HP Operations Smart Plug-in for Microsoft Enterprise Servers

For HP Operations Manager for Windows®

Software Version: 7.10

PDF version of the online help

This document is a PDF version of the online help that is available in the Microsoft Active Directory SPI. It is provided to allow you to print the help, should you want to do so. Note that some interactive topics are not included because they will not print properly, and that this document does not contain hyperlinks.

Document Release Date: March 2009

Software Release Date: October 2008

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

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

AMD is a trademark of Advanced Micro Devices, Inc.

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

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

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

Windows Vista™ is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

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.

Support

You can 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 Support Online 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 HP Software 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 find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

TABLE OF CONTENTS

Smart Plug-in for Microsoft Enterprise Servers 3
- Getting started 5
  - Service Discovery 7
    - Deploying discovery policies 8
    - Creating service maps 10
  - Graphs 12
  - Policies 14
  - Reports 16
  - Installing reports with HP Reporter 18
  - Troubleshooting 19
  - Self Healing Info tool 20
  - Uninstalling 21
- Application Center Server 23
  - Application Center Server service map 25
  - Application Center Server policies 27
  - Application Center Server reports 37
  - Application Center Server graphs 39
- BizTalk Server 40
  - Configuring for BizTalk 2004 and 2006 44
  - BizTalk Server service map 45
  - BizTalk Server policies 48
    - BizTalk Server 2000 policies 49
    - BizTalk Server 2002 policies 55
    - BizTalk Server 2004 policies 63
    - BizTalk Server 2006 policies 70
  - BizTalk Server reports 77
    - BizTalk 2002 Server Reports 79
    - BizTalk 2004 Server reports 82
    - BizTalk 2006 Server reports 85
  - BizTalk Server graphs 88
  - BizTalk Server tools 91

Self Healing Info 20
Commerce Server 96
Commerce Server service map 98
Commerce Server policies 100
Commerce Server reports 107
Commerce Server graphs 111
Commerce Server troubleshooting 113
Content Management Server 114
Content Management Server service map 118
Content Management Server policies 119
Content Management Server reports 123
Content Management Server graphs 127
Internet Security and Acceleration Server 129
ISA Server service map 131
ISA Server 2000 policies 134
ISA Server 2006 policies 139
ISA Server reports 149
ISA Server graphs 154
SharePoint Portal Server 157
SharePoint Portal Server service map 158
SharePoint Portal Server 2001 162
SharePoint Portal Server 2001 policies 164
SharePoint Portal Server 2001 reports 167
SharePoint Portal Server 2001 graphs 169
SharePoint Portal Server 2003 171
SharePoint Portal Server 2003 policies 173
SharePoint Portal Server 2003 reports 180
SharePoint Portal Server 2003 graphs 183
Sharepoint Portal Server 2007 186
SharePoint Portal Server 2007 policies 190
SharePoint Portal Server 2007 reports 198
SharePoint Portal Server 2007 graphs 200

HP Operations Smart Plug-in for Microsoft Enterprise Servers

The HP Operations Smart Plug-in for Microsoft Enterprise Servers (Microsoft Enterprise Servers SPI) provides pre-configured policies, reports and graphs for managing the operations and performance of the following Microsoft Enterprise Servers:

- Application Center 2000
- BizTalk Server 2000, 2002, 2004 and 2006
- Commerce Server 2000 and 2002
- Content Management Server 2001 and 2002
- Internet Security and Acceleration Server 2000 and 2006
- SharePoint Portal Server 2001 and 2003.

The Microsoft Enterprise Servers SPI offers:

- **Topology/Service Mapping:** the Microsoft Enterprise Servers SPI discovers and maps Microsoft Enterprise Servers on your network. The servers are displayed in the service map, showing dependencies to other systems where appropriate.
- **Availability Monitoring:** the Microsoft Enterprise Servers SPI monitors the services that need to run to ensure complete availability of your Microsoft Enterprise Servers.
- **Performance Monitoring:** the Microsoft Enterprise Servers SPI monitors Windows performance counters, notifying you if thresholds are exceeded.
- **Event Log Monitoring:** the Microsoft Enterprise Servers SPI monitors the Windows Event Logs.
- **Reporting and Graphing:** the Microsoft Enterprise Servers SPI creates reports and graphs that show historical data and trend information based on the logged data. This can be used for capacity planning and SLA compliance.
- **Troubleshooting** assistance with the Self Healing Info tool .

NOTE:
Smart Plug-ins are available for the Exchange Server and SQL Server as separate products. Host Integration Server 2000 and Mobile Information Server 2000 are now monitored by the Windows OS SPI.

- Application Center Server Overview
- BizTalk Server Overview
- Commerce Server Overview
- Content Management Server Overview
- Internet Security and Acceleration Server Overview
- Sharepoint Portal Server Overview

NOTE:
The online help for the Microsoft Enterprise Servers SPI provides information specific to the discovery of services and the deployment of policies for the Microsoft Enterprise Servers.
Refer to the HPOM online help for information about all other topics, such as Configure managed nodes , HP Reporter Integration , and HP Performance Manager Integration .

