VM or host. (This is because the monitor is limited to monitoring 100 counters, and every VM or host has an average of 80-90 counters.)

For task details on adding a monitor, see How to Deploy a Monitor in the Using SiteScope Guide.

- b. Configure the following filter options to avoid overloading the monitor:

For Virtual machine:

- **Get real-time data only:** Selected
- **Get VMs and Hosts in powered on state only:** Selected
- **Host:** /--/
- **Virtual machine:** < Enter VM name>

For Host:

- **Get real-time data only:** Selected
- **Get VMs and Hosts in powered on state only:** Selected
- **Host:** <Enter host name>
- **Virtual machine:** /--/

- c. Configure the other monitor properties as required.

For user interface details, see the UI Descriptions section below.

4. **Enable topology reporting - optional**

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "VMware Performance Topology" on page 756.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

5. **Configure the connection pool mechanism - optional**

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. We recommend setting the maximum size of total connections (the `_vmWareConnectionPoolMaxTotal` property in **Preferences > Infrastructure Preferences > Custom Settings** to the number of configured VM monitors in SiteScope, and letting the internal connection pool mechanism optimize itself.

For details, see "Connection Pool Settings" on page 762.

How to import the VMware Server Certificates

If the VMware server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate.

You can import the certificates either:

- Manually using the keytool method (see procedure below for details).
- Directly from the monitor using SiteScope's Certificate Management. Click the **Import Certificates**  icon in the monitor settings panel to open the Import Certificates dialog box, and select the server certificates to import. For task details, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.

To manually import server certificates:

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 **cacerts** file.

Note: The default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Therefore, you should create a copy of the **cacerts** file with a different name before SiteScope is upgraded or re-installed so that the file is not overwritten when new certificates are imported.

3. In SiteScope, select **Preferences > Certificate Management**, and click the **Reload Certificate List** button to reload the keystore certificates from the **cacerts** file. This enables you to manually reload keystore changes without having to restart SiteScope.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

VMware Performance Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
URL	<p>URL of the VMware infrastructure for the server you want to monitor.</p> <p>The format of the URL is: <protocol>://<server_name>/sdk</p> <p>where <protocol> is either http or https, and <server_name> is the name of the ESX server.</p> <p>Note: If you get 'Error Code: 31008. Error getting counters' when SSL is used, navigate to Preferences > Infrastructure Preferences > General Settings, and select Accept untrusted SSL certificates.</p>
Credentials	<p>User name and password required to access the VMware Web service. Select the option to use for providing credentials:</p> <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Get real-time data only	<p>Select to retrieve real-time metrics data only and exclude historical metrics data.</p> <p>Default value: Selected</p>
Get VMs and Hosts in powered on state only	<p>Select to retrieve metrics data from powered on VMs and hosts only (data from powered off VMs/hosts is excluded).</p> <p>Default value: Selected.</p>
Host	<p>Enter a regular expression to match the name of one or more hosts. Only hosts that match this expression are displayed in the Counters list. Click the Open Tool button to use the Regular Expression tool to check the correctness of your regular expression.</p>

UI Element	Description
Virtual machine	Enter a regular expression to match the name of one or more virtual machines. When you apply this filter, only the virtual machines that match this string are displayed in the Get Counters list. Click the Open Tool button to use the Regular Expression tool to check the correctness of a regular expression.
Counter Settings	
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

HP Integration Settings (for VMware Performance Monitor)

The setting below is specific to the VMware Performance monitor. For HP Integration Settings common to all monitors, see HP Integration Settings in the Using SiteScope Guide.

UI Element	Description
BSM Integration Data and Topology Settings	
Interval to check server for topology changes (minutes)	Each time the monitor is run or updated, if the specified time since the last such server check has passed, the monitor checks the target server to see if migration of the monitored VMs has occurred. If it has, it updates the relationship of monitored VMs to the ESX servers on which they are running. Default value: 60 minutes

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

This section includes:

- "General Notes/Tips" below
- "Troubleshooting and Limitations" below

General Notes/Tips

- For VMware Performance monitors that were configured in earlier versions of SiteScope, the **Get real-time data only** and **Get VMs and Hosts in powered on state only** options are not selected by default.
- When deploying this monitor using a template, clearing the **Verify monitor properties with remote server** option deploys the monitor without connecting to the server, thereby enabling template deployment on powered on and powered off VMs. When this option is selected (the default setting), deployment fails for VMs that are not powered on.
- The CPU shares counter in the resource pool (**Resource Pool > summary > config > cpuAllocation > shares > shares**) displays a value of 0 instead of the actual number of shares allocated if level is not set to custom on the VMware server. For more details, see the VMware support site (<http://www.vmware.com/support/developer/vc-sdk/visdk41pubs/ApiReference/vim.SharesInfo.html>).

Troubleshooting and Limitations

This section contains the following troubleshooting issues:

- "Counter Errors After SiteScope Upgrade" below
- "Inaccurate Performance Analysis Using Perfmon to Monitor CPU on VMware" below

Counter Errors After SiteScope Upgrade

If you encounter errors retrieving the counters after upgrading from an earlier version of SiteScope, you should re-install the server certificate as follows:

1. Create a backup of the **cacerts** file in a directory outside of the SiteScope directory. The **cacerts** file is located in the **<SiteScope root directory>java\lib\security** folder.
2. Remove the **cacerts** file from the SiteScope folder.
3. Restart the SiteScope server.
4. Create a new **cacerts** file with the new certificate.

Inaccurate Performance Analysis Using Perfmon to Monitor CPU on VMware

Problem: SiteScope uses Perfmon to connect to the operating system of the VMware virtual machine and query it for CPU usage of the virtual host. When used over a period of time to monitor CPU on VMware, Perfmon provides inaccurate performance analysis.

Solution: VMware resolved this issue by integrating virtual machine performance counters such as CPU and memory into Perfmon for Microsoft Windows guest operating systems when VMware Tools is installed.

Monitor Reference

Chapter 98: VMware Performance Monitor

- For vSphere v4.0, install the latest version of VMware Tools from vSphere v4.0. When running the Windows perfmon utility, use the new counter groups, VM Processor and VM Memory, to see real CPU utilization.
- For VMs running on ESX/ESXi v3.5, contact VMware alliances for a standalone version of this Perfmon integration tool.

Use the VMware Performance monitor to monitor the new counters groups to get accurate CPU utilization and memory data.

Chapter 99

Web Script Monitor

The Web Script monitor provides 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.

Note: The Web Script monitor is an optional SiteScope monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. Contact your HP sales representative for more information.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Web Script monitor.

Learn More

This section includes:

- ["Web Script Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Counter Measurements and Transaction Breakdown Data" below](#)
- ["Working with VuGen" on the next page](#)
- ["Advanced Information" on page 776](#)
- ["Web Script Performance Counters" on page 776](#)

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.

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 use a back-end database).

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. For information on working with VuGen, see ["Web Script Monitor" on the previous page](#).

Note to BSM users: The Web Script monitor is not available when working in BSM. The monitor's data cannot be reported to BSM.

Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows versions only.
- This monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.

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.

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 the counter metrics available for the monitor, see ["Web Script Performance Counters" on page 776](#).

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 11.0 and earlier.

This section also includes:

- ["Getting Started" below](#)
- ["Supported VuGen Protocols" on the next page](#)
- ["Inserting Transactions and Creating Checkpoints" on page 775](#)
- ["Saving and Storing the Script" on page 775](#)

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 HP Virtual User Generator guide.

For more detailed information on creating scripts, refer to "Working with VuGen" > "Recording with VuGen" > "Creating New Virtual User Scripts" in the HP Virtual User Generator guide.

Supported VuGen Protocols

The following are the protocols supported for the Web Script monitor when VuGen scripts are invoked by SiteScope:

- ["Web \(Click and Script\) Protocol" below](#)
- ["Web \(HTTP/HTML\) Protocol" below](#)

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 user interface-level scripting API, and a quicker way to create scripts.

- Easy-to-use scripting.
- Intuitive API functions describe user actions on Web objects (for example, button and text link).
- 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 HP Virtual User Generator guide.

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.
- Recording of an application in a specific language (for example, French, Japanese) must be performed on a machine whose default locale (in **Control Panel >Regional Options**) is the same language.

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 HP Virtual User Generator 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 HP Virtual User Generator 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 HP Virtual User Generator guide.

- VuGen's Content Check mechanism enables you to check the contents of a page for a specific string. This is useful for detecting non-standard errors. We recommend 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 HP Virtual User Generator guide.

Saving and Storing the Script

The script you create in VuGen must be saved as a zip file. We recommend saving only the runtime files. For details, refer to the "Recording with VuGen" and "Using Zip Files" sections of the HP Virtual User Generator guide.

When saving the zip file:

- make sure that the zip file has the same name as the script
- make sure 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 drop-down list of available scripts 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 (**Preferences > General Preferences > General Settings**). The scripts stored in the location you enter appear in the drop-down list of available scripts when configuring the monitor.

- Any other location accessible to the SiteScope machine.

When configuring the monitor, you can also enter 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.

Advanced Information

The Web Script monitor uses an internal engine to run the VuGen scripts you create. This section includes some advanced issues.

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.

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	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. Retry time only relates to HTTP or TCP errors that execute a retry after the error.
DNS Time	Displays the average amount of time needed to resolve the DNS name to an IP address, using the closest DNS server. The DNS Lookup measurement is a good indicator of slow DNS resolution or other problems with the DNS server.
Connection Time	Displays the amount of time needed to establish an initial connection with the Web server performing the transaction. The connection measurement is a good indicator of problems along the network or whether the server is responsive to requests.

Name	Description
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>
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	<p>Displays the time during the script run when the client is not sending or receiving data from the server.</p>
Duration	<p>The time in milliseconds for the transaction to be run.</p>
Status	<p>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.</p>
Size	<p>The size in bytes received from the Web sites being monitored by the transaction.</p>
Number of Errors	<p>Number of errors that occurred during the transaction run.</p>

Monitor Reference

Chapter 99: Web Script Monitor

Name	Description
Number of Pages	Number of pages accessed when running the transaction.

Tasks

How to Configure the Web Script Monitor

1. Create a script using Virtual User Generator (VuGen)

Prior to configuring the Web Script monitor in SiteScope, you must create the script in VuGen.

- a. Download HP Virtual User Generator (VuGen).

Go to the [HP Software Support](http://www.hp.com/go/hpssoftwaresupport) site (<http://www.hp.com/go/hpssoftwaresupport>) and click the **Downloads** tab. Then click **Software patches**, and enter your HP user name and password to access the Software Patches page. 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 on 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.

- b. 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 contains different access points for getting help. For details, see ["Getting Started" on page 773](#) in ["Web Script Monitor" on page 771](#).

- c. Use the supported protocols in HP Virtual User Generator to create your script.

Tip: We recommend that you 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 774](#) in ["Web Script Monitor" on page 771](#).

- d. 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. 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 HP Virtual User Generator guide.

Checkpoints are recommended for checking contents of a page for a specific string while running the VuGen script. This is useful for detecting non-standard errors. For details on checkpoints, refer to the ["Checking Web Page Content"](#) and ["Verifying Web Pages under Load"](#) sections under ["E-Business Protocols"](#) in the HP Virtual User Generator guide.

- e. 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 775](#) in ["Web Script Monitor" on page 771](#).

- f. Make sure that the script runs properly in VuGen before continuing.

For details, refer to ["Working with VuGen" > "Running Vuser Scripts in Standalone Mode"](#) in the HP Virtual User Generator guide.

2. Create the monitor and configure the monitor properties.

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Web Script Monitor Settings

User interface elements are described below:

UI Element	Description
Web script URL	<p>Select from the following options:</p> <ul style="list-style-type: none">• 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 VuGen scripts path root in General Preferences. For details, see General Settings in the Using SiteScope Guide.• Full path Web script name. Enter the full path for the VuGen script. The script must be a <code>.zip</code> file and the path must be a location to which the machine running SiteScope has file system access. <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.
Web script timeout (seconds)	<p>Amount of 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> <p>Default value: 60 seconds</p>
Counters	<p>Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters.</p>

UI Element	Description
<p>Get Counters</p>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters available for the monitor, see "Web Script Performance Counters" on page 776.</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:</p> <ul style="list-style-type: none"> • Not all counters return values for all transactions. • When working in template mode, the maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Web Script monitor.

- 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.

- 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 HP Virtual User Generator 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, we recommend 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 (sec)** value in the monitor settings.
- By default, the number of Web Script monitors that can run simultaneously is 20. When this number is exceeded, SiteScope places the rest in a queue to await execution. You can change the number of monitors that can run simultaneously by modifying the **Web Script monitor queue size** in **Preferences > Infrastructure Preferences > Monitor Settings**. The maximum number of Web Script monitors that can run simultaneously is 40. You can also change the amount of time for the monitor to wait in the queue before timing out by modifying the **Web Script monitor queue timeout (seconds)** property. The default queue timeout is 120 seconds.
- The Web Script monitor supports script names with English characters only.
- The Web Script monitor is not available when working in BSM and cannot be configured in System Availability Management. The monitor's data cannot be reported to BSM or HPOM.

Chapter 100

Web Server Monitor

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. 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 in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Web Server monitor.

Tasks

[How to Configure the Web Server Monitor](#)

Configure the monitor properties as described in the UI Descriptions section below.

[Related workflow](#)

[How to Deploy a Monitor in the Using SiteScope Guide](#)

UI Descriptions

Web Server Monitor Settings

User interface elements are described below:

UI Element	Description
Server	<p>Name of the server where the Web server instance you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server.</p> <p>Note: If SiteScope is installed on a Windows platform, this monitor can monitor a target Windows server that has a Web Server installed on it. If SiteScope is installed on a UNIX platform, this monitor can monitor local log files only (monitoring a Web Server on UNIX platforms is no longer supported).</p> <p>Note when working in template mode: You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p>Default value: SiteScope Server (the server on which SiteScope is installed)</p>
Browse Servers	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to select the server to be monitored:</p> <ul style="list-style-type: none">• Browse servers. Select a server from the drop-down list of Windows servers visible in the local domain.• Enter server name. 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 Servers, enter the IP address or name of the server to monitor. <p>Note:</p> <ul style="list-style-type: none">• This button is available for SiteScope running on Windows platforms only.• To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.
Add Remote Server	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p>Note: This button is available for SiteScope running on Windows platforms only.</p>

UI Element	Description
Web server	<p>Web server type for the selected Web server.</p> <p>Default value: Microsoft IIS</p> <p>Note: This field is available for SiteScope running on Windows platforms only.</p>
Log file path	<p>For SiteScope running on Windows platforms: Select the Web Server from the list. If your Web server does not appear in the list, enter the full path to the Web server log file.</p> <p>For SiteScope running on UNIX platforms: Enter the full path of the Web server log file.</p> <p>Example: <code>c:/ns-home/httpd-test/logs/access</code></p> <p>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.</p>
Request size column	<p>Enter the column number which contains the Request Size if your Web server saves information in a custom format.</p> <p>If this item is blank, the common log file format is assumed.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

Chapter 101

Web Service Monitor

The Web Service monitor enables you 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.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Web Service monitor.

Learn More

This section includes:

- "Web Service Monitor Overview" below
- "Supported Platforms/Versions" below
- "Support for IPv6 Addresses" on the next page
- "Status" on the next page
- "Integration with Business Service Management for SOA" on page 792
- "Web Service Topology" on page 792

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/) (<http://www.w3.org/TR/SOAP/>).

For information about WSDL, refer to the [Microsoft site](http://msdn2.microsoft.com/en-us/library/ms996486.aspx) (<http://msdn2.microsoft.com/en-us/library/ms996486.aspx>).

Supported Platforms/Versions

The following specification features are currently supported:

- WSDL 1.1, 2.0
- SOAP 1.1, 1.2
- 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: 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>
```

Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

Status

The status reading shows the most recent result for the monitor. It is also recorded in the SiteScope log files, email 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

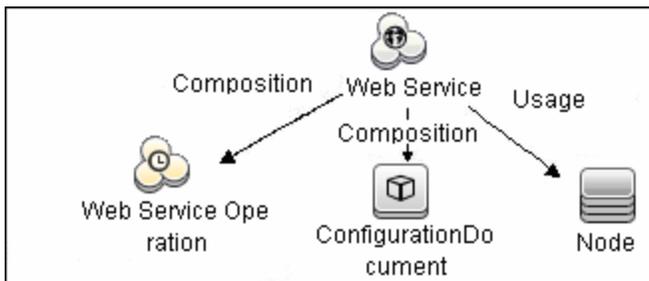
The final status result is either `OK`, `error`, or `warning` based on the threshold established for these conditions.

Integration with Business Service Management for SOA

If SiteScope is reporting to BSM, the monitor sends SOA samples, in addition to the regular samples it sends, for use in BSM for SOA. If the logging setting in **HP Integration Settings** is set to **Disable reporting metrics to BSM**, the monitor does not send any samples to BSM.

Web Service Topology

The Web Service monitor can identify the topology of the Web Service being monitored. If **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting), the monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

For information about the SOA topology, see SOA Views and Their Components in the BSM User Guide in the BSM Help.

Tasks

How to Configure the Web Service Monitor

1. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

2. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "[Web Service Topology](#)" on the previous page.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

Tip: The **Web Service Tool** is available when configuring this monitor to test the availability of SOAP enabled Web Services (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Web Service Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

Web Service Monitor Settings

User interface elements are described below:

UI Element	Description
WSDL Settings	
WSDL location	Select one of the following options: <ul style="list-style-type: none">• File. Select the WSDL file to be used for this monitor. This list reflects the files found by searching on <SiteScope root directory>\templates.wsdl/*.wsdl.• URL. Enter the URL of the WSDL file to be used for this monitor. Your WSDL files must have the extension .wsdl.
Get Data	Retrieves the specified WSDL file and analyzes it for method arguments. The ensuing page displays the measurements available for monitoring.
Service name	Name of the service to be invoked. During initial setup, this is extracted from the WSDL file.
Port name	Name of the port to be invoked. During initial setup, this is extracted from the WSDL file.
Method name	Name of the method to be invoked. During initial setup, this is extracted from the WSDL file.
Method name space	XML name space for the method in the SOAP request. During initial setup, this value is extracted from the WSDL file.
Schema name space	XML name space for the schema in the SOAP request. During initial setup, this value is extracted from the WSDL file.
SOAP action	SOAP action URL in the header of the SOAP request to the Web Service. During initial setup, this is extracted from the WSDL file.

UI Element	Description
<p>Name of arguments</p>	<p>Displays the name and type/structure of the arguments to the method specified above. SiteScope supports both simple (primitive) and complex (user-defined using XML schema) types.</p> <p>Simple type arguments appear in the form: <code>parm-name (parm-type) =</code></p> <p>where you need to enter the parameter value to be used in invoking the Web service after the equal sign. Strings with embedded spaces should be enclosed in double quotes. Each parameter must be in a separate line, that is, do not remove the carriage return at the end of each parameter.</p> <p>A complex type parameter is displayed as one long string, with needed input fields marked with asterisks (***) . An example of a complex type parameter is shown below:</p> <pre>stocksymbol[COMPLEX] =<stocksymbol xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:so- apenc="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">***</ticker></stocksymbol></pre> <p>You must replace these occurrences of asterisks with meaningful values of the required type (in the example above, <code>xsd:string</code>), otherwise the Web service request may fail. Do not add any carriage returns within a complex type parameter.</p> <p>If the Web service method does not take any parameters, the text box must be empty.</p> <p>Note: SiteScope cannot set the order of arguments. If the order is important, enter arguments in the same order in which they appear in the WSDL file.</p>
<p>Use user-defined SOAP XML</p>	<p>Uses the XML in the User SOAP XML box. This enables you to use XML that has been manually defined.</p>
<p>User SOAP XML</p>	<p>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.</p>
<p>Main Settings</p>	
<p>Request's schema</p>	<p>The request schema. Currently SiteScope only supports SOAP.</p>

UI Element	Description
Timeout (seconds)	<p>Amount of time, in seconds, that SiteScope should wait for the Web service request to complete.</p> <p>Default value: 30 seconds</p>
Use .NET SOAP	Select if the Web service is based on Microsoft .NET.
Content match	<p>Text string 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/ or /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:</p> <ul style="list-style-type: none"> • The search is case sensitive. • Content match behavior was changed for the Web Service monitor in SiteScope 10.12. To enable Web Service monitors defined prior to SiteScope 10.12 to match the correct value, the Web Service Monitor use common content match setting must be selected in Preferences > Infrastructure Preferences > Monitor Settings.
HTTP Settings	
Web service server URL	Displays the URL of the Web service server to be monitored.
HTTP user agent	HTTP user agent for the SOAP request.
HTTP content type	Content type of the HTTP request.
Proxy Settings	
HTTP proxy	Domain name and port of an HTTP Proxy Server if a proxy server can be used to access the URL.

UI Element	Description
Proxy server user name	Proxy server user name if required to access the URL. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Proxy server password	Proxy server password if required to access the URL. Note: Your proxy server must support Proxy-Authentication for these options to function.
Login Settings	
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).
Author-ization user name	Authorization user name if the web service requires a user name and password for access (Basic, Digest, or NTLM authentication). Alternately, you can leave this entry blank and enter 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.
Author-ization password	Authorization password if the web service requires a user name and password for access (Basic, Digest, or NTLM authentication). Alternately, you can leave this entry blank and enter 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.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 102

WebLogic Application Server Monitor

The WebLogic Application Server monitor enables you to monitor the statistics of WebLogic Application Servers version 6 through 8 .

Note: To monitor WebLogic Application Servers 11g (10.3.1-10.3.5), use a JMX monitor. For further details, see ["How to create a JMX Monitor for a WebLogic Server" on page 301](#).

Tip: 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 Templates](#).

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the WebLogic Application Server monitor.

Learn More

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 enables 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 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.

Note:

- WebLogic Application Server Monitors cannot be used to monitor WebLogic11g servers. To monitor these servers, use a JMX monitor as described in ["JMX Monitor" on page 296](#). For further details, see ["How to create a JMX Monitor for a WebLogic Server" on page 301](#).
- SiteScope can discover the topology of WebLogic Application Servers using the JMX monitor. You cannot use the WebLogic Application Server monitor to discover topology data for reporting to BSM. For details, see ["WebLogic Application Server Topology" on page 299](#).
- SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of a WebLogic Application Server. For details, see WebLogic Solution Templates in the Using SiteScope Guide.

Supported Platforms/Versions

This monitor supports monitoring agents of SNMP versions 1.0, 2.0, and 3.0 MD5 and SHA.

Tasks

How to Configure the WebLogic Application Server Monitor

1. Set permissions for monitoring 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.

2. Set permissions for monitoring WebLogic 7.x or 8.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 and later 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. Refer to the WebLogic server documentation for more information.

3. Configure SiteScope to use T3 over SSL against a WebLogic 7.x or 8.x server - optional

Perform the following steps to configure a WebLogic monitor with the **Secure Server** option to monitor a WebLogic 7.x or 8.x server.

- a. 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.
- b. 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
```
- c. Obtain a valid Oracle license file and put it somewhere on the SiteScope machine. This is the file named **license.bea** in the BEA installation directory.
- d. 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>\javallib\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.

- e. Open SiteScope and add a WebLogic Application Server monitor.
- f. Configure the WebLogic Application Server Monitor Settings as follows:
 - o In the Authentication Settings area, select the **Secure server** option.
 - o In the Advanced Settings area:
 - o Enter the full path to the **wlcipher.jar** and **weblogic.jar** files in the **WLCipher jar file** and the **WebLogic jar file** boxes, respectively.
 - o Enter the full path to the Oracle license file in the **WebLogic license file** box.
 - o Enter 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 **JVM** box.
- g. Click the **Get Counters** button to browse the counters on the WebLogic server over SSL.

4. **Configure the monitor properties**

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

WebLogic Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
Authentication Settings	
Target	Name of the server where WebLogic is running.
Server	Address of the server where WebLogic is running.
Port number	Port number that the WebLogic server is responding on. Default value: 7001
User name	User name required to log on to the WebLogic server.
Password	Password required to log on to the WebLogic server.
Secure server	Select if using a secure server connection option. If you select this option, you must enter the applicable port number used by the WebLogic server for secure connections. Default value: 7002
Advanced Settings	
WLCipher jar file	For some versions of WebLogic Server, you must install a copy of the wlcipher.jar file from the WebLogic server onto the SiteScope server to enable monitoring over SSL. Enter the absolute path to the file on the SiteScope machine. Example: C:\bea\weblogic81\server\lib\wlcipher.jar Note: This option is for use only with the Secure Server (SSL) option.
WebLogic license file	Enables the Secure Server (SSL) option. Enter the absolute path to the Oracle license file that was copied to the SiteScope machine. Example: C:\bea\license.bea

UI Element	Description
JVM	<p>Full path to the Java Virtual Machine (JVM) in which the WebLogic monitoring process should be run.</p> <p>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>
WebLogic jar file	<p>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>
Classpath	<p>Additional classpath variables that are to be used by the WebLogic JVM running on the SiteScope machine. File path elements should be separated by a colon (":") on UNIX systems, and by a semicolon (";") on Microsoft Windows systems.</p>
Timeout (seconds)	<p>Amount of time, in seconds, to 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 (using a value other than the default timeout value may adversely affect performance)</p>
Counter Settings	
Counters	<p>Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.</p>
Get Counters	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p>Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 103

WebSphere Application Server Monitor

The WebSphere Application Server monitor enables you to monitor the availability and server statistics of WebSphere Application Servers. This enables you to watch server loading for performance, availability, and capacity planning.

Create a separate WebSphere Application Server monitor instance for each WebSphere 5.x, 7.0x, and 8.0x Application Server in your environment. For WebSphere 6.0 and 6.1 Application Servers, you can monitor different instances of WebSphere 6.0 and 6.1 Application Servers simultaneously within one SiteScope process. Previously, you could monitor only one WebSphere 6.0 or 6.1 version at one time.

Tip: 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 Templates in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the WebSphere Application Server monitor.

Learn More

This section includes:

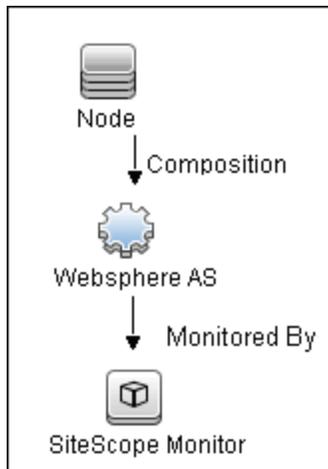
- "Supported Versions/Platforms" below
- "WebSphere Application Server Topology" below

Supported Versions/Platforms

This monitor supports monitoring server performance statistics from WebSphere 5.x, 6.0x, 6.1x, 7.0x, and 8.0x servers.

WebSphere Application Server Topology

The WebSphere Application Server monitor can identify the topology of the WebSphere Application Servers being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

Tasks

This section includes:

- "How to Configure the WebSphere 5.x Application Server Monitoring Environment" below
- "How to Configure the WebSphere 6.0x Application Server Monitoring Environment" on the next page
- "How to Configure the WebSphere 6.1x Application Server Monitoring Environment" on page 812
- "How to Configure the WebSphere 7.0x or 8.0x Application Server Monitoring Environment" on page 817

How to Configure the WebSphere 5.x Application Server Monitoring Environment

1. Configure the WebSphere 5.x server environment

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.

- a. Install the **Administration (or admin console) Performance Analysis** option from the custom options menu in the WebSphere 5.x install.

Caution: 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.

- b. 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 in the previous step.
- c. 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.

- d. Enable PMI Counters or 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.
 - Click **Servers > Application Servers**.
 - Select the server to be monitored from the Application Server list.

- From the Configuration tab, click the Performance Monitoring Service in the Additional Properties list.
 - Select the **Start Up** check box and select the **Initial specification** level as Standard or Custom.
 - Click **Apply**.
- e. 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.

2. Configure the monitor properties

Configure the WebSphere Application Server monitor settings as required.

For monitor user interface details, see "[WebSphere Application Server Monitor Settings](#)" on [page 824](#).

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "[WebSphere Application Server Topology](#)" on [page 806](#).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

How to Configure the WebSphere 6.0x Application Server Monitoring Environment

1. Configure the WebSphere version 6.0x monitoring environment according to whether you are using internal or external Java:
 - For details on configuring the WebSphere 6.0x monitoring environment using internal Java, see "[How to Configure the WebSphere 6.0x Server Environment Using Internal Java](#)" on the [next page](#).
 - For details on configuring the WebSphere 6.0x monitoring environment using external Java, see "[How to Configure the WebSphere 6.0x Server Environment Using External Java](#)" on [page 811](#).

Tip: We recommend using internal Java for each WebSphere monitor because it reduces system load and increases SiteScope performance. When using external java, SiteScope creates a new java process for each monitor taking up to 254 MB of memory per monitor. It is also takes longer to create an external process and connect it.

2. Configure the monitor properties

Create the WebSphere Application Server monitor, and enter the following information in the Monitor Settings panel:

- **WebSphere directory:** %WAS_ENV%
- **Trust store:** %WAS_ENV%\DummyClientTrustFile.jks
- **Trust store password:** WebAS
- **Key store:** %WAS_ENV%\DummyClientKeyFile.jks
- **Key store password:** WebAS

Note:

- If you configured the WebSphere environment to use internal JVMs, make sure that the **Launch an external JVM** check box is not selected. By default, the WebSphere monitor uses internal JVMs for new monitors. When upgrading from previous versions of SiteScope, this check box is selected automatically during the upgrade for existing monitors.
- You can use certificates added using Certificate Management only if **Launch an external JVM** is not selected.
- When using SSL, you also need to define the **User name** and **Password** to access the WebSphere Application Server.

For user interface details, see "[WebSphere Application Server Monitor Settings](#)" on page 824.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

4. Monitor different instances simultaneously - Optional

After configuring settings for the WebSphere Application Server monitor version 6.0x, select **6.1x** from the **Version** drop-down list. The monitor runs simultaneously with the monitor that you just created for WebSphere version 6.0x.

Note: To monitor a WebSphere version 6.1x simultaneously, you must have configured the WebSphere version 6.1x monitoring environment. For details, see "[How to Configure the WebSphere 6.1x Application Server Monitoring Environment](#)" on page 812.

How to Configure the WebSphere 6.0x Server Environment Using Internal Java

- a. On the SiteScope machine, create a directory and give it a name, for example, C:\WAS_6. This directory is referred to as %WAS_ENV%, and the SiteScope root folder is referred to as %SIS_HOME% (you should replace all appearances of %WAS_ENV% and %SIS_HOME% with the actual value).
- b. Copy the following contents from WebSphere Application Server to the SiteScope machine:

From WebSphere Application Server:	To SiteScope machine:
Copy the entire folder: <WAS_SERVER>\WebSphere\AppServer\lib	%WAS_ENV%\lib
<WAS_SERVER>\WebSphere\ AppServer\java\jre\lib\ ibmcertpathprovider.jar	%WAS_ENV%\libmce- rtpathprovider.jar (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\WebSphere\ AppServer\java\jre\lib\ext\ ibmjceprovider.jar	%WAS_ENV%\ibmjceprovider.jar (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\WebSphere\ AppServer\profiles\ <ServerName>\etc\ DummyClientTrustFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named default)	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\profiles\ <ServerName>\etc\ DummyClientKeyFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named default)	%WAS_ENV%\

- c. (SSL only) Import the SSL server certificates. You can use Certificate Management to import the certificates, or you can import the certificates manually.
 - o For details on importing certificates using Certificate Management, see [How to Import Server Certificates Using Certificate Management](#) in the [Using SiteScope Guide](#).
 - o For details on importing certificates manually, see ["How to manually import server certificates for WebSphere 6.0x" on the next page](#).

Note: Make sure you enter the WebSphere SOAP port which you specify in the WebSphere Application Server Monitor Settings.

- d. After importing the server certificates, restart the SiteScope server.
- e. Continue with step 2 of ["How to Configure the WebSphere 6.0x Application Server Monitoring Environment"](#) on page 808.

How to Configure the WebSphere 6.0x Server Environment Using External Java

a. You must have the following directories copied onto the SiteScope machine:

- AppServer/Java
- AppServer/lib

These directories must 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. We recommend this 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. We do not recommend this option because of the size of the application server files.

Once you have the **AppServer/Java** and **Appserver/lib** files on the SiteScope machine, you can prepare the WebSphere environment for monitoring WebSphere 6.x.

- b. On the WebSphere server, select **Servers > Application Servers > <server name> > Performance Monitoring Infrastructure (PMI)** and make sure that the counters are set to **Extended**.
- c. From the SiteScope machine, make sure that you can access the SOAP from a browser. For example, open a browser and enter the following sample address:
`http://jberantlab:8880`. If an XML page is returned, the monitor is ready to be added to SiteScope and configured.

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.

- d. Continue with step 2 of "How to Configure the WebSphere 6.0x Application Server Monitoring Environment" on page 808.

How to manually import server certificates for WebSphere 6.0x

Instead of using Certificate Management, you can import certificates manually using the keytool method, if preferred. Certificates imported this way can still be managed using Certificate Management. For details on Certificate Management, see Certificate Management in the Using SiteScope Guide.

- a. Using Internet Explorer 6 or 7, export the SSL certificate to **%WAS_ENV%\was_certificate.cert** (in base-64 format).

- i. Download the server certificate by double-clicking the key lock icon in Internet Explorer when there is an SSL connection. The icon is located in the status bar for Internet Explorer 6, and to the right of the URL field for Internet Explorer 7 (the field is marked red when self-signed certified is used by the server).
 - ii. In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
 - iii. In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- b. Import the certificate to the **cacerts** file in the SiteScope java folder as follows:

```
%SIS_HOME%\java\bin\keytool -import -v -file %WAS_ENV%\was_certificate.cert -alias was_cert -keystore %SIS_HOME%\java\lib\security\cacerts
```

When prompted for the password, type `changeit` (default password for JRE).

When asked if you trust the imported certificate, type `yes`.
- c. Continue with step d of "How to Configure the WebSphere 6.0x Server Environment Using Internal Java" on page 809.

How to Configure the WebSphere 6.1x Application Server Monitoring Environment

1. Configure the WebSphere version 6.1x monitoring environment according to whether you are using internal or external Java:
 - For details on configuring the WebSphere 6.1x monitoring environment using internal Java, see "How to Configure the WebSphere 6.1x Server Environment Using Internal Java" on the next page.
 - For details on configuring the WebSphere 6.1x monitoring environment using external Java, see "How to Configure the WebSphere 6.1x Server Environment Using External Java" on page 815.

Tip: We recommend using internal Java for each WebSphere monitor because it reduces system load and increases SiteScope performance. When using external java, SiteScope creates a new java process for each monitor taking up to 254 MB of memory per monitor. It is also takes longer to create an external process and connect it.

2. Configure the monitor properties

Create the WebSphere Application Server monitor, and enter the following information in the Monitor Settings panel:

- **WebSphere directory:** %WAS_ENV%
- **Trust store:** %WAS_ENV%\DummyClientTrustFile.jks
- **Trust store password:** WebAS
- **Key store:** %WAS_ENV%\DummyClientKeyFile.jks
- **Key store password:** WebAS

Note:

- If you configured the WebSphere environment to use internal JVMs, make sure that the **Launch an external JVM** check box is not selected. By default, the WebSphere monitor uses internal JVMs for new monitors. When upgrading from previous versions of SiteScope, this check box is selected automatically during the upgrade for existing monitors.
- You can use certificates added using Certificate Management only if **Launch an external JVM** is not selected.
- When using SSL, you also need to define the **User name** and **Password** to access the WebSphere Application Server.

For user interface details, see the UI Descriptions section below.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

4. Monitor different instances simultaneously - Optional

To monitor a WebSphere version 6.0x simultaneously, choose **6.0x** from the **Version** drop-down list. The monitor runs simultaneously with the monitor that you just created for WebSphere version 6.1x.

How to Configure the WebSphere 6.1x Server Environment Using Internal Java

- a. On the SiteScope machine, create a directory and give it a name, for example, C:\WAS_6_1. This directory is referred to as %WAS_ENV%, and the SiteScope root folder is referred to as %SIS_HOME% (you should replace all appearances of %WAS_ENV% and %SIS_HOME% with the actual value).
- b. Copy the following contents from WebSphere Application Server to the SiteScope machine:

From WebSphere Application Server:	To SiteScope machine:
<WAS_SERVER>\WebSphere\ AppServer\plugins\ com.ibm.ws.security.crypto_6.1.0.jar	%SIS_HOME%\java\lib\ext\ com.ibm.ws.security.crypto_6.1.0.jar (jar name must be exactly as listed here; rename it if it has a different name)

From WebSphere Application Server:	To SiteScope machine:
<WAS_SERVER>\WebSphere\ AppServer\runtimes\ com.ibm.ws.admin.client_6.1.0.jar	%WAS_ENV%\com.ibm.ws.admin. client_6.1.0.jar (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\plugins\ com.ibm.ws.runtime_6.1.0.jar	%WAS_ENV\ com.ibm.ws.runtime_6.1.0.jar
<WAS_SERVER>\WebSphere\ AppServer\profiles\<<ServerName> etc\DummyClientTrustFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named default)	%WAS_ENV\
<WAS_SERVER>\WebSphere\ AppServer\profiles\<<ServerName> etc\DummyClientKeyFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named default)	%WAS_ENV\
<WAS_SERVER>\WebSphere\ AppServer\java\jre\lib\ext\ ibmkeycert.jar	%SIS_HOME%\java\lib\ext

- c. (SSL only) Import the SSL server certificates. You can use Certificate Management to import the certificates, or you can import the certificates manually.

Note: Make sure you enter the WebSphere SOAP port which you specify in the WebSphere Application Server Monitor Settings.

- o For details on importing certificates using Certificate Management, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
- o For details on importing certificates manually, see ["How to manually import server certificates for WebSphere 6.1x" on page 817.](#)
- d. (SSL only) After importing the server certificates, modify the **%SIS_HOME%\java\lib\security\java.security** file as follows:

- i. Change it so that it reads:

```
# Default JSSE socket factories

ssl.SocketFactory.provider=com.sun.net.ssl.internal.ssl.SSLSocketFactoryImpl

ssl.ServerSocketFactory.provider=com.sun.net.ssl.internal.ssl.SSLServerSocketFactoryImpl
```

- ii. Add the following additional provider to the list of providers, where N is the number of the next provider in the list:

```
## List of providers and their preference orders (see above):
#
<all existing providers>
security.provider.N=com.ibm.crypto.provider.IBMJCE
```

- e. Restart the SiteScope server.
- f. Continue with step 2 of "How to Configure the WebSphere 6.1x Application Server Monitoring Environment" on page 812.

How to Configure the WebSphere 6.1x Server Environment Using External Java

- a. On the SiteScope machine, create a directory and give it a name, for example, C:\WAS_6_1. This directory is referred to as %WAS_ENV% (you should replace all appearances of %WAS_ENV% with the actual value).
- b. Copy the following contents from WebSphere Application Server to the SiteScope machine:

From WebSphere Application Server:	To SiteScope machine:
<WAS_SERVER>\java***.*	%WAS_ENV%\java***.*
<WAS_SERVER>\runtimes\ com.ibm.ws.admin.client_6.1.0.jar	%WAS_ENV%\com.ibm.ws.admin. client_6.1.0.jar (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\plugins\ com.ibm.ws.runtime_6.1.0.jar	%WAS_ENV%\com.ibm.ws. runtime_6.1.0.jar (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\WebSphere\ AppServer\profiles\<<ServerName>\ etc\DummyClientTrustFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named default)	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\profiles\<<ServerName>\ etc\DummyClientKeyFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named default)	%WAS_ENV%\

- c. (SSL only) Using Internet Explorer 6 or 7, export the SSL certificate to %WAS_

ENV%\was_certificate.cert (in base-64 format).

- i. Download the server certificate by double-clicking the key lock icon in Internet Explorer when there is an SSL connection. The icon is located in the status bar for Internet Explorer 6, and to the right of the URL field for Internet Explorer 7 (the field is marked red when self-signed certified is used by the server).
 - ii. In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
 - iii. In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- d. (SSL only) Import the certificate to the **cacerts** file in the above java folder as follows:

```
%WAS_ENV%\java\bin\keytool -import -v -file %WAS_ENV%\was_
certificate.
cert -alias was_cert -keystore %WAS_
ENV%\java\jre\lib\security\cacerts
```

When prompted for the password, type **changeit** (default password for JRE).

When asked if you trust the imported certificate, type **yes**.

- e. (SSL only) Modify the **%WAS_ENV%\java\jre\lib\security\java.security** file so that it reads as follows:

```
== FROM==
# Default JSSE socket factories
#ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl

#ssl.Serv-
erSock-
etFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
# WebSphere socket factories (in cryptosf.jar)

ssl.Soc-
ket-
Factory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory

ssl.Serve-
rSock-
etFactory.provider=com.ibm.websphere.ssl.protocol.SSLServerSocketFactory
==TO==
# Default JSSE socket factories
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl

ssl.Serve-
rSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
# WebSphere socket factories (in cryptosf.jar)

#ssl.Soc-
cket-
Factory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory
```

```
#ssl.ServerSocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLServerSocketFactory
```

- f. Restart the SiteScope machine.
- g. Continue with step 2 of "How to Configure the WebSphere 6.1x Application Server Monitoring Environment" on page 812.

How to manually import server certificates for WebSphere 6.1x

Instead of using Certificate Management, you can import certificates manually using the keytool method, if preferred. Certificates imported this way can still be managed using Certificate Management. For details on Certificate Management, see Certificate Management Overview in the Using SiteScope Guide.

- a. Using Internet Explorer 6 or 7, export the SSL certificate to **%WAS_ENV%\was_certificate.cert** (in base-64 format).
 - i. Download the server certificate by double-clicking the key lock icon in Internet Explorer when there is an SSL connection. The icon is located in the status bar for Internet Explorer 6, and to the right of the URL field for Internet Explorer 7 (the field is marked red when self-signed certified is used by the server).
 - ii. In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
 - iii. In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- b. Import the certificate to the **cacerts** file in the SiteScope java folder as follows:

```
%SIS_HOME%\java\bin\keytool -import -v -file %WAS_ENV%\was_certificate.cert -alias was_cert -keystore %SIS_HOME%\java\lib\security\cacerts
```

When prompted for the password, type `changeit` (default password for JRE).

When asked if you trust the imported certificate, type `yes`.

- c. Continue with step d of "How to Configure the WebSphere 6.1x Server Environment Using Internal Java" on page 813.

How to Configure the WebSphere 7.0x or 8.0x Application Server Monitoring Environment

1. Configure the WebSphere 7.0x or 8.0x server environment

Configure the WebSphere 7.0x or 8.0x monitoring environment according to whether you are using internal or external Java.

- For configuring the monitoring environment using internal Java, see "How to Configure the WebSphere 7.0x or 8.0x Server Environment Using Internal Java" on the next page.
- For configuring the monitoring environment using external Java, see "How to Configure the WebSphere 7.0x or 8.0x Server Environment Using External Java" on page 820.

Tip: We recommend using internal Java for each WebSphere monitor because it

reduces system load and increases SiteScope performance. When using external java, SiteScope creates a new java process for each monitor taking up to 254 MB of memory per monitor. It also takes longer to create an external process and connect it.

2. Configure the monitor properties

Create the WebSphere Application Server monitor, and enter the following information in the Monitor Settings panel:

- **WebSphere directory:** %WAS_ENV%
- **Trust store:** %WAS_ENV%\DummyClientTrustFile.jks
- **Trust store password:** WebAS
- **Key store:** %WAS_ENV%\DummyClientKeyFile.jks
- **Key store password:** WebAS

Note:

- If you configured the WebSphere environment to use internal JVMs, make sure that the **Launch an external JVM** check box is not selected. By default, the WebSphere monitor uses internal JVMs for new monitors. When upgrading from previous versions of SiteScope, this check box is selected automatically during the upgrade for existing monitors.
- You can use certificates added using Certificate Management only if **Launch an external JVM** is not selected.
- When using SSL, you also need to define the **User name** and **Password** to access the WebSphere Application Server.

For user interface details, see "[WebSphere Application Server Monitor Settings](#)" on page 824.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

How to Configure the WebSphere 7.0x or 8.0x Server Environment Using Internal Java

- a. On the SiteScope machine, create a directory and give it a name, for example, C:\WAS_7. This directory is referred to as %WAS_ENV%, and the SiteScope root folder is referred to as %SIS_HOME% (you should replace all appearances of %WAS_ENV% and %SIS_HOME% with the actual value).
- b. Copy the following contents from WebSphere Application Server to the SiteScope machine:

From WebSphere Application Server:	To SiteScope machine:
<WAS_SERVER>\WebSphere\ AppServer\plugins\ com.ibm.ws.security.crypto.jar	%SIS_ HOME%\java\lib\ext\ com.ibm.ws- .security.crypto.jar (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\WebSphere\ AppServer\runtimes\ com.ibm.ws.admin.client_7.0.0.jar (for WebSphere 7.0x) or com.ibm.ws.admin.client_8.0.0.jar (for WebSphere 8.0x)	%WAS_ENV%\ com.ibm.ws.admin.client_ 7.0.0.jar or com.ibm.ws.admin.client_ 8.0.0.jar (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\WebSphere\ AppServer\plugins\ com.ibm.ws.runtime.jar	%WAS_ENV%\ com.ibm.ws.runtime.jar
<WAS_SERVER>\WebSphere\ AppServer\pr- ofiles\<<ServerName>\etc\DummyClientTrustFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named default)	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\pr- ofiles\<<ServerName>\etc\DummyClientKeyFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named default)	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\java\jre\lib\ext\ ibmkeycert.jar	%SIS_ HOME%\java\lib\ext
<WAS_SERVER>\WebSphere\ AppServer\java\jre\lib\ibmorb.jar (for WebSphere 8.0x only)	%WAS_ENV%\

- c. (SSL only) Import the SSL server certificates. You can use Certificate Management to import the certificates, or you can import the certificates manually.
 - o For details on importing certificates using Certificate Management, see [How to Import Server Certificates Using Certificate Management](#) in the [Using SiteScope Guide](#).
 - o For details on importing certificates manually, see ["How to manually import server](#)

certificates for WebSphere 7.0x or 8.0x" on page 822.

Note: Make sure you enter the WebSphere SOAP port which you specify in the WebSphere Application Server Monitor Settings.

- d. After importing the server certificates, modify the **%SIS_HOME%\java\lib\security\java.security** file as follows:

- i. Change it so that it reads:

```
# Default JSSE socket factories

ssl.SocketFactory.provider=sun.security.ssl.SSLSocketFactoryImpl

ssl.ServerSocketFactory.provider=sun.security.ssl.SSLServerSocketFactoryImpl
```

- ii. Add the following additional provider to the list of providers, where N is the number of the next provider in the list:

```
## List of providers and their preference orders (see
above):
#
<all existing providers>
security.provider.N=com.ibm.crypto.provider.IBMJCE
```

- e. Restart the SiteScope server.
 - f. Continue with step 2 of "How to Configure the WebSphere 7.0x or 8.0x Application Server Monitoring Environment" on page 817.

How to Configure the WebSphere 7.0x or 8.0x Server Environment Using External Java

- a. On the SiteScope machine, create a directory and give it a name, for example, C:\WAS_7. This directory is referred to as %WAS_ENV% (you should replace all appearances of %WAS_ENV% with the actual value).
- b. Copy the following contents from WebSphere Application Server to the SiteScope machine:

From WebSphere Application Server:	To SiteScope machine:
<WAS_SERVER>\java***.*	%WAS_ENV%\java***.*

From WebSphere Application Server:	To SiteScope machine:
<p><WAS_SERVER>\runtimes\ com.ibm.ws.admin.client_7.0.0.jar (for WebSphere 7.0x) or com.ibm.ws.admin.client_8.0.0.jar (for WebSphere 8.0x)</p>	<p>%WAS_ ENV%\com.ibm.ws.admin.c- lient_7.0.0.jar or %WAS_ ENV%\com.ibm.ws.admin.c- lient_8.0.0.jar</p> <p>(jar name must be exactly as listed here; rename it if it has a different name)</p>
<p><WAS_SERVER>\plugins\com.ibm.ws.runtime.jar</p>	<p>%WAS_ ENV%\com.ibm.w- s.runtime.jar</p> <p>(jar name must be exactly as listed here; rename it if it has a different name)</p>
<p><WAS_SERVER>\WebSphere\ AppServer\pr- ofiles\<<ServerName>\etc\DummyClientTrustFile.jks</p> <p>(where <ServerName> is the name of monitored WAS server and not the folder named default)</p>	<p>%WAS_ENV%\</p>
<p><WAS_SERVER>\WebSphere\ AppServer\pr- ofiles\<<ServerName>\etc\DummyClientKeyFile.jks</p> <p>(where <ServerName> is the name of monitored WAS server and not the folder named default)</p>	<p>%WAS_ENV%\</p>
<p><WAS_SERVER>\WebSphere\ AppServer\java\jre\ibmorb.jar (for WebSphere 8.0x only)</p>	<p>%WAS_ENV%\</p>

- c. (SSL only) Using Internet Explorer 6 or 7, export the SSL certificate to **%WAS_ENV%\was_certificate.cert** (in base-64 format).
- i. Download the server certificate by double-clicking the key lock icon in Internet Explorer when there is an SSL connection. The icon is located in the status bar for Internet Explorer 6, and to the right of the URL field for Internet Explorer 7 (the field is marked red when self-signed certified is used by the server).
 - ii. In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
 - iii. In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- d. (SSL only) Import the certificate to the **cacerts** file in the above java folder as follows:

```
%WAS_ENV%\java\bin\keytool -import -v -file %WAS_ENV%\was_certificate.
```

```
cert -alias was_cert -keystore %WAS_
ENV%\java\jre\lib\security\cacerts
```

When prompted for the password, type `changeit` (default password for JRE).

When asked if you trust the imported certificate, type `yes`.

- e. Modify the `%WAS_ENV%\java\jre\lib\security\java.security` file so that it reads as follows:

```
== FROM==
# Default JSSE socket factories
#ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl

#ssl.Serve-
erSock-
etFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
# WebSphere socket factories (in cryptosf.jar)

ssl.Soc-
ket-
Factory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory

ssl.Serve-
rSocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLServer
SocketFactory
==TO==
# Default JSSE socket factories
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl

ssl.Serve-
rSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
# WebSphere socket factories (in cryptosf.jar)

#ssl.So-
cket-
Factory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory

#ssl.Serve-
erSock-
etFactory.provider=com.ibm.websphere.ssl.protocol.SSLServer
SocketFactory
```

- f. Restart the SiteScope machine.
- g. Continue with step 2 of "How to Configure the WebSphere 7.0x or 8.0x Application Server Monitoring Environment" on page 817.

How to manually import server certificates for WebSphere 7.0x or 8.0x

Instead of using Certificate Management, you can import certificates manually using the `keytool` method, if preferred. Certificates imported this way can still be managed using

Certificate Management. For details on Certificate Management, see Certificate Management Overview in the Using SiteScope Guide.

- a. Using Internet Explorer 6 or 7, export the SSL certificate to **%WAS_ENV%\was_certificate.cert** (in base-64 format).
 - i. Download the server certificate by double-clicking the key lock icon in Internet Explorer when there is an SSL connection. The icon is located in the status bar for Internet Explorer 6, and to the right of the URL field for Internet Explorer 7 (the field is marked red when self-signed certified is used by the server).
 - ii. In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
 - iii. In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- b. Import the certificate to the **cacerts** file in the SiteScope java folder as follows:

```
%SIS_HOME%\java\bin\keytool -import -v -file %WAS_ENV%\was_certificate.cert -alias was_cert -keystore %SIS_HOME%\java\lib\security\cacerts
```

When prompted for the password, type `changeit` (default password for JRE).

When asked if you trust the imported certificate, type `yes`.

- c. Continue with step d of "How to Configure the WebSphere 7.0x or 8.0x Server Environment Using Internal Java" on page 818.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

WebSphere Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
Server	Name of the server where the WebSphere Application Server you want to monitor is running. Note: Do not include backslashes in the name.
Target	Logical name of the server you want to monitor. If this box is left empty, the server name entered above is used.
Launch an external JVM	External JVMs are used for monitoring. By default, the WebSphere monitor uses internal JVMs. External JVMs consume greater resources, take longer to start up, and have bad error handling. Note: You cannot use certificates added using Certificate Management if this setting is selected. Default value: Not selected (if upgrading from previous versions of SiteScope, this check box is selected automatically during the upgrade for existing monitors).
Port number	Port number for the SOAP. Default value: 8880
Credentials	User name and password required to access the WebSphere Application Server. Select the option to use for providing credentials: <ul style="list-style-type: none"> • Use user name and password. Select this option to manually enter user credentials. Enter the user name and password in the User name and Password box if one has been configured. • Select predefined credentials. Select this option to have SiteScope automatically supply a predefined user name and password (selected by default). Select the credential profile to use from the Credential profile drop-down list, or click Add Credentials and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences in the Using SiteScope Guide.
Version	Version of the WebSphere application you are monitoring (5.x, 6.0x, 6.1x, 7.0x, 8.0x). Default value: 6.1x
WebSphere directory	Path to the WebSphere AppServer directory. Default value: C:\WebSphere\AppServer

UI Element	Description
Classpath	Additional classpath variables that are to be used by the WebSphere JVM running on the SiteScope machine.
Timeout (seconds)	Amount of time, in seconds, that the monitor should wait for a response from the server. If a response is not received within the interval of the timeout, the monitor reports a timeout error. Default value: 60 seconds
Trust store	Full directory path of file DummyClientTrustFile.jks . The trust file is typically used to store signer certificates, which specify whether the signer of the server's certificate is trusted. This file is in the client monitor directory on the SiteScope machine. Default value: C:\WebSphere\AppServer\profiles\default\etc\DummyClientTrustFile.jks
Trust store password	Password for the SSL trust store file. Default value: WebAS
Key store	Full directory path of file DummyClientKeyFile.jks . This file is typically used to store personal certificates, including private keys. This file is in the client monitor directory on the SiteScope machine. Default value: C:\WebSphere\AppServer\profiles\default\etc\DummyClientTrustFile.jks
Key store password	Password for the SSL key store file. Default value: WebAS 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: <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/ 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.
Client properties file	Name of the custom client properties file. Default value: soap.client.props (use the default for version 6.x)
Security realm	The security realm of the WebSphere application server.

UI Element	Description
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.
Check Configuration	Runs the WebSphere monitor configuration check tool and displays configuration results. This tool provides a step-by-step check of the connection to the server. It checks: <ul style="list-style-type: none">• WebSphere AppClient jars were copied to the SiteScope server.• Certificates were imported into the SiteScope java keystore.• WebSphere jks files.• Secure properties are used (if SSL is enabled).

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Troubleshooting and Limitations

If you encounter "java.lang.ClassNotFoundException: com.ibm.security.krb5.KrbException" while setting up this monitor for a WebSphere Application Server environment where security is enabled, copy the **ibmjgssprovider.jar** from **<WAS_SERVER>\WebSphere\AppServer\java\jre\lib** to **<SiteScope root directory>\java\lib\ext**, and then restart SiteScope.

Chapter 104

WebSphere MQ Status Monitor

The WebSphere MQ Status monitor enables you to monitor the performance attributes of MQ Objects (channels and queues) on MQ Servers. Both performance attributes and events for channels and queues can be monitored. You can set the error and warning thresholds for the WebSphere MQ Status monitor on as many as fifteen function measurements.

Note: The WebSphere MQ Status monitor is an optional SiteScope monitor that requires additional licensing to enable it in the SiteScope interface after the free evaluation period expires. Contact your HP sales representative for more information.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the WebSphere MQ Status monitor.

Learn More

This section includes:

- "Supported Platforms/Versions" below
- "Monitoring MQ Events" below
- "Authentication" below
- "Channel Status Codes" on the next page

Supported Platforms/Versions

This monitor supports monitoring on WebSphere MQ (formerly known as MQSeries) Servers 5.2, 5.3, 5.3.1, 6.0, 7.0, 7.0.1, and 7.0.1.3.

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 Status Monitor Settings panel), 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>\javallib\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.

Channel Status Codes

You can choose from two different reporting schemes for Channel status code values:

- **IBM MQ 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

Monitor Reference

Chapter 104: WebSphere MQ Status Monitor

You can select the required coding scheme in the **Channel status code scheme** box under WebSphere MQ Status Monitor Settings.

Tasks

How to Configure the WebSphere MQ Status Monitor

1. **Download and install the IBM MQ 7.0 SupportPacs (when monitoring using WebSphere MQ 7.0 libraries)**
 - a. Download the WebSphere MQ V7.0 client from the IBM Web site (<http://www-01.ibm.com/support/docview.wss?uid=swg24019253>) and install it on the machine where the SiteScope server is running.
Follow the instructions for installing the support pack.
 - b. Stop SiteScope.
 - c. Copy the following jars from the installed MQ directory (**IBM\WebSphere MQ\javallib**) to the **<SiteScope root directory>\java\lib\ext** folder.
 - **com.ibm.mq.commonservices.jar**
 - **com.ibm.mq.headers.jar**
 - **com.ibm.mq.jar**
 - **com.ibm.mq.jmqi.jar**
 - **connector.jar**
 - d. Restart SiteScope.
2. **Download and install the IBM MQ 6.0 SupportPacs (when monitoring using WebSphere MQ 6.0 libraries)**
 - a. Download the WebSphere ms0b support pack from the IBM Web site (<http://www-01.ibm.com/support/docview.wss?uid=swg24000668>) and install it on the machine where the SiteScope server is running.
Follow the instructions for installing the support pack.
 - b. Stop SiteScope.
 - c. Copy **com.ibm.mq.pcf-6.1.jar** from **ms0b.zip** to the **<SiteScope root directory>\java\lib\ext** folder.
 - d. Copy the following files from the installed MQ client to the **<SiteScope root directory>\java\lib\ext** folder.
 - **com.ibm.mq.jar**
 - **connector.jar**
 - e. Restart SiteScope.
3. **Deploy a security exit class (if MQ server requires SiteScope authentication)**

If the MQ server requires SiteScope to authenticate itself when connecting to retrieve metrics,

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>\javalib\ext**. You can deploy only one security exit class for a SiteScope instance, and every MQ monitor running on that instance runs that security exit.

Note: For 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.

4. **Configure the monitor properties**

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

WebSphere MQ Status Monitor Settings

User interface elements are described below:

UI Element	Description
MQ server name	Host name of the MQ Server you want to monitor. Enter the network name of the server or the IP address of the server. Example: mqmachinename
MQ server port	Port number of the target MQ Server. Default value: 1414
Server connection channel	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	Name of the queue manager whose queues or channels are to be monitored.
User name	User name for the MQ Server you want to monitor. To connect to the server using the SiteScope user, leave this field and the Password empty.
Password	Password for the MQ Server you want to monitor. To connect to the server using the SiteScope user, leave this field and the User name empty.
Alternate queue manager	(Optional) 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.
Channel status code scheme	Select a reporting schemes for Channel Status Code values, and click Apply . <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 830.

UI Element	Description
<p>Available Measurements</p>	<p>Displays available MQ queue instances and channel instances, and counters to choose from.</p> <p>In the Objects drop-down list, select either Queue or Channel Objects to work with. After an object is selected, a connection to the MQ server is made. A list of available queues or channels is displayed, both system and user instances, depending on the object type selected. Select the instances and counters you want to monitor, and click the Add Selected Measurements  button. The selected measurements are moved to the Selected Measurements list.</p>
<p>Selected Measurements</p>	<p>Displays the measurements currently selected for this monitor, and the total number of selected counters.</p> <p>To remove measurements selected for monitoring, select those measurements, and click the Remove Selected Measurements  button. The measurements are moved to the Available Measurements list.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 105

WebSphere Performance Servlet Monitor

Use the WebSphere Performance Servlet Monitor to monitor the server performance statistics for WebSphere servers. You can monitor multiple parameters or counters with a single monitor instance. This enables 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. The error and warning thresholds for the monitor can be set on one or more performance statistics.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the WebSphere Performance Servlet monitor.

Learn More

Supported Platforms/Versions

This monitor supports monitoring WebSphere 3.0x, 3.5, 3.5.x, 4.0, 5.0, 5.1, 5.1.1, 6.0, 6.0.1, 6.0.2, 6.1, 7.0, 7.0.0.19, 7.0.0.21, 8.0, 8.0.0.1, and 8.0.0.2 servers.

Tasks

How to Configure the WebSphere Performance Servlet Monitor

1. Prerequisites

The following are 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 included as part of WebSphere 4.0 must 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.Performance
Servlet
```

2. Configure the monitor properties

Configure the monitor properties as described in the UI Descriptions section below.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

WebSphere Performance Servlet Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Server	Name of the server you want to monitor. On UNIX servers, enter the full path of the server.
Secure server	Select if the server being monitored is secure. Default value: Not selected
Target	Logical name of the server that is the target of this monitor instance. Depending on the deployment of the WebSphere application in your infrastructure, this may be the same as the Server selected above. Default value: Empty (the host name is used)
Port	Port number to the WebSphere server you want to monitor.
Servlet URL	URL of the performance servlet. For WebSphere 6.0 and later, you can use either of the following URLs: <code>/wasPerfTool/servlet/perfservlet</code> or <code>/wasPerfTool/servlet/perfservlet?version=5</code> For previous versions of WebSphere, use the following URL only: <code>/wasPerfTool/servlet/perfservlet?version=5</code> Note: <ul style="list-style-type: none"> Make sure that WebSphere Performance Servlet is deployed on all versions of WebSphere. If you need to monitor WebSphere with SSL, you may configure it in the WebSphere Security.
User name	User name if the URL requires authorization.
Password	Password if the URL requires authorization.
Advanced Settings	

UI Element	Description
Timeout (seconds)	Amount of 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. Default value: 60 seconds
Refresh frequency	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 in Monitor Run Settings. Default value: 10 minutes
Proxy Settings	
HTTP proxy	Name of the proxy server if required.
Proxy user name	Proxy server user name if required to access the server. Note: Your proxy server must support Proxy-Authenticate for these options to function.
Proxy password	Proxy server password if required to access the server.
WebSphere Performance Counters	
Counters	Displays the server performance counters selected for this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Chapter 106

XML Metrics Monitor

The XML Metrics monitor enables you to monitor metrics for systems that make performance data available in the form of an XML file or page.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the XML Metrics monitor.

Learn More

This section includes:

- "XML Metrics Monitor Overview" below
- "XML Requirements" below

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 enables 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.

The error and warning thresholds for the monitor can be set on one or more different objects.

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 Transformation Tool in the Using SiteScope Guide.

Tasks

How to Configure the XML Metrics Monitor

Configure the monitor properties as described in the UI Descriptions section below.

Tip: The **XSL Transformation Tool** is available when configuring this monitor to test a user defined XSL file that can be used to transform an XML file or output (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see XSL Transformation Tool in the Using SiteScope Guide.

Related workflow

How to Deploy a Monitor in the Using SiteScope Guide

UI Descriptions

XML Metrics Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	
XML URL	URL of the XML page or file that contains the metrics that you want to monitor.
XSL file	Convert the XML metrics file into a format that SiteScope can use.
Authorization NTLM domain	Domain for Windows NT LAN Manager (NTLM) authorization if it is required to access the URL.
Pre-emptive authorization	<p>Option for sending Authorization user name and Authorization password if SiteScope requests the target URL:</p> <ul style="list-style-type: none">• Use global preference. SiteScope uses the authenticate setting as specified in the Pre-emptive authorization section of the General Preferences page. This is the default value.• Authenticate first request. Sends the user name and password on the first request SiteScope makes for the target URL. <p>Note: If the URL does not require a user name and password, this option may cause the URL to fail.</p> <ul style="list-style-type: none">• Authenticate if requested. Sends the user name and password on the second request if the server requests a user name and password. <p>Note: If the URL does not require a user name and password, this option may be used.</p> <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 user name and Default authentication password specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p>Note: Pre-emptive authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
Timeout (seconds)	<p>Amount of time, in seconds, to wait for the XML page to complete downloading before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p>Default value: 60 seconds</p>
Authentication Settings	

UI Element	Description
Authorization user name	Authorization user name to access the URL with the XML content, if required.
Authorization password	Authorization password to access the URL with the XML content, if required.
Proxy server	Host or domain name and port of the proxy server if using a proxy server to access the XML URL.
Proxy server user name	Proxy server user name if you using a proxy server and the proxy requires a name and password to access the target URL. Note: The proxy server must support Proxy-Authenticate for these options to function.
Proxy server password	Proxy server password if you using a proxy server and the proxy requires a name and password to access the target URL. Note: The proxy server must support Proxy-Authenticate for these options to function.
Accept untrusted certificates for HTTPS	Select if you need to use certificates that are untrusted in the cert chain to access the target XML URL using Secure HTTP (HTTPS). Default value: Not selected
Accept invalid certificates for HTTPS	Select 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. Default value: Not selected
Counter Settings	
Counters	Displays the server performance counters you want to check with this monitor. Use the Get Counters button to select counters.
Get Counters	Opens the Select Counters Form, enabling you to select the counters you want to monitor. Note when working in template mode: The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

Part 2

Integration Monitors (A-Z)

Chapter 107

HP OM Event Monitor

The HP OM Event Monitor enables you to integrate an existing HP OpenView installation with BSM by transferring HPOM messages from HPOM Server to an BSM server.

Note:

- The HP OM Event monitor is not available when SiteScope is connected to BSM version 9.00 or later (unless the monitor was created in an earlier version of SiteScope that was upgraded to SiteScope 11.20). OM events can be forwarded to BSM 9.00 from the HPOM Server, provided you have an Event Management Foundation license and an integration is configured between Operations Manager and BSM.
- This monitor supports English only. It does not support I18N mode.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP OM Event monitor.

Learn More

This section includes:

- "HP OM Event Monitor Overview" below
- "Supported Versions" below
- "Status" below

HP OM Event Monitor Overview

The HP OM Event monitor depends on an HP OM Integration Add-on module to collect events from the HPOM Server. The Add-on, when installed on the HP OM Server, listens to events received by the HPOM system and sends them to the HP OM Event Monitor. The HP OM Event Monitor transfers the events to an BSM server. The HP OM Integration Add-on and the HP OM Event Monitor communicate using TCP/IP networking (with a customizable TCP port).

The HP OM 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 BSM. Do not modify this configuration file.

Supported Versions

This monitor supports:

- HPOM 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.
- HPOM versions 9.0 or later when installed on Red Hat Linux.
- HPOM versions 7.5 or later when installed on Windows.

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 OM Alert Monitor Configuration Form.

For information about Integration Monitor logging and troubleshooting, see Troubleshooting and Limitations in the Using SiteScope Guide.

Tasks

This section includes:

- "How to Configure the HPOM Integration Add-on (UNIX Platforms)" below
- "How to Configure the HPOM Integration Add-on (Windows Platforms)" on page 854

How to Configure the HPOM Integration Add-on (UNIX Platforms)

The purpose of the HPOM Integration Add-on is to connect to the HPOM message infrastructure, to receive events from the HPOM, and to forward these events to the SiteScope machine.

Note: The HPOM Integration Add-on module is platform specific. Modules are provided for all platforms supported by HPOM/UNIX version 8.24.

1. Install the HPOM integration add-on

Installation packages for the various platforms used below is in **<SiteScope root directory>\conf\ems\hp\addon\OVO-BAC.zip** file.

On HP-UX 11.11 platforms:

- Log on as superuser to the HPOM Server. Alternatively, use the `su` command to gain superuser permissions.
- Copy **HPOvOBac-01.00.000-HPUX11.0-release.depot** installation package to `\tmp`.
- Perform the following command:

```
swinstall -s /tmp/HPOvOBac-01.00.000-HPUX11.0-release.depot \*
```

On HP-UX 11.23 platforms:

- Log on as superuser to the HPOM Server. Alternatively, use the `su` command to gain superuser permissions.
- Copy **HPOvOBac-01.00.000-HPUX11.22_IPF32-release.depot** installation package to `\tmp`.
- Perform the following command:

```
swinstall -s /tmp/HPOvOBac-01.00.000-HPUX11.22_IPF32-release.depot \*
```

On Solaris 5.7 or later platforms:

- Log on as user `root` to the HPOM Server. Alternatively, use the `su` command to gain super-user permissions.
- Copy **HPOvOBac-01.00.000-SunOS5.7-release.sparc** installation package to `\tmp`.
- Perform the following command:

```
pkgadd -d /tmp/HPOvOBac-01.00.000-SunOS5.7-release.sparc HPOvOBac
```

2. Configure the HPOM integration add-on

Once installed, the HPOM Integration Add-on must be configured on the HPOM Server before it can be used.

- a. To configure the HPOM Integration Add-on on the HPOM Server, configure the host name or IP address of the SiteScope machine on which the HPOM Event Monitor is installed:

```
ovconfchg -ns opc.bac -set TargetHost <host name>
```

Note: 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>
```

If you change this setting, make sure to update the HP OM Event Monitor.

Tip: HPOM Integration Add-on for UNIX provides a function that improves performance of internal message processing. Enabling this function improves the performance of the HPOM Integration Add-on (and other HPOM components, such as the HPOM Java user interface). This function is disabled by default.

- b. To enable improved HPOM Add-on performance on UNIX feature, on the HPOM Server, perform the following commands:

- `opcsv -stop`
- `ovconfchg -ovrg server -ns opc -set OPCMSGM_USE_GUI_THREAD NO_RPC`
- `opcsv -start`

3. Tune the HPOM integration add-on

You can tune the HPOM Integration Add-on by running utilities from the command line on the HPOM Server.

To check the current settings, perform the following command:

```
ovconfget opc.bac
```

To change a parameter, perform the following command:

```
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.

Variable Name	Default Value	Description
CacheKeep	500	If cache size reaches <code>CacheMax</code> , only the most-recently-used messages in <code>CacheKeep</code> 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 HPOM 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 <code>MaxWaitTime</code> .
MaxWaitTime	120	Maximum number of seconds to wait after connection failures before retry. When doubling the wait time after connection failures exceeds <code>MaxWaitTime</code> , the wait time is no longer doubled and <code>MaxWaitTime</code> 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 <code>MaxQueueLen</code> , the oldest entries are removed from the queue.
NodeKeepTime	900	The HPOM Integration Add-on looks up IP addresses from host names. In addition, OM/Windows host names also need to be looked up from the HPOM database. These IP addresses (and host names on OM/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 <code>NodeKeepTime</code> seconds.

Changing any of these variables automatically updates the HPOM Integration Add-on. There is no need to stop and restart the HP OM Integration Add-on process.

4. Start and stop the HPOM integration add-on

The HPOM Integration Add-on must be started after it is installed.

On UNIX platforms, the HPOM Integration Add-on is controlled by OpenView Control Daemon (`ovcd`). Using the command line tool `ovc` on the HPOM Server, perform the command:

```
ovc -stop <or start> opc2bac
```

If the HPOM 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 HPOM Integration Add-on.

If the HPOM 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 HPOM API libraries, it may be necessary to stop the Integration Add-on before installing HPOM patches, and start it after the patch installation.

5. Uninstall the HPOM integration add-on files from the HPOM server

If you must uninstall the HPOM Integration Add-on files from the HPOM Server, perform the following procedure:

On HP-UX platforms:

- Log on as superuser.
- Perform the command: `swremove HPOvOInt.HPOVOBAC`

On Solaris platforms:

- Log on as superuser.
- Perform the command: `pkgrm HPOvOBac`

6. Support in HPOM cluster installation

The HPOM Integration Add-on is supported in an HPOM cluster environment. You can do the following tasks:

- Install HPOM Integration Add-on on each cluster node separately.
- Configure HPOM Integration Add-on on each cluster node separately. All configuration settings on all cluster nodes must be identical.
- Uninstall HPOM Integration Add-on on each cluster node separately.

7. View log file messages

The HPOM Integration Add-on writes log messages into the log file **`/var/opt/OV/logSystem.txt`**.

Log file entries use the process name **`opc2bac`** for messages logged by the HPOM Integration Add-on.

How to Configure the HPOM Integration Add-on (Windows Platforms)

The purpose of the HPOM Integration Add-on is to connect to the HPOM message infrastructure, to receive events from the HPOM, and to forward these events to the SiteScope machine.

Note:

- The HPOM Integration Add-on module is platform specific. Modules are provided for all platforms supported by OM/Windows version 7.5.
- Added support to install the HPOM Integration Add-on module on a Windows Server R2 64-bit machine from the **`OVO-BAC.zip`** installation file.

1. Install the HPOM integration add-on

Installation packages for the various platforms used below is in **<SiteScope root directory>\conf\ems\hp\addon\OVO-BAC.zip** file.

- a. Log on as user `administrator` to the HPOM Server.
- b. Copy **HPOvXpl-03.10.040-WinNT4.0-release.msi** and **HPOvOBac-01.00.000-WinNT4.0-release.msi** installation packages to **C:\tmp**. Perform the following commands:
 - `msiexec /I C:\tmp\HPOvXpl-03.10.040-WinNT4.0-release.msi /qn`
 - `msiexec /I C:\tmp\HPOvOBac-01.00.000-WinNT4.0-release.msi /qn`

2. Configure the HPOM integration add-on

Once installed, the HPOM Integration Add-on must be configured on the HPOM Server before it can be used. To configure the HPOM Integration Add-on on the HPOM Server, configure the host name or IP address of the SiteScope machine on which the HP OM Event Monitor is installed:

```
ovconfchg -ns opc.bac -set TargetHost <host name>
```

Note:

- 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>`
- If you change this setting, make sure to update the HP OM Event Monitor.

3. Tune the HPOM integration add-on

You can tune the HPOM Integration Add-on by running utilities from the command line on the HPOM Server.

To check the current settings, perform the following command:

```
ovconfget opc.bac
```

To change a parameter, perform the following command:

```
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.

Variable Name	Default Value	Description
CacheMax	1000	Maximum number of messages stored in cache memory to avoid database lookups.
CacheKeep	500	If cache size reaches <code>CacheMax</code> , only the most-recently-used messages in <code>CacheKeep</code> 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 HPOM 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 <code>MaxWaitTime</code> .
MaxWaitTime	120	Maximum number of seconds to wait after connection failures before retry. When doubling the wait time after connection failures exceeds <code>MaxWaitTime</code> , the wait time is no longer doubled and <code>MaxWaitTime</code> 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 <code>MaxQueueLen</code> , the oldest entries are removed from the queue.
NodeKeepTime	900	The HPOM Integration Add-on looks up IP addresses from host names. In addition, OM/Windows host names also need to be looked up from the OM database. These IP addresses (and host names on OM/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 <code>NodeKeepTime</code> seconds.

Changing any of these variables automatically updates the HP OM Integration Add-on. There is no need to stop and restart the HP OM Integration Add-on process.

4. Start and stop the HPOM integration add-on

The HPOM Integration Add-on runs as a Windows service and must be started after it is installed. To start or stop the HPOM Integration Add-on on Windows platforms:

- a. On the HPOM Server, click **Start > Settings > Control Panel > Administrative Tools > Services**.
- b. Select the service **HP OpenView Operations Message Forwarder to BAC**.
- c. Click **Start** or **Stop**.

5. Uninstall the HPOM integration add-on files from the HPOM server

If you must uninstall the HPOM Integration Add-on files from the HPOM Server, perform the following procedure:

- a. On the HPOM Server, click **Start > Settings > Control Panel > Administrative Tools > Services**.
- b. 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.

6. Support in HPOM cluster installation

The HPOM Integration Add-on is supported in an HPOM cluster environment. You can do the following tasks:

- Install HPOM Integration Add-on on each cluster node separately.
- Configure HPOM Integration Add-on on each cluster node separately. All configuration settings on all cluster nodes must be identical.
- Uninstall HPOM Integration Add-on on each cluster node separately.

7. View log file messages

The HPOM Integration Add-on writes log messages into the **System.txt** log file in the **<DataDir>\log** directory, where **<DataDir>** is the data directory chosen during OM/Windows installation (for example, **C:\Program Files\HP OpenView\Data**).

Log file entries use the process name **opc2bac** for messages logged by the HP OM Integration Add-on.

Related workflow

How to Deploy Integration Monitors in the Using SiteScope Guide

UI Descriptions

This section includes:

- "HP OM Event Monitor Settings" below
- "Field Mapping" below
- "Topology Settings" below
- "Settings Common to All Monitors"

HP OM Event Monitor Settings

User interface elements are described below:

UI Element	Description
HPOM Add-on TCP port	TCP port number as configured in the HPOM Integration Add-on. Default value: 9000

Field Mapping

User interface elements are described below:

UI 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 OM installation to a format recognizable by the monitor and BSM.</p> <p>Field mapping is not editable while configuring the monitor and we recommend that you use the out-of-the-box integration mapping. 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 Field Mapping Data Types in the Using SiteScope Guide.</p>

Topology Settings

User interface elements are described below:

UI Element	Description
Script	<p>The out-of-the-box integration script that creates a topology in BSM that is based on the collected data from the OM 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 OM system and BSM's applications.</p> <p>We recommend that you 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_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 Editing the Topology Script in the Using SiteScope Guide.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Tips/Troubleshooting

General Notes/Limitations

- The HP OM Event monitor is not available when SiteScope is connected to BSM version 9.00 or later (unless the monitor was created in an earlier version of SiteScope that was upgraded to SiteScope 11.10). OM events can be forwarded to BSM 9.00 from the HPOM server, provided you have an Event Management Foundation license and an integration is configured per the instructions in the BSM Installation Guide in the BSM Help.
- For script alerts to be sent to Operations Manager when using an OM script, the **Template** setting in Action Type Settings must be changed to **Default** (by default it is set to **Typical**).

Chapter 108

HP Service Manager Monitor

This monitor enables you to integrate HP Service Manager incidents with BSM. The incidents in Service Manager are forwarded to BSM as samples by this SiteScope monitor. The samples are used in reporting data to the BSM applications, such as Service Level Management and Service Health.

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 Service Manager environment. For details, see HP Service Manager Solution Templates in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP Service Manager monitor.

Learn More

This section includes:

- "HP Service Manager Monitor Overview" below
- "Supported Versions" below

HP Service Manager Monitor Overview

The HP Service Manager Monitor enables you to integrate Incident Management data from an HP ServiceCenter or HP Service Manager installation with BSM. In general, this chapter uses the name Service Manager when referring to both ServiceCenter and Service Manager. If there are specific differences, they are noted.

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 Service Manager monitor forwards business service-related incidents to BSM 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 Service Manager. 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 Service Manager monitor CI and the business service CI. The monitor integrates the incident data into samples which are forwarded to BSM applications, such as Service Health and Service Level Management.

For more details on the capabilities of the integration, see *How to Integrate HP Service Manager with Business Service Management Components* in the BSM User Guide in the BSM Help.

For more detailed information on the CIs and related KPIs, see *Integration with HP Service Manager* in the BSM User Guide in the BSM Help.

Supported Versions

This monitor supports:

- ServiceCenter 6.2.6
- Service Manager 7.01, 7.02, 7.11 and 9.20 (previously 7.2)

Tasks

This section includes:

- "How to Work with the HP Service Manager Integration" below
- "Copy the JAR File" on the next page
- "Create the JAR File" on the next page

How to Work with the HP Service Manager Integration

1. Prerequisites

Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see How to Configure the Integration Between SiteScope and BSM in the Using SiteScope Guide.

2. Edit clocks and Incident Management configuration files

If any changes were made to the clocks table, the incident management tables in HP Service Manager, or both, 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 Service Manager. 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. Add or create the JAR file (if required)

You can add or create the JAR file for this monitor as follows:

- For integrations with ServiceCenter 6.2.6 and HP Service Manager 7.0.x using default settings, no additional JAR configurations are required.
- For integrations with HP Service Manager 7.1 or 9.2 using default settings, you must copy the JAR file to the **WEB-INF\lib** directory and edit the configuration file. For details, see "Copy the JAR File" on the next page.
- For any integration with ServiceCenter or HP Service Manager that does not use the default configuration, you must create the JAR file. For details, see "Create the JAR File" on the next page.

Note: SiteScope cannot monitor HP Service Manager 7.1 and earlier versions of HP Service Manager at the same time, since they require different JARs and configurations.

4. Configure an HP Service Manager monitor in SiteScope

You can create this monitor:

- Using the EMS Integrations Administration portal in BSM.
- Directly in SiteScope.

Tip: Monitors must be created in a group in the monitor tree. We recommend that you create a special group for the Service Manager integration.

For details on configuring the monitor settings, see "HP Service Manager Monitor Settings" on page 866.

Copy the JAR File

1. To enable SiteScope to integrate with HP Service Manager 7.1 or 9.2 using default settings, copy the JAR file from **<SiteScope root directory>\conf\ems\peregrine\lib<SM version>** to **<SiteScope root directory>WEB-INF\lib**.
2. Open the **incidentAttributesMapping.config** file located in **<SiteScope root directory>conf\ems\peregrine**, and change the line `target_name=configurationItem` to `target_name=affectedItem`.

Note: The **peregrine.jar** located in **<SiteScope root directory>conf\ems\peregrine\lib\6x-7.0x** can be used as backup for the out-of-the-box JAR.

Create the JAR File

This batch file creates and compiles the files needed for the HP Service Manager monitor. The result of this batch is the file **peregrine.jar** that is automatically copied to the **WEB-INF\lib** directory. You should also create a backup of the .jar file. To create the .jar file:

1. Stop the SiteScope service on the SiteScope machine.
2. Ensure that JDK version 1.5 is installed (1.5.0_08 recommended – can be downloaded from Sun archives, <http://java.sun.com/products/archive/>).
3. Set **JAVA_HOME** system variable to the JDK directory (for example **C:\j2sdk1.5.0_08**). You must recompile the peregrine.jar file if you made changes to the monitor tables.
4. Update the **<SiteScope root directory>\conf\ems\peregrine\build.properties** file with the wsdl locations.
 - When integrating with HP ServiceCenter 6.2.6, use the following syntax:

```
clocks.wsdl.url=http://<SM host>:<SM port>/sc61server/PW/Clocks?wsdl
prob.wsdl.url=http://<SM host>:<SM port>/sc61server/PW/IncidentManagement?wsdl
```
 - When integrating with Service Manager 7.x, use the following syntax:

```
clocks.wsdl.url=http://<SM host>:<SM port>/sc62server/PWS/Clocks?wsdl
```

```
prob.wsdl.url=http://<SM host>:<SM port>/sc62server/PWS/  
IncidentManagement?wsdl
```

5. Run the batch file:
 - **Windows:** Double-click the **<SiteScope root directory>\confiems\peregrine\create-peregrine-jar.bat** file to run the batch.
 - **UNIX:** You must run the **<SiteScope root directory>\confiems\peregrine\create-peregrine-jar.sh** file from the full path in a terminal window.
6. Restart the SiteScope service on the SiteScope machine.

Related workflow

How to Deploy Integration Monitors in the Using SiteScope Guide

UI Descriptions

This section includes:

- "HP Service Manager Monitor Settings" below
- "Topology Settings" on the next page
- "Settings Common to All Monitors"

HP Service Manager Monitor Settings

User interface elements are described below:

UI Element	Description
HP Service Manager Web Service Endpoint	<p>URL for the HP Service Manager Web Service. Use the following format: <protocol>://<host_name>:<port>/ where host_name is the name of the Service Manager server and port is the port number of the Service Manager server.</p> <p>The URL syntax when integrating with Service Manager 7.01 and 7.02 is: <protocol>://<SM host>:<SM port>/sc62server/PWS/</p> <p>The URL syntax when integrating with Service Manager 6.2.6 is: <protocol>://<SM host>:<SM port>/sc61server/PWS/</p>
Username	Designated user name created in HP Service Manager for the purpose of this integration monitor.
Password	Password of the designated user created in HP Service Manager for the purpose of this integration monitor.
Field Mapping	<p>The out-of-the-box integration script that enables the monitor to correctly map the data it collects from the Service Manager installation to a format recognizable by the monitor and BSM.</p> <p>Field mapping is not editable while configuring the monitor and we recommend that you use the out-of-the-box integration mapping. If you must customize the field mapping, locate the following file: <SiteScope root directory>\conflms\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 Field Mapping Data Types in the Using SiteScope Guide.</p>

UI Element	Description
Test Script	<p>Tests the field mapping script. We recommend that you test the script before running the monitor. This test gives you the results of what events are forwarded to BSM.</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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>
Synch Flag	<p>Enables the monitor to query Service Manager 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 Service Manager.</p>
Synch Time	<p>Time from which the monitor retrieves incidents. Enter a value only when Synch Flag is selected.</p>
Incident Management (probsummary table) query	<p>Text to add to the query that the monitor sends to Service Manager. You can add to the query to determine which Incidents the monitor retrieves.</p> <p>Default value: <code>type="bizservice"</code>. 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 Service Manager application. We recommend that you consult the Service Manager help to create the text to add to the query and to test the query using the advanced search found in the Service Manager application.</p>
Incident Open State	<p>Indicates the initial state as defined in Service Manager for the incident lifecycle.</p> <p>Default value: Open</p>

Topology Settings

User interface elements are described below:

UI Element	Description
<p>Script</p>	<p>The out-of-the-box integration script that creates a topology in BSM that is based on the collected data from the Service Manager 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 Service Manager system and BSM's applications.</p> <p>We recommend that you use the topology settings as is (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_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 Editing the Topology Script in the Using SiteScope Guide.</p>
<p>Test Script</p>	<p>Tests the topology script. This test gives you the results of what events are forwarded to BSM 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 109

NetScout Event Monitor

The NetScout Event Monitor monitors alerts received from the NetScout nGenius server and forwards them to BSM.

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 Service Manager environment. For details, see HP Service Manager Solution Templates in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the NetScout Event monitor.

Learn More

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 BSM. 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.

The NetScout Event Monitor forwards alerting instances to BSM 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 relevant host, interface, or application CI. The monitor integrates the incident data into samples that are forwarded to BSM applications, such as Service Health and Service Level Management.

Note: For information about Integration Monitor logging and troubleshooting, see Troubleshooting and Limitations in the Using SiteScope Guide.

Tasks

How to Integrate Data From a NetScout System

The following are the steps necessary to integrate data from a NetScout system and view the NetScout data in a way that is customized to your needs.

1. Prerequisites

The following are important guidelines and requirements for using the NetScout Event Monitor to forward alerts to BSM.

- Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see [How to Configure the Integration Between SiteScope and BSM in the Using SiteScope Guide](#).
- 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.

- The NetScout Event Monitor must be set to synchronize integration monitor data with BSM. You can use the configuration file for the NetScout Event Monitor to control the data that is sent from SiteScope to BSM. For details on the file structure and syntax, see [Field Mapping Data Types in the Using SiteScope Guide](#).

2. Configure a NetScout Event monitor in SiteScope

You can create this monitor:

- Directly in SiteScope.
- Using the System Availability Management Administration portal in BSM.

For details on configuring the monitor settings, see ["NetScout Event Monitor Settings" on the next page](#).

3. Activate NetScout EMS integration in BSM

Activate the assignment rules in BSM. For details on how to perform this task, see [NetScout nGenius Integration in the BSM Application Administration Guide in the BSM Help](#).

Related workflow

[How to Deploy Integration Monitors in the Using SiteScope Guide](#)

UI Descriptions

This section includes:

- "NetScout Event Monitor Settings" below
- "Field Mapping" below
- "Topology Settings" on the next page

NetScout Event Monitor Settings

User interface elements are described below:

UI Element	Description
Run Alerts	<p>Method for running alerts:</p> <ul style="list-style-type: none">• For each event received from NetScout system. 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> <ul style="list-style-type: none">• Once, after all events from NetScout system were received. 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>Value that accounts 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>

Field Mapping

User interface elements are described below:

UI 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 BSM.</p> <p>This script is not editable.</p>

Topology Settings

User interface elements are described below:

UI Element	Description
Script	<p>The out-of-the-box integration script that creates a topology in BSM. The topology is based on the collected data 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 BSM's applications.</p> <p>We recommend that you use the topology settings as is (it is not editable while creating the monitor). If you must customize the topology, 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 Editing the Topology Script in the Using SiteScope Guide.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Chapter 110

Technology Database Integration Monitor

Note: The Technology Database Integration monitor was deprecated and is used for backward compatibility only. If you intended to use this monitor (it is supported for BSM 9.1x and earlier versions only), you should contact HP Customer Support for assistance.

The Technology Database Integration Monitor enables 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 Service Management as samples (one sample for each row that was returned by a SQL query).

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the monitor from the New Monitor Page.

Learn More

This section includes:

- ["Technology Database Integration Monitor overview" below](#)
- ["What Data Is Forwarded" below](#)
- ["Understanding How Data in the Enumerating Field is Processed" on the next page](#)
- ["Notes and Limitations" on page 877](#)

Technology Database Integration Monitor overview

The Technology Database Integration Monitor enables you to collect data from database tables used by Enterprise Management Systems (EMS) by performing a query through a JDBC connection.

The following are examples of data that can be integrated into BSM using the Technology Database Integration Monitor:

- Events from monitoring applications event tables or views.
- Open tickets from ticketing systems applications.
- Time series data from monitoring applications metrics tables.
- Topology from a third-party topology database.

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 data records are forwarded only once. Using an initial value enables you to specify an initial threshold value for the data that should be forwarded.

For example, if **Enumerating Field Type** uses `DATE` and **Start from value** uses `2003-20-03 12:00:00`, only data records 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 data records are forwarded. For details on how data from the enumerating field is processed, see ["Understanding How Data in the Enumerating Field is Processed" on the next page below](#).

You use the field mapping script selected for the Technology Database Integration Monitor to control the data that is sent from SiteScope to BSM (for script types, see [Field Mapping Data Types](#) in the [Using SiteScope Guide](#)). For details on the file structure and syntax, see [Event Handler Structure and Syntax](#) in the [Using SiteScope Guide](#). For best practices and details on configuring the integration (depending on the type of sample data being captured), see [How to Deploy Integration Monitors](#) in the [Using SiteScope Guide](#).

Data can also be mapped to a topology to forward data to the correct CI hierarchy in BSM. You can configure topology settings for the monitor by selecting one of the predefined scripts, or configuring

your own topology script during monitor creation. For more details on editing the script, see [Topology Settings for Technology Integration Monitors](#) in the [Using SiteScope Guide](#).

Before setting up the Technology Database Integration Monitor, you should be clear about the purpose and usage of the data in BSM (for presentation in Service Health, Service Level Management, reports, or all).

Understanding How Data in the Enumerating Field is Processed

Since the data in the enumerating field is not unique key, the data in the column used for the enumerating field must have constantly increasing values or values that changed since the scheduled monitor run. For example, if before the first monitor run the table contains the following data:

Run 1:

ENUM_FIELD	DATA_NAME
1	Alice
1	Alice
2	Bob

The monitor reads all entries, stores "1" as the position where all data was send, and skips the lines with ENUM_FIELD=2, because there is a possibility that new lines with ENUM_FIELD=2 will be added later.

Run 2:

ENUM_FIELD	DATA_NAME
1	Alice
1	Alice
2	Bob
2	Bob
2	Bob

At the end of the run, the monitor runs a query with filter "where ENUM_FIELD>1". However, it does not send any data because it did not reach the end of the values listed as having ENUM_FIELD=2. The monitor cannot send this partial list until a new higher value appears in the table.

Run 3:

ENUM_FIELD	DATA_NAME
1	Alice
1	Alice

ENUM_FIELD	DATA_NAME
2	Bob
2	Bob
2	Bob
3	Charlie

At this stage, the monitor runs the same query with filter "where ENUM_FIELD>1", and sends all the data with ENUM_FIELD equals to 2. It also updates the internal variable for last read position to 2, and skips the last line with ENUM_FIELD equals to 3, until new lines with a value higher than 3 appears.

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.

Tasks

How to Integrate database data into BSM

This section provides the workflow for setting up the Technology Database Integration Monitor to work with BSM.

This task includes the following steps:

- "Prerequisites" below
- "Use the SiteScope Database Connection tool" on page 880
- "Create a Technology Database Integration monitor" on page 880
- "Edit the monitor's field mapping" on page 880
- "Edit the monitor's topology settings - optional" on page 881
- "View data from the monitor in BSM" on page 881

1. Prerequisites

- Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see *How to Configure SiteScope to Communicate with BSM in the Using SiteScope Guide*.
- There are several key database driver requirements for using this monitor.
 - You can use the database drivers supplied with SiteScope by default, or you can 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. If the file is in zip format, unzip the contents to a temporary directory. 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:
 - **com.mercury.jdbc.sqlserver.SQLServerDriver**. DataDirect driver from DataDirect Technologies. It is a driver for those Microsoft SQL databases that use Windows authentication. For details on installing the driver, see the note below.

Note: To install the MSSQL JDBC driver:

- Download the MSSQL JDBC driver from the [Microsoft Download Center](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2505) (<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2505>), and unzip the contents to a temporary directory.
- Copy the **sqljdbc4.jar** file to the **<SiteScope root directory>\WEB-INF\lib** subdirectory.
- Restart the **SiteScope** service.

- Use the Database Connection Tool for connection tuning:
 - Database Connection URL:** `jdbc:sqlserver://<IP Address>:<port>;InstanceName=<name>;DatabaseName=<name>`
 - Database Driver:** `com.microsoft.sqlserver.jdbc.SQLServerDriver`
 - Create the desired database monitor type.
- **com.mercury.jdbc.oracle.OracleDriver.** A driver for Oracle databases. This driver is deployed with SiteScope. When using the driver, the database connection URL has the form of: `jdbc:mercury:oracle://<server name or IP address>:<database server port>;sid=<sid>`
- **oracle.jdbc.driver.OracleDriver.** SiteScope supports the following categories of JDBC driver that are supplied by Oracle:
 - JDBC thin driver for Oracle 7 and 8 databases.
 - JDBC OCI (thick) driver. For details on accessing Oracle databases using OCI driver, see [Access Oracle databases using OCI driver](#).
- **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. Database Connection URLs for this monitor are:
 - **`jdbc:mercury:sqlserver://<hostname>:1433;DatabaseName=master;AuthenticationMethod=type2`**
where `<hostname>` is the name of the host where the database is running.
 - **`jdbc:mercury:oracle://<hostname or IP address>:<port>;sid=<sid>`**
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 `<sid>` is the Oracle system ID.
 - **`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.
 - **`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.
- Use a database client to connect to the relevant software database. Identify which tables contain the required data (the software schema documentation may help you with this).

2. Use the SiteScope Database Connection tool

Run the SiteScope Database Connection tool (for details, see Database Connection Tool in the Using SiteScope Guide) and follow these steps:

- a. Verify the driver can be loaded and that it successfully connects.
- b. Add a user name and password to verify that a connection can be established to the database.
- c. Add a native query. Refine the query until you get all the required events/metrics required for BSM.

3. Create a Technology Database Integration monitor

Add a Technology Database Integration Monitor to SiteScope. For monitor user interface details, see "Technology Database Integration Monitor Settings" on page 882.

- 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.
- **Name.** It is recommended that the monitor name include the name of the integrated software.
- Enter all connection parameters for connecting to the database in the **Connection parameters** area.
- **SELECT/FROM/WHERE query clauses.** **SELECT** and **FROM** are mandatory. 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 **Query Settings** section for the monitor.

- **Enumerating field parameters.** Enter details for the enumerating field.

4. Edit the monitor's field mapping

The mapping defines the processing of incoming data and the output sample forwarded to BSM.

Note: The Field Mapping panel is not available when the **Report topology without data** check box is selected in Topology Settings.

- a. In the New Technology Database Integration Monitor dialog box, expand the **Field Mapping** panel. Select a field mapping type and click **Load File**. For details on field mapping types, see Field Mapping Data Types in the Using SiteScope Guide.

For user interface details, see "Field Mapping" on page 884.
- b. A template script is displayed in the **Field mapping** box. Edit the script to enable SiteScope to retrieve the data from the monitored application that you want to forward to BSM. For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide.

5. **Edit the monitor's topology settings - optional**

In the **Topology Settings** panel, you can create or select a script that creates a topology of configuration items in BSM's RTSM to match your EMS system.

For details on this topic, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.

For user interface details, see "Topology Settings" on page 885.

6. **View data from the monitor in BSM**

View the data in BSM:

- If you chose and edited the **Common Events/Legacy Events** script in the Field Mapping panel, you can view events in Service Health, System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- If you chose and edited the **Metrics** script in the Field Mapping panel, you can view the data in any application that supports SiteScope data, including SiteScope Over Time 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 **<BSM root directory>\bin**.
- To troubleshoot problems with data arriving to BSM, see "Troubleshooting" on page 888.

Related workflow

How to Deploy Integration Monitors in the Using SiteScope Guide

UI Descriptions

This section includes:

- "Technology Database Integration Monitor Settings" below
- "Field Mapping" on page 884
- "Topology Settings" on page 885

Technology Database Integration Monitor Settings

User interface elements are described below:

UI Element	Description
Basic Settings	
Database connection URL	<p>URL to a database connection (sometimes referred to as an Authentication string).</p> <p>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, enter <code>jdbc:odbc:test</code> as the connection URL. Alternatively, use the supplied Microsoft SQL or Oracle driver to connect to the database.</p>
Database driver	Driver used to connect to the database. Use the fully qualified class name of the JDBC driver you are using.
Database user name	User name used to log on to the database.
Database password	Password used to log on to the database.
OS integrated security	<p>Uses 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>
EMS server name	<p>Text identifier describing the database server that this monitor is monitoring if you are reporting monitor data to an installation of HP Business Service Management. This text descriptor is used to identify the database server when the monitor data is viewed in an HP Business Service Management report.</p> <p>Syntax exceptions: Use only alphanumeric characters for this entry. You can enter the name of the monitored server or a description of the database to be used to identify the host machine.</p>

UI Element	Description
EMS time difference	<p>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>
Timeout	<p>Amount of time, in seconds, that SiteScope should wait before the monitor times out.</p> <p>Default value: 60 seconds</p>
Query Settings	
SELECT	<p>SELECT clause to be used in the SQL query. Enter * for all fields or a comma separated list of column names to be retrieved from the database.</p> <p>When specifying the SELECT clause, the column used as the enumerating field must appear in the clause.</p>
FROM	<p>FROM clause to be used in the SQL query. Enter a table name or a comma separated list of tables from which the selected columns should be extracted.</p>
WHERE	<p>WHERE clause to be used in the SQL query. This is an optional field which enables you to define the select criteria.</p> <p>Leaving it empty results in retrieving all the rows from the table defined in the FROM option.</p>
Enumerating field	<p>Name for a database field that can be used to order the data that is returned from the database query.</p> <p>For details on how data from the enumerating field is processed, see "Understanding How Data in the Enumerating Field is Processed" on page 876 above.</p> <p>Note: The column used as enumerating field must be included in the SELECT clause.</p>

UI Element	Description																			
Enumerating field type	<p>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"> <thead> <tr> <th>SQL Type</th> <th>Enumerating Field Type</th> </tr> </thead> <tbody> <tr> <td>SMALLINT</td> <td>INTEGER</td> </tr> <tr> <td>INTEGER</td> <td>INTEGER / LONG</td> </tr> <tr> <td>BIGINT</td> <td>LONG</td> </tr> <tr> <td>NUMERIC</td> <td>LONG</td> </tr> <tr> <td>DOUBLE</td> <td>DOUBLE</td> </tr> <tr> <td>DECIMAL</td> <td>DOUBLE</td> </tr> <tr> <td>FLOAT</td> <td>DOUBLE</td> </tr> <tr> <td>TIMESTAMP</td> <td>TIMESTAMP</td> </tr> <tr> <td>DATE</td> <td>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
SQL Type	Enumerating Field Type																			
SMALLINT	INTEGER																			
INTEGER	INTEGER / LONG																			
BIGINT	LONG																			
NUMERIC	LONG																			
DOUBLE	DOUBLE																			
DECIMAL	DOUBLE																			
FLOAT	DOUBLE																			
TIMESTAMP	TIMESTAMP																			
DATE	TIMESTAMP																			
Initial enumerating value	<p>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 <code>DATE</code> and you enter a value of <code>2000-01-31 12:00:00</code> in the Initial enumerating 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>																			
Max rows	<p>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>																			

Field Mapping

User interface elements are described below:

UI Element	Description
Data Type	<p>Select from the following data types for this integration:</p> <ul style="list-style-type: none"> • Common Events. For details, see Configuring Field Mapping for Common Event Samples in the Using SiteScope Guide. • Legacy Events. For details, see Configuring Field Mapping for Legacy Event Samples in the Using SiteScope Guide. • Metrics. For details, see Configuring Field Mapping for Metrics Samples in the Using SiteScope Guide. • Tickets. For details, see Configuring Field Mapping for Ticket Samples in the Using SiteScope Guide.
Load File	<p>Loads the script that is applicable to the data 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 BSM. To enable the integration, you must configure the mapping as required by the environment you are monitoring.</p> <p>The mapping is editable in this box using the script editor provided (you can make the script field read only by right-clicking the script and selecting Configure > Read Only). You can also 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 Field Mapping Data Types in the Using SiteScope Guide.</p>
Test Script	<p>Tests the field mapping script. We recommend that you test the script before running the monitor. This test gives you the results in a separate window of what events or metrics are forwarded to BSM.</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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Topology Settings

User interface elements are described below:

UI Element	Description
Report topology without data	<p>Reports the topology for the integration monitor without sending the data samples to BSM. When this option is selected, the Field Mapping panel is not available.</p> <p>Default value: Not selected</p>

UI Element	Description
Topology script	<p>Script to create the topology in BSM for the samples retrieved from the monitored third-party application. The script is based on the Jython scripting language (Python enabled by Java). The monitor propagates its status to the CIs mapped in this topology. The template options displayed depend on the data type selected in the Field Mapping panel.</p> <p>For Event data type:</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 Computer or Running Software CIs. • Computer. Creates a topology with a Computer CI. Available for Common Event samples only. • Computer - Running Software. Creates a topology with a Computer CI and a Running Software CI connected to it with a <code>Composition</code> relationship. Available for Common Event samples only. <p>Note: Legacy Event samples (Node and Node - Running Software) are also available. For details, see Legacy Topology Scripts.</p> <p>For Metrics data type:</p> <ul style="list-style-type: none"> • Computer - Monitor. Sends the SiteScope topology with SiteScope Monitor and Computer CIs. If selected, the script area is not available. <p>The Computer - Monitor topology integration requires that the names or IP addresses of the nodes that it adds to RTSM are accessible through DNS resolution. To successfully populate a Node CI specified in the <code>TargetName</code> field to RTSM, SiteScope must be able to resolve the node's fully qualified domain name and IP address through a DNS service.</p> <ul style="list-style-type: none"> • No Topology. No topology is sent (although data is still sent). If selected, the script area is not available. <p>For Tickets data type:</p> <ul style="list-style-type: none"> • Tickets. Creates a Business Service CI with an EMS monitor CI connected to it with <code>Monitored By</code> relationship. <p>Note: You should only select Custom if you are familiar with the Jython language, since you must create the topology script in Jython yourself. Depending on the data type you select, we recommend that you begin with and edit one of the predefined scripts.</p> <p>For more details, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.</p>

UI Element	Description
Load Script	Loads the required script for the topology you selected in the Topology template option. If you selected Custom , there is no script to load. The script is based on the Jython scripting language (Python enabled by Java).
Script	<p>The contents of the script are visible in this box. You can edit the script contents in this field using the script editor provided by SiteScope, or you can copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>Note: The topology script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see <i>Editing the Topology Script</i> in the <i>Using SiteScope Guide</i>.</p>
Test Script	<p>Tests the topology script. We recommend that you test the script before running the monitor. This test gives you the results of what events or metrics are forwarded to BSM 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

For information on configuring setting panels that are common to all monitors, see *Common Monitor Settings* in the *Using SiteScope Guide*.

Troubleshooting

Debugging Errors/Troubleshooting

This section describes troubleshooting and limitations when working with the Technology Database Integration monitor.

- 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 **Service Health/Event Log/SiteScope reports**, look in **<BSM 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 Service Health to verify that Service Health received the samples. Open the following file on the Gateway Server machine:
<BSM 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.IgnoredSamples
Logger=${loglevel}, IgnoredSamples.appender`
- `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisher
Samples=${loglevel}, PublishedSamples.appender`

Look at the corresponding log files:

- **<BSM root directory>\logs\mercury_wde\wdeIgnoredSamples.log**
- **<BSM root directory>\logs\mercury_wde\wdePublishedSamples.log**

Chapter 111

Technology Log File Integration Monitor

Note: The Technology Log File Integration monitor was deprecated and is used for backward compatibility only. If you intended to use this monitor (it is supported for BSM 9.1x and earlier versions only), you should contact HP Customer Support for assistance.

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 BSM.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the monitor from the New Monitor Page.

Learn More

This section includes:

- "Technology Log File Integration Monitor Overview" below
- "What Data Is Collected" below

Technology Log File Integration Monitor Overview

Each time that SiteScope runs the Technology Log File Integration monitor, the monitor starts from the point in the log file where it stopped reading the last time the monitor 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 BSM. For details on using back references, see Retaining Content Match Values in the Using SiteScope Guide.

Note: 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 BSM. For examples of regular expressions, see Examples for Log File Monitoring in the Using SiteScope Guide.

What Data Is Collected

The Technology Log File Integration monitor sends to BSM 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 BSM (for presentation in Service Health, Service Level Management, and reports).

The specific data that is forwarded to BSM is controlled by the field mapping script (for script types, see Field Mapping Data Types in the Using SiteScope Guide). You use this script to specify the preferred value fields that you want forwarded. For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide. For best practices and details on configuring the integration (depending on the type of sample data being captured), see How to Deploy Integration Monitors in the Using SiteScope Guide.

Data can also be mapped to a topology to forward data to the correct CI hierarchy in BSM. You can configure topology settings for the monitor by selecting one of the predefined scripts, or configuring your own topology script during monitor creation. For more details on editing the script, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.

Tasks

How to integrate data from a Technology Log File

This section provides the overall flow for setting up the Technology Log File Integration Monitor to work with BSM. If you need more information on performing any of the steps, see [Technology Log File Integration Monitor Settings](#).

This task includes the following steps:

- "Prerequisites" below
- "Analyze the log file to be monitored" below
- "Create a Technology Log File Integration monitor" below
- "Edit the monitor's field mapping" on the next page
- "Edit the monitor's topology settings - optional" on the next page
- "Check the regular expression - optional" on page 893
- "View data from the monitor in BSM" on page 893

1. Prerequisites

Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see [How to Configure the Integration Between SiteScope and BSM in the Using SiteScope Guide](#).

2. Analyze the log file to be monitored

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 monitor.
- Make sure that values are extracted correctly from the line.

For user interface details, see [Regular Expression Tool](#) in the [Using SiteScope Guide](#).

3. Create a Technology Log File Integration monitor

Add a Technology Log File Integration Monitor to SiteScope. For user interface details, see ["Technology Log File Integration Monitor Settings" on page 894](#).

- 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.
- **Name.** It is recommended that the monitor name include the name of the integrated software.
- **Log file path name 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, enter the UNC path in the **Log file path name** field (SiteScope should run under a privileged user for the machine that holds the file), and leave the **Server** box empty.
- **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.

4. Edit the monitor's field mapping

The mapping defines the processing of incoming data and the output sample forwarded to BSM.

Note: The Field Mapping panel is not available when the **Report topology without data** check box is selected in Topology Settings.

- a. In the New Technology Log File Integration Monitor dialog box, expand the **Field Mapping** panel. Select a field mapping type and click **Load File**. For details on field mapping types, see Field Mapping Data Types in the Using SiteScope Guide.

For user interface details, see "Field Mapping" on page 898.

- b. A template script is displayed in the **Field mapping** box. Edit the script to enable SiteScope to retrieve the data from the monitored application that you want to forward to BSM. For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide.

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 `$groupn` label corresponds to the order of the parentheses in the expression:

```
$group0 = (21)
$group1 = (HELLO)
$group2 = (world)
```

5. Edit the monitor's topology settings - optional

In the **Topology Settings** panel, you can create or select a script that creates a topology of configuration items in BSM's RTSM to match your EMS system.

For details on this topic, see [Topology Settings for Technology Integration Monitors in the Using SiteScope Guide](#).

For user interface details, see ["Topology Settings" on page 899](#).

6. **Check the regular expression - optional**

After entering the settings for the Technology Log File Integration Monitor, it is recommended that you perform optimization of the regular expression (for example, to check for problems with use of quantifiers such as `.*`). Use the SiteScope Regular Expression tool to perform the optimization. Update the monitor with any corrections.

For user interface details, see [Regular Expression Tool in the Using SiteScope Guide](#).

7. **View data from the monitor in BSM**

View the data in BSM:

- If you chose and edited the **Common Events/Legacy Events** script in the Field Mapping panel, you can view events in Service Health, System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- If you chose and edited the **Tickets** script in the Field Mapping panel, you can view events in any application that supports SiteScope data, including SiteScope Over Time reports.
- If you chose and edited the **Metrics** script in the Field Mapping panel, you can view the data in any application that supports SiteScope data, including SiteScope Over Time 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 **<BSM root directory>\bin**.
- To troubleshoot problems with data arriving to BSM, see ["Troubleshooting" on page 902](#).

Related workflow

[How to Deploy Integration Monitors in the Using SiteScope Guide](#)

UI Descriptions

Technology Log File Integration Monitor Settings

User interface elements are described below:

UI Element		Description
Monitor Settings		
Server	Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the Browse Servers button to select a server from the local domain, or Add Remote Server to add a new server. Default value: SiteScope Server (the server on which SiteScope is installed)	

UI Element	Description
Log file path name	<p>Path to the log file from which you want to extract data.</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 log on to the remote machine. Select Remote Servers > UNIX Remote Servers for information about which UNIX user account is being used. Remote Windows 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 Windows connection profiles (displayed in the Microsoft Windows remote server list). If an exact match is found for <code>\\remoteserver</code> in the remote Windows 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. It is not necessary to select a remote Windows server if you are using NetBIOS to connect to remote Windows servers. Remote Windows through SSH. Select a remote server from the drop-down list. The path of the log file depends on the type of SSH server installed on the remote Windows server: <ul style="list-style-type: none"> SSH servers that provide a UNIX-like interface (for example, Cygwin OpenSSH): <code>/cygdrive/<drive_letter>/<directory>/filename.log</code> SSH servers that provide a Windows command prompt (for example, OpenSSH for Windows): <code><drive_letter>:\<folder>\filename.log</code> <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>

UI Element	Description
Content match	<p>Text to look for in the log entries. You can also use a 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 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.</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. For details on regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.</p>
Open Tool	<p>Opens the Regular Expression Tool, enabling you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see Regular Expression Tool in the Using SiteScope Guide.</p>
No error if file not found	<p>Keeps the monitor in <code>good</code> status if the file is not found.</p>
Log file encoding	<p>Log file encoding that is used if you are reading a log file whose encoding is different than the SiteScope machine's default encoding.</p> <p>Default value: windows-1252</p>

UI Element	Description
Run alerts	<p>Method for running alerts for this monitor:</p> <ul style="list-style-type: none"> • For each log entry matched. Triggers alerts for each 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 <code>error</code> or <code>warning</code> status in the SiteScope interface, regardless of the results of the content match or if the target log file is not found. The monitor triggers alerts if one or more matching entries are found and the <code>Error if</code> or <code>Warning if</code> thresholds are defined accordingly (for example, setting <code>Error if</code> to the default of <code>matchCount > 0</code>).</p> • Once, after all log entries have been checked. Counts the number of matches and trigger alerts one time. The alert is based on the Error if and <code>Warning if</code> thresholds defined for the monitor. <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 <code><matchDetails></code> 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 email alerts or other alert types that work with template properties.</p> <p>Email alert templates are stored in the <code><SiteScope root directory>\templates.mail</code> directory.</p>
EMS time difference	<p>Value that accounts 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: <code><SiteScope root directory>\logs\bac_integration.log</code>.</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>
Timeout Settings	
Enable timeout	<p>The monitor stops its run after the specified timeout period has been exceeded.</p> <p>Default value: Not selected</p>

UI Element	Description
After timeout, resume reading from end of file	<p>If selected, the monitor resumes reading from the end of the log file during the next run, instead of from the current location.</p> <p>Default value: Selected</p> <p>Note: This setting is only available when Enable timeout is selected.</p>
Status after timeout	<p>The status condition that the monitor goes into if the monitor times out.</p> <p>The status categories include: Error, Warning, Good</p> <p>Default value: Warning</p> <p>Note: This setting is only available when Enable timeout is selected.</p>
Timeout (seconds)	<p>Amount of time, in seconds, that SiteScope should wait before the monitor times out.</p> <p>Default value: 60 seconds</p> <p>Note: This setting is only available when Enable timeout is selected.</p>

Field Mapping

User interface elements are described below:

UI Element	Description
Data Type	<p>Select from the following data types for this integration:</p> <ul style="list-style-type: none"> • Common Events. For details, see Configuring Field Mapping for Common Event Samples in the Using SiteScope Guide. • Legacy Events. For details, see Configuring Field Mapping for Legacy Event Samples in the Using SiteScope Guide. • Metrics. For details, see Configuring Field Mapping for Metrics Samples in the Using SiteScope Guide. • Tickets. For details, see Configuring Field Mapping for Ticket Samples in the Using SiteScope Guide.
Load File	<p>Loads the script that is applicable to the data type selected above.</p>

UI 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 BSM. To enable the integration, you must configure the mapping as required by the environment you are monitoring.</p> <p>The mapping is editable in this box using the script editor provided (you can make the script field read only by right-clicking the script and selecting Configure > Read Only). You can also 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 Field Mapping Data Types in the Using SiteScope Guide.</p>
Test Script	<p>Tests the field mapping script. We recommend that you test the script before running the monitor. This test gives you the results of what events or metrics are forwarded to BSM. 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Topology Settings

User interface elements are described below:

UI Element	Description
Report topology without data	<p>Reports the topology for the integration monitor without sending the data samples to BSM. When this option is selected, the Field Mapping panel is not available.</p> <p>Default value: Not selected</p>

UI Element	Description
Topology script	<p>Script to create the topology in BSM for the samples retrieved from the monitored third-party application. The script is based on the Jython scripting language (Python enabled by Java). The monitor propagates its status to the CIs mapped in this topology. The template options displayed depend on the data type selected in the Field Mapping panel.</p> <p>For Event data type:</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 Computer or Running Software CIs. • Computer. Creates a topology with a Computer CI. Available for Common Event samples only. • Computer - Running Software. Creates a topology with a Computer CI and a Running Software CI connected to it with a <code>Composition</code> relationship. Available for Common Event samples only. <p>Note: Legacy Event samples (Node and Node - Running Software) are also available. For details, see Legacy Topology Scripts.</p> <p>For Metrics data type:</p> <ul style="list-style-type: none"> • Computer - Monitor. Sends the SiteScope topology with Sitescope Monitor and Computer CIs. If selected, the script area is not available. <p>The Computer - Monitor topology integration requires that the names or IP addresses of the nodes that it adds to RTSM are accessible through DNS resolution. To successfully populate a Node CI specified in the <code>TargetName</code> field to RTSM, SiteScope must be able to resolve the node's fully qualified domain name and IP address through a DNS service.</p> <ul style="list-style-type: none"> • No Topology. No topology is sent (although data is still sent). If selected, the script area is not available. <p>For Tickets data type:</p> <ul style="list-style-type: none"> • Tickets. Creates a Business Service CI with an EMS monitor CI connected to it with <code>Monitored By</code> relationship. <p>Note: You should only select Custom if you are familiar with the Jython language, since you must create the topology script in Jython yourself. Depending on the data type you select, we recommend that you begin with and edit one of the predefined scripts.</p> <p>For more details, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.</p>

UI Element	Description
Load Script	Loads the required script for the topology you selected in the Topology template option. If you selected Custom , there is no script to load. The script is based on the Jython scripting language (Python enabled by Java).
Script	<p>The contents of the script are visible in this box. You can edit the script contents in this field using the script editor provided by SiteScope, or you can copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>Note: The topology script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see Editing the Topology Script in the Using SiteScope Guide.</p>
Test Script	<p>Tests the topology script. It is recommended that you test the script before running the monitor. This test gives you the results of what events or metrics are forwarded to BSM 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Troubleshooting

Debugging Errors/Troubleshooting

This section describes troubleshooting and limitations when working with the Technology Log File Integration monitor.

- 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 **Service Health/Event Log/SiteScope reports**, look in **<BSM 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 Service Health to verify that Service Health received the samples. Open the following file on the Gateway Server machine:
<BSM 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.IgnoredSamples
Logger=${loglevel}, IgnoredSamples.appender`
- `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisher
Samples=${loglevel}, PublishedSamples.appender`

Look at the corresponding log files:

- **<BSM root directory>\logs\mercury_wde\wdeIgnoredSamples.log**
- **<BSM root directory>\logs\mercury_wde\wdePublishedSamples.log**

Chapter 112

Technology SNMP Trap Integration Monitor

Note: The Technology SNMP Trap Integration monitor was deprecated and is used for backward compatibility only. If you intended to use this monitor (it is supported for BSM 9.1x and earlier versions only), you should contact HP Customer Support for assistance.

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 BSM containing the SNMP trap values. The third-party EMS systems must be configured to send traps to the SiteScope server.

Note: The **SNMP Trap Tool** is available when configuring this monitor to view SNMP Traps received by SiteScope's SNMP listener (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Trap Tool in the Using SiteScope Guide.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the monitor from the New Monitor Page.

Learn More

This section includes:

- ["Technology SNMP Trap Integration Monitor Overview" below](#)
- ["What Data Is Collected" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)

Technology SNMP Trap Integration Monitor Overview

The Technology SNMP Trap Integration Monitor is useful for integrating traps that your external devices create into the BSM framework. For example, you can use this monitor to forward information from Hewlett Packard Network Node Manager to BSM. For more information, see [Network Node Manager Integration Overview](#) in the [Using SiteScope Guide](#).

What Data Is Collected

The Technology SNMP Trap Integration Monitor collects data that is extracted from any SNMP trap (version 1 and 2) received by SiteScope and sends notifications to BSM 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 BSM (for presentation in Service Health, Service Level Management, reports, or all).

The specific data that is forwarded to BSM is controlled by the field mapping script (for script types, see [Field Mapping Data Types](#) in the [Using SiteScope Guide](#)). You use this script to specify the preferred value fields that you want forwarded. For details on the file structure and syntax, see [Event Handler Structure and Syntax](#) in the [Using SiteScope Guide](#). For best practices and details on configuring the integration (depending on the type of sample data being captured), see [How to Deploy Integration Monitors](#) in the [Using SiteScope Guide](#).

Data can also be mapped to a topology to forward data to the correct CI hierarchy in BSM. You can configure topology settings for the monitor by selecting one of the predefined scripts, or configuring your own topology script during monitor creation. For more details on editing the script, see [Topology Settings for Technology Integration Monitors](#) in the [Using SiteScope Guide](#).

IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see [Support for IP Version 6](#) in the [Using SiteScope Guide](#).

Tasks

How to integrate data from an SNMP trap

This section provides the overall flow for setting up the Technology SNMP Trap Integration Monitor to work with BSM. If you need more information on performing any of the steps, see the section on [Technology SNMP Trap Integration Monitor Settings](#).

This task includes the following steps:

- "Prerequisites" below
- "Configure the relevant software to send SNMP traps to the SiteScope machine" below
- "Use SiteScope SNMP Trap tool to watch if the traps are received" below
- "Create a Technology SNMP Trap Integration monitor" on the next page
- "Edit the monitor's field mapping" on the next page
- "Edit the monitor's topology settings - optional" on the next page
- "View data from the monitor in BSM" on the next page

1. Prerequisites

Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see [How to Configure the Integration Between SiteScope and BSM in the Using SiteScope Guide](#).

2. Configure the relevant software to send SNMP traps to the SiteScope machine

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.

3. Use SiteScope SNMP Trap tool to 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. The Technology SNMP Trap Integration Monitor uses port 162 for receiving traps.

- a. Stop the SiteScope service.
- b. Verify that the SNMP trap port (162) is available—`netstat -na | find "162"` shows no output.
- c. If the port is busy, locate the process or program that uses it (for example the Microsoft SNMP Trap Service) and terminate it.

Note: To see which process uses this port, you can download `tcpview` from <http://live.sysinternals.com/>.

- d. Restart SiteScope.

4. Create a Technology SNMP Trap Integration monitor

Add a Technology SNMP Trap Integration Monitor to SiteScope. For monitor user interface details, see "Technology SNMP Trap Monitor Settings " on page 908.

- 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.
- **Name.** It is recommended that the monitor name include the name of the integrated software.

5. Edit the monitor's field mapping

The mapping defines the processing of incoming data and the output sample forwarded to BSM.

Note: The Field Mapping panel is not available when the **Report topology without data** check box is selected in Topology Settings.

- a. In the New Technology SNMP Trap Integration Monitor dialog box, expand the **Field Mapping** panel. Select a field mapping type and click **Load File**. For details on field mapping types, see Field Mapping Data Types in the Using SiteScope Guide.

For user interface details, see "Field Mapping" on page 908.
- b. A template script is displayed in the **Field mapping** box. Edit the script to enable SiteScope to retrieve the data from the monitored application that you want to forward to BSM. For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide.

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, 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.

6. Edit the monitor's topology settings - optional

In the **Topology Settings** panel, you can create or select a script that creates a topology of configuration items in BSM's RTSM to match your EMS system.

For details on this topic, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.

For user interface details, see "Topology Settings" on page 909.

7. View data from the monitor in BSM

View the data in BSM:

- 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.snmpwalk.org.)
- If you chose and edited the **Common Events/Legacy Events** script in the Field Mapping panel, you can view events in Service Health, System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- If you chose and edited the **Metrics** script in the Field Mapping panel, you can view the data in any application that supports SiteScope data, including SiteScope Over Time 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 **<BSM root directory>\bin**.
- To troubleshoot problems with data arriving to BSM, see "Troubleshooting" on page 913.

Related workflow

How to Deploy Integration Monitors in the Using SiteScope Guide

UI Descriptions

This section includes:

- "Technology SNMP Trap Monitor Settings " below
- "Field Mapping" below
- "Topology Settings" on the next page

Technology SNMP Trap Monitor Settings

User interface elements are described below:

UI Element	Description
Run alerts	<p>Method for running alerts:</p> <ul style="list-style-type: none"> • For each SNMP Trap received from EMS system. The monitor triggers alerts for every matching entry found. When the Technology SNMP Trap Integration Monitor is run in the <code>for each SNMP Trap received from EMS system</code> 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. • Once, after all SNMP Traps from EMS system were received. The monitor counts up the number of matches and triggers alerts based on the <code>Error If</code> and <code>Warning If</code> thresholds defined for the monitor in the Advanced Settings section.
EMS time difference	<p>Value that accounts 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>

Field Mapping

User interface elements are described below:

UI Element	Description
Data Type	<p>Select from the following data types for this integration:</p> <ul style="list-style-type: none"> • Common Events. For details, see Configuring Field Mapping for Common Event Samples in the Using SiteScope Guide. • Legacy Events. For details, see Configuring Field Mapping for Legacy Event Samples in the Using SiteScope Guide. • Metrics. For details, see Configuring Field Mapping for Metrics Samples in the Using SiteScope Guide. • Tickets. For details, see Configuring Field Mapping for Ticket Samples in the Using SiteScope Guide.
Load File	Loads the script that is applicable to the data type selected above.
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 BSM. To enable the integration, you must configure the mapping as required by the environment you are monitoring.</p> <p>The mapping is editable in this box using the script editor provided (you can make the script field read only by right-clicking the script and selecting Configure > Read Only). You can also 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 Field Mapping Data Types in the Using SiteScope Guide.</p>
Test Script	<p>Tests the field mapping script. We recommend that you test the script before running the monitor. This test gives you the results of what events or metrics are forwarded to BSM. 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Topology Settings

User interface elements are described below:

Monitor Reference

UI Element	Description
Report topology without data	Reports the topology for the integration monitor without sending the data samples to BSM. When this option is selected, the Field Mapping panel is not available. Default value: Not selected

UI Element	Description
Topology script	<p>Script to create the topology in BSM for the samples retrieved from the monitored third-party application. The script is based on the Jython scripting language (Python enabled by Java). The monitor propagates its status to the CIs mapped in this topology. The template options displayed depend on the data type selected in the Field Mapping panel.</p> <p>For Event data type:</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 Computer or Running Software CIs. • Computer. Creates a topology with a Computer CI. Available for Common Event samples only. • Computer - Running Software. Creates a topology with a Computer CI and a Running Software CI connected to it with a <code>Composition</code> relationship. Available for Common Event samples only. <p>Note: Legacy Event samples (Node and Node - Running Software) are also available. For details, see Legacy Topology Scripts.</p> <p>For Metrics data type:</p> <ul style="list-style-type: none"> • Computer - Monitor. Sends the SiteScope topology with Sitescope Monitor and Computer CIs. If selected, the script area is not available. <p>The Computer - Monitor topology integration requires that the names or IP addresses of the nodes that it adds to RTSM are accessible through DNS resolution. To successfully populate a Node CI specified in the <code>TargetName</code> field to RTSM, SiteScope must be able to resolve the node's fully qualified domain name and IP address through a DNS service.</p> <ul style="list-style-type: none"> • No Topology. No topology is sent (although data is still sent). If selected, the script area is not available. <p>For Tickets data type:</p> <ul style="list-style-type: none"> • Tickets. Creates a Business Service CI with an EMS monitor CI connected to it with <code>Monitored By</code> relationship. <p>Note: You should only select Custom if you are familiar with the Jython language, since you must create the topology script in Jython yourself. Depending on the data type you select, we recommend that you begin with and edit one of the predefined scripts.</p> <p>For more details, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.</p>

UI Element	Description
Load Script	Loads the required Jython script for the topology you selected in the Topology template option. If you selected Custom , there is no script to load. The script is based on the Jython scripting language (Python enabled by Java).
Script	<p>The contents of the script are visible in this box. You can edit the script contents in this field using the script editor provided by SiteScope, or you can also copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>Note: The topology script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see <i>Editing the Topology Script</i> in the <i>Using SiteScope Guide</i>.</p>
Test Script	<p>Tests the topology script. We recommend that you test the script before running the monitor. This test gives you the results of what events or metrics are forwarded to BSM 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

For information on configuring setting panels that are common to all monitors, see *Common Monitor Settings* in the *Using SiteScope Guide*.

Troubleshooting

This section contains:

- "Basic Troubleshooting Guidelines" below
- "Verify SNMP Trap Reception to SiteScope" below
- "Common Problems and Solutions" on the next page

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 Service Health to verify that Service Health received the samples. Open the following file on the Gateway Server machine:
<BSM 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.IgnoredSamples
Logger=${loglevel}, IgnoredSamples.appender`
- `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisher
Samples=${loglevel}, PublishedSamples.appender`

Refer to the following log files:

- **<BSM root directory>\logs\mercury_wde\wdeIgnoredSamples.log**
- **<BSM 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.

1. 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.
2. 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 monitor reports an Address in use error and the monitor type is unavailable.	Another application or process on the machine where SiteScope is running has bound the port 162, the port used to receive SNMP traps.	You must stop the SiteScope service, terminate the process or service that is using the port, and restart SiteScope.
The SNMP traps are not forwarded to BSM 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.
	The EMS configuration file contains errors.	Click the Test Script button in the Field Mapping panel to verify the field mapping.
	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 operating system.
	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 Service Health/Event Log/SiteScope reports.	Samples were dropped due to missing fields or values.	Check in <BSM root directory>\log\mercury_wde\wdeIgnoredSamples.log .

Chapter 113

Technology Web Service Integration Monitor

Note: The Technology Web Service Integration monitor was deprecated and is used for backward compatibility only. If you intended to use this monitor (it is supported for BSM 9.1x and earlier versions only), you should contact HP Customer Support for assistance.

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 the Web service.

Events, metrics, and topology entry points into BSM are published for external systems to use. For each event, metric, or topology that SiteScope receives, a sample is forwarded to BSM containing the event, metrics, or topology values.

To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the monitor from the New Monitor Page.

Learn More

This section includes:

- ["Technology Web Services Overview" below](#)
- ["What Data Is Collected" below](#)

Technology Web Services Overview

SiteScope supplies a WSDL file which the user can use to create a client code. The client code reports the events, metrics, and/or topology data to SiteScope. The client has several ways to report data to BSM:

- report one event or an array of events (this is for legacy events and has been deprecated)
- report one metric or an array of metrics
- data - an array of key value pairs

What Data Is Collected

The Technology Web Service Integration Monitor collects data that is extracted from any message received by the SiteScope Web service. The monitor processes the data, and then sends the data to BSM which contains the values selected 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 BSM. You should determine if the data is for presentation in the Service Health, Service Level Management, reports, or all.

The specific data that is forwarded to BSM is controlled by the field mapping script (for script types, see [Field Mapping Data Types](#) in the [Using SiteScope Guide](#)). You use this script to specify the preferred value fields that you want forwarded. For details on the file structure and syntax, see [Event Handler Structure and Syntax](#) in the [Using SiteScope Guide](#). For best practices and details on configuring the integration (depending on the type of sample data being captured), see [How to Deploy Integration Monitors](#) in the [Using SiteScope Guide](#).

Data can also be mapped to a topology to forward data to the correct CI hierarchy in BSM. You can configure topology settings for the monitor by selecting one of the predefined scripts, or configuring your own topology script during monitor creation. For more details on editing the script, see [Topology Settings for Technology Integration Monitors](#) in the [Using SiteScope Guide](#).

Tasks

How to Integrate Data into BSM Using Web Service Entry Points

This section provides the overall flow for setting up the Technology Web Service Integration Monitor to work with BSM.

This task includes the following steps:

- "Prerequisites" below
- "Create a Technology Web Service Integration monitor" below
- "Enable the connection to the SiteScope reportMonitorData Web service" below
- "Use the client tool to check connectivity" on the next page
- "Technology Web Service Integration Monitor" on page 915

1. Prerequisites

Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see How to Configure the Integration Between SiteScope and BSM in the Using SiteScope Guide.

2. Create a Technology Web Service Integration monitor

Add a Technology Web Service Integration Monitor to SiteScope. For monitor user interface details, see "Technology Web Service Integration Monitor Settings" on page 925.

3. Enable the connection to the SiteScope reportMonitorData Web service

To enable the connection to the 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.

- a. Open a Web browser 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 BSM. This file is used to create the client stubs that connect to the service and report the data.

- b. 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.

- c. 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.
- d. Run your code and check if you get data in the SiteScope Technology Web Service Integration monitor.

4. Use the client tool to check connectivity

After creating a Technology Web Service Integration monitor in SiteScope, you can check connectivity to the Web service by using the client check tool. This tool sends constant messages to the SiteScope **reportMonitorData** Web service. The messages can be metrics or event messages.

- a. In the **<SiteScope root directory>\conf\ems\webservice\test_client** directory:
 - For events or metrics, run: **test_data_client.bat [Target Host][System ID]**
 - For metrics, run: **test_metrics_client.bat [Target Host][Number of messages to send][System ID][Quality][Time in seconds]**
 - For legacy events (deprecated), run: **test_event_client.bat [Target Host][Number of messages to send][System ID][Severity][Time in seconds]**

where:

- **Target Host** is the address of the SiteScope host which receives the messages.
 - **System ID** is the system ID of the monitor that receives the messages.
 - **Number of messages to send** is the number of messages to send to SiteScope.
 - **Quality** is the severity of metrics when forwarding metrics data (default is 0-3).
- b. If you are forwarding other values to BSM, you must edit the field mapping 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 quality is 3.

If you use the option of running the test, you must activate it on the SiteScope machine and add a Technology Web Service Integration monitor with the system id: **Test Event System ID**.

- c. After running the tool, go to the required SiteScope monitor and see if you received a message (or messages if you sent more than one message). In addition, you can access BSM and see if the data that you sent is displayed.
5. Choose one of the following reporting methods depending on the type of data you want to send:

- **For events, metrics, or topology: configure the reportData method**

Tip: For sending metrics data, it is recommended that you use the **reportMetricObject** and **reportMetricsArray** methods. The **reportMetricsArray** method enables you to

submit metrics in bulk instead of one by one. This is a more efficient method than the `reportMetricObject` method because it involves less network traffic.

You can configure the `reportData` method while creating your SOAP message to send to SiteScope. This method contains a data structure that gets an array of key-value objects (see `DataMessage` object below).

Enter the following service request:

```
<wsdl:message name="reportDataRequest">
  <wsdl:part name="systemId" type="xsd:string" />
  <wsdl:part name="data" type="impl:ArrayOf_tns1_DataMessage" />
</wsdl:message>
```

where:

"systemId" is the unique text ID for the Technology Web Service Integration Monitor instance.

"data" is an array of any data type named `DataMessage` that contains key and value strings:

```
<complexType name="DataMessage">
  <complexContent>
    <extension base="tns1:AbstractMessage">
      <sequence>
        <element name="key" nillable="true" type="soapenc:string" />
        <element name="value" nillable="true" type="soapenc:string" />
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

The service success response is:

```
<wsdl:message name="reportDataResponse">
  <wsdl:part name="reportDataReturn" type="xsd:int" />
</wsdl:message>
```

Example - Sending a common event using the reportData request

The question marks in the following example represent string values.

Example:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:web="http://webservice.soa.monitors.sitescope.mercury.com"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
  <soapenv:Header/>
  <soapenv:Body>
```

```
<web:reportData
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
  <systemId xsi:type="xsd:string"?></systemId>
  <data xsi:type="rep:ArrayOf_tns1_DataMessage" soapenc:arrayType="mes:DataMessage
[]"
    xmlns:rep="http://localhost:8080/SiteScope/services/reportMonitorData"
    xmlns:mes="messages.client.webservice.soa.monitors.sitescope.mercury.com">
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">Title</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">Severity</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">SourceHint</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">CiHint</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">EtiHint</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">ComponentCi</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">HostHint</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">Description</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">Category</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">SubCategory</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">Key</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">CloseKey</key>
    <value xsi:type="soapenc:string"?></value>
  </data>
  <data xsi:type="mes:DataMessage">
    <key xsi:type="soapenc:string">LogOnly</key>
```

```

        <value xsi:type="soapenc:string"?></value>
    </data>
</data>
</web:reportData>
</soapenv:Body>
</soapenv:Envelope>

```

■ For metrics: configure the reportMetricObject method

Use the **reportMetricObject** method to submit a single metric. If you want to submit metrics in bulk, use the **reportMetricsArray** method.

Enter the following service request:

```

<wsdl:message name="reportMetricObjectRequest">
  <wsdl:part name="metric" type="tns1:MetricMessage" />
</wsdl:message>

```

where:

"metric" is one metric or an array of metrics of type `MetricMessage` that contains various value strings:

```

<complexType name="MetricMessage">
  <complexContent>
    <extension base="tns1:AbstractMessage">
      <sequence>
        <element name="measurementName" nillable="true" type="soapenc:string" />
        <element name="measurementValue" nillable="true" type="soapenc:double" />
        <element name="monitorName" nillable="true" type="soapenc:string" />
        <element name="monitorState" nillable="true" type="soapenc:string" />
        <element name="monitorType" nillable="true" type="soapenc:string" />
        <element name="quality" nillable="true" type="soapenc:int" />
        <element name="measurementETI" nillable="true" type="soapenc:string" />
        <element name="measurementCIHint" nillable="true" type="soapenc:string" />
      </sequence>
    </extension>
  </complexContent>
</complexType>

```

The service success response is:

```

<wsdl:message name="reportMetricObjectResponse">
  <wsdl:part name="reportMetricObjectReturn" type="xsd:int" />
</wsdl:message>

```

Example - Sending a metric using the reportMetricObject request

The question marks in the following example represent string values as follows:

- **xsd:double** is a double value
- **xsd:int** is an integer value

- o **xsd:string** is a string value

Example:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:web="http://webservice.soa.monitors.sitescope.mercury.com">
<soapenv:Header/>
<soapenv:Body>
  <web:reportMetricObject
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
  <metric xsi:type="mes:MetricMessage"
    xmlns:mes="messages.client.webservice.soa.monitors.sitescope.mercury.com">
    <sourceTimeStamp xsi:type="xsd:double"?></sourceTimeStamp>
    <targetName xsi:type="xsd:string"?></targetName>
    <timeStamp xsi:type="xsd:double"?></timeStamp>
    <uniqueSystemId xsi:type="xsd:string"?></uniqueSystemId>
    <measurementCIHint xsi:type="xsd:string"?></measurementCIHint>
    <measurementETI xsi:type="xsd:string"?></measurementETI>
    <measurementName xsi:type="xsd:string"?></measurementName>
    <measurementValue xsi:type="xsd:double"?></measurementValue>
    <monitorName xsi:type="xsd:string"?></monitorName>
    <monitorState xsi:type="xsd:string"?></monitorState>
    <monitorType xsi:type="xsd:string"?></monitorType>
    <quality xsi:type="xsd:int"?></quality>
  </metric>
</web:reportMetricObject>
</soapenv:Body>
</soapenv:Envelope>
```

- **For metrics arrays: configure the reportMetricsArray method**

The **reportMetricsArray** method enables you to submit metrics in bulk instead of one by one. This is a more efficient method than the **reportMetricObject** method because it involves less network traffic.

Enter the following service request:

```
<wsdl:message name="reportMetricsArrayRequest">
  <wsdl:part name="metrics" type="impl:ArrayOf_xsd_anyType"/>
</wsdl:message>
```

where:

"metrics" is an array of metrics of the type `ArrayOf_xsd_anyType`, which contains various value strings:

```
<complexType name="ArrayOf_xsd_anyType">
  <complexContent>
    <restriction base="soapenc:Array">
      <attribute ref="soapenc:arrayType" wsdl:arrayType="xsd:anyType[]" />
    </restriction>
  </complexContent>
</complexType>
```

Example - Sending an array of metrics using the reportMetricsArray request

The question marks in the following example represent string values as follows:

- **xsd:double** is a double value
- **xsd:int** is an integer value
- **xsd:string** is a string value

Example:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:web="http://webservice.soa.monitors.sitescope.mercury.com"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
<soapenv:Header/>
<soapenv:Body>
  <web:reportMetricsArray
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
  <metrics xsi:type="rep:ArrayOf_xsd_MetricMessage"
soapenc:arrayType="mes:MetricMessage[]">
  <metric xsi:type="mes:MetricMessage"
    xmlns:mes="messages.client.webservice.soa.monitors.sitescope.mercury.com">
    <sourceTimeStamp xsi:type="xsd:double"?></sourceTimeStamp>
    <targetName xsi:type="xsd:string"?></targetName>
    <timeStamp xsi:type="xsd:double"?></timeStamp>
    <uniqueSystemId xsi:type="xsd:string"?></uniqueSystemId>
    <measurementCIHint xsi:type="xsd:string"?></measurementCIHint>
    <measurementETI xsi:type="xsd:string"?></measurementETI>
    <measurementName xsi:type="xsd:string"?></measurementName>
    <measurementValue xsi:type="xsd:double"?></measurementValue>
    <monitorName xsi:type="xsd:string"?></monitorName>
    <monitorState xsi:type="xsd:string"?></monitorState>
    <monitorType xsi:type="xsd:string"?></monitorType>
    <quality xsi:type="xsd:int"?></quality>
  </metric>
  <metric xsi:type="mes:MetricMessage"
    xmlns:mes="messages.client.webservice.soa.monitors.sitescope.mercury.com">
    <sourceTimeStamp xsi:type="xsd:double"?></sourceTimeStamp>
    <targetName xsi:type="xsd:string"?></targetName>
    <timeStamp xsi:type="xsd:double"?></timeStamp>
    <uniqueSystemId xsi:type="xsd:string"?></uniqueSystemId>
    <measurementCIHint xsi:type="xsd:string"?></measurementCIHint>
    <measurementETI xsi:type="xsd:string"?></measurementETI>
    <measurementName xsi:type="xsd:string"?></measurementName>
    <measurementValue xsi:type="xsd:double"?></measurementValue>
    <monitorName xsi:type="xsd:string"?></monitorName>
    <monitorState xsi:type="xsd:string"?></monitorState>
    <monitorType xsi:type="xsd:string"?></monitorType>
    <quality xsi:type="xsd:int"?></quality>
  </metric>
  </metrics>
  </web:reportMetricsArray>
</soapenv:Body>
</soapenv:Envelope>
```

- **For legacy events (deprecated): configure the reportEvent method**

Enter the following service request:

```
<wsdl:message name="reportEventRequest">
  <wsdl:part name="event" type="tns1:EventMessage" />
</wsdl:message>
```

where:

"event" is one event or an array of events of type `EventMessage` that contains various value strings:

Example:

```
<complexType name="EventMessage">
  <complexContent>
    <extension base="tns1:AbstractMessage">
      <sequence>
        <element name="acknowledgedBy" nillable="true" type="soapenc:string" />
        <element name="attr1" nillable="true" type="soapenc:string" />
        <element name="attr2" nillable="true" type="soapenc:string" />
        <element name="attr3" nillable="true" type="soapenc:string" />
        <element name="attr4" nillable="true" type="soapenc:string" />
        <element name="attr5" nillable="true" type="soapenc:string" />
        <element name="dataSource" nillable="true" type="soapenc:string" />
        <element name="description" nillable="true" type="soapenc:string" />
        <element name="eventId" nillable="true" type="soapenc:string" />
        <element name="instance" nillable="true" type="soapenc:string" />
        <element name="logicalGroup" nillable="true" type="soapenc:string" />
        <element name="monitorGroup" nillable="true" type="soapenc:string" />
        <element name="object" nillable="true" type="soapenc:string" />
        <element name="origSeverityName" nillable="true" type="soapenc:string" />
        <element name="owner" nillable="true" type="soapenc:string" />
        <element name="severity" nillable="true" type="soapenc:int" />
        <element name="status" nillable="true" type="soapenc:string" />
        <element name="subject" nillable="true" type="soapenc:string" />
        <element name="targetIp" nillable="true" type="soapenc:string" />
        <element name="value" nillable="true" type="soapenc:double" />
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

The service response is:

```
<wsdl:message name="reportEventResponse">
  <wsdl:part name="reportEventReturn" type="xsd:int" />
</wsdl:message>
```

Related workflow

[How to Deploy Integration Monitors in the Using SiteScope Guide](#)

UI Descriptions

This section includes: <optional signposting - if use, change to PrintOnly condition - use if section content goes over several pages>

- "Technology Web Service Integration Monitor Settings" below
- "Field Mapping" below
- "Topology Settings" on the next page

Technology Web Service Integration Monitor Settings

User interface elements are described below:

UI Element	Description
System ID	Text system ID for the Technology Web Service Integration Monitor instance. 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 must be unique for all monitors. Enter the system id that represents the messages that you want this monitor to receive.

Field Mapping

User interface elements are described below:

UI Element	Description
Data Type	Select from the following data types for this integration: <ul style="list-style-type: none"> • Common Events. For details, see Configuring Field Mapping for Common Event Samples in the Using SiteScope Guide. • Legacy Events. For details, see Configuring Field Mapping for Legacy Event Samples in the Using SiteScope Guide. • Metrics. For details, see Configuring Field Mapping for Metrics Samples in the Using SiteScope Guide. • Tickets. For details, see Configuring Field Mapping for Ticket Samples in the Using SiteScope Guide.
Load File	Loads the script that is applicable to the data type selected above.

UI 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 BSM. To enable the integration, you must configure the mapping as required by the environment you are monitoring.</p> <p>The mapping is editable in this box using the script editor provided (you can make the script field read only by right-clicking the script and selecting Configure > Read Only). You can also 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 Field Mapping Data Types in the Using SiteScope Guide.</p> <p>Note: All parameters in the field mapping should be in the format <code>logical_group</code> and not <code>logicalGroup</code>. Therefore, the target name parameter should be filled as follows:</p> <pre>target_name=resolveHostName (\$target_name)</pre>
Test Script	<p>Tests the field mapping script. We recommend that you test the script before running the monitor. This test gives you the results of what events or metrics are forwarded to BSM. 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

Topology Settings

User interface elements are described below:

UI Element	Description
Report topology without data	<p>Reports the topology for the integration monitor without sending the data samples to BSM. When this option is selected, the Field Mapping panel is not available.</p> <p>Default value: Not selected</p>

UI Element	Description
Topology script	<p>Script to create the topology in BSM for the samples retrieved from the monitored third-party application. The script is based on the Jython scripting language (Python enabled by Java). The monitor propagates its status to the CIs mapped in this topology. The template options displayed depend on the data type selected in the Field Mapping panel.</p> <p>For Event data type:</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 Computer or Running Software CIs. • Computer. Creates a topology with a Computer CI. Available for Common Event samples only. • Computer - Running Software. Creates a topology with a Computer CI and a Running Software CI connected to it with a <code>Composition</code> relationship. Available for Common Event samples only. <p>Note: Legacy Event samples (Node and Node - Running Software) are also available. For details, see Legacy Topology Scripts.</p> <p>For Metrics data type:</p> <ul style="list-style-type: none"> • Computer - Monitor. Sends the SiteScope topology with Sitescope Monitor and Computer CIs. If selected, the script area is not available. <p>The Computer - Monitor topology integration requires that the names or IP addresses of the nodes that it adds to RTSM are accessible through DNS resolution. To successfully populate a Node CI specified in the <code>TargetName</code> field to RTSM, SiteScope must be able to resolve the node's fully qualified domain name and IP address through a DNS service.</p> <ul style="list-style-type: none"> • No Topology. No topology is sent (although data is still sent). If selected, the script area is not available. <p>For Tickets data type:</p> <ul style="list-style-type: none"> • Tickets. Creates a Business Service CI with an EMS monitor CI connected to it with <code>Monitored By</code> relationship. <p>Note: You should only select Custom if you are familiar with the Jython language, since you must create the topology script in Jython yourself. Depending on the data type you select, we recommend that you begin with and edit one of the predefined scripts.</p> <p>For more details, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.</p>

UI Element	Description
Load Script	Loads the required Jython script for the topology you selected in the Topology template option. If you selected Custom , there is no script to load. The script is based on the Jython scripting language (Python enabled by Java).
Script	<p>The contents of the script are visible in this box. You can edit the script contents in this field using the script editor provided by SiteScope, or you can copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>Note: The topology script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see Editing the Topology Script in the Using SiteScope Guide.</p>
Test Script	<p>Tests the topology script. We recommend that you test the script before running the monitor. This test gives you the results of what events or metrics are forwarded to BSM 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

Troubleshooting

Debugging Errors/Troubleshooting

This section describes troubleshooting and limitations when working with the Technology Web Service Integration monitor.

- Check for errors in the following files:

<SiteScope root directory>\logs\error.log

<SiteScope root directory>\logs\RunMonitor.log

<SiteScope root directory>\logs\bac_integration\bac_integration.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 BSM Service Health, Event Log, or SiteScope reports, look in **<BSM 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 Service Health to verify that Service Health received the samples. Open the following file on the Gateway Server machine:

<BSM 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:

- **<BSM root directory>\logs\mercury_wde\wdeIgnoredSamples.log**
- **<BSM root directory>\logs\mercury_wde\wdePublishedSamples.log**