Related Topics:

- Getting Started
- Configuring the Microsoft Enterprise Servers SPI for BizTalk Server

Getting started with Microsoft Enterprise Servers SPI

The Microsoft Enterprise Servers SPI provides a set of pre-configured policies that enable you to monitor the operations and performance of your Microsoft Enterprise Servers. The deployment of policies allows systems to begin collecting data.

The Microsoft Enterprise Servers SPI is designed to help you start monitoring your systems as quickly as possible by automating the discovery of services and the deployment of policies. Since many tasks are automated, plan ahead by identifying the systems you want to manage and the information you want to collect.

This is the recommended order in which to perform tasks:

> **NOTE:**
> Perform these steps for each type of Microsoft Enterprise Server you want to monitor.

1. Evaluate the policies that are located in the Auto-Deploy policy group. Delete policies you do not want to deploy automatically.
2. Optionally, make modifications to the default values of the policies remaining in the Auto-Deploy group.
3. Configure the Windows nodes you want to monitor.
4. Discover the Microsoft Enterprise Servers:

   For most servers this occurs automatically, but for the following servers the Discovery Policy group must be manually deployed after editing the individual Discovery policies to include server administrator user and password information:

   - Application Center Servers
   - BizTalk Servers
   - SharePoint Portal Server 2003
5. Policies in the Auto-Deploy group are then automatically deployed.
6. Optionally deploy policies in the Manual-Deploy group.

7. View the Service Map to see the Microsoft Enterprise Server hierarchy and dependencies.

Related Topics:

- Configuring the Microsoft Enterprise Servers SPI for BizTalk Server
- Using Policies
- Modifying Policies
- Discovering Microsoft Enterprise Servers
- Deploying Discovery Policies for Microsoft Enterprise Servers
- Deploying Policies for Microsoft Enterprise Servers
- Creating Service Maps for Microsoft Enterprise Servers

Discovering Microsoft Enterprise Servers

After configuring your nodes, the next step is to discover the servers on those nodes. For most of the Microsoft Enterprise Servers, the discovery is automatic. For BizTalk and Application Center Servers, deploy the Discovery Policy group.

Auto Discovery If the Microsoft Enterprise Server does not require a specific administrator user name and password, then the Discovery Policy is automatically deployed. This happens for the following Microsoft Enterprise Servers:

- Commerce Server
- Content Management Server
- Internet Security and Acceleration Server

Manual Discovery If the Microsoft Enterprise Server application requires a server administrator user name and password, then the Discovery Policy group must be manually deployed. The following servers require manual deployment of Discovery Policies:

- Application Center Server
- BizTalk Server
- SharePoint Portal Server

Within each Discovery policy group is a Discovery error policy which tracks errors in the discovery process and forwards this information in messages to the console.

> **NOTE:**
> If the Microsoft Enterprise Servers SPI is installed **after** the nodes have been configured, deploy the discovery policy groups manually for all Microsoft Enterprise servers.

Related Topics:

- Configuring the Microsoft Enterprise Servers SPI for BizTalk Server
- Deploying Discovery Policies for Microsoft Enterprise Servers
- Using Policies for Microsoft Enterprise Servers

Deploying discovery policies for Microsoft Enterprise servers

For most of the Microsoft Enterprise Servers, the discovery of servers is automatic. However, if the Microsoft Enterprise Server application requires a specific administrator user name and password, then the Discovery Policy must be edited and manually deployed. This is true for the following servers:

- Application Center Server--Edit and deploy the Discovery policy group
- BizTalk Server--Edit one Discovery policy and deploy the Discovery policy group
- SharePoint Portal Server--Edit and deploy the Discovery policy group.

The deployment is a two-step process. First, the policies need to be edited to include the administrator's user name and password for the Microsoft Enterprise Server. Next, deploy the policy folder.

Edit the Policy

This example explains how to edit a discovery policy for the Application Center 2000 Server:

1. From the console tree, select **Policy management** → **Policy groups** → **SPI for Microsoft Enterprise Servers** → **Application Center 2000** → **Discovery** .
2. Select **NET_ApplicationCenter2000_Discovery** and double-click to open the editor. The **Discover** tab displays, and the **System Infrastructure** entry is expanded by default.
3. Click **Application Center Cluster** .
4. Any editable parameters display in the **User Editable Parameters** box. For Microsoft Enterprise Servers, these will be **User** and **Password** .
5. Select a parameter and type in the field beside it. For Application Center, enter the administrator User name and Password for the Application Center Server. The fully-qualified domain name is required.
6. Click the **Save and Close** button.

Deploy the Discovery Policy Folder

1. Select the policy folder.
2. Right-click and select **All Tasks** → **Deploy On** .

3. Select the nodes or node groups to which you want to deploy.
4. Select **OK** .

You can watch the progress of the deployment by clicking on the Deployment Jobs icon in the console tree. Only active, failed, or suspended deployment jobs are shown. (If a deployment job fails, the icon in the console tree turns red.)

Refer to the policy section for the names of the individual discovery policies.

> **NOTE:**
> You can also deploy policies or policy groups using a drag-and-drop operation.

Related Topics:

- Discovering Microsoft Enterprise Servers
- Using Policies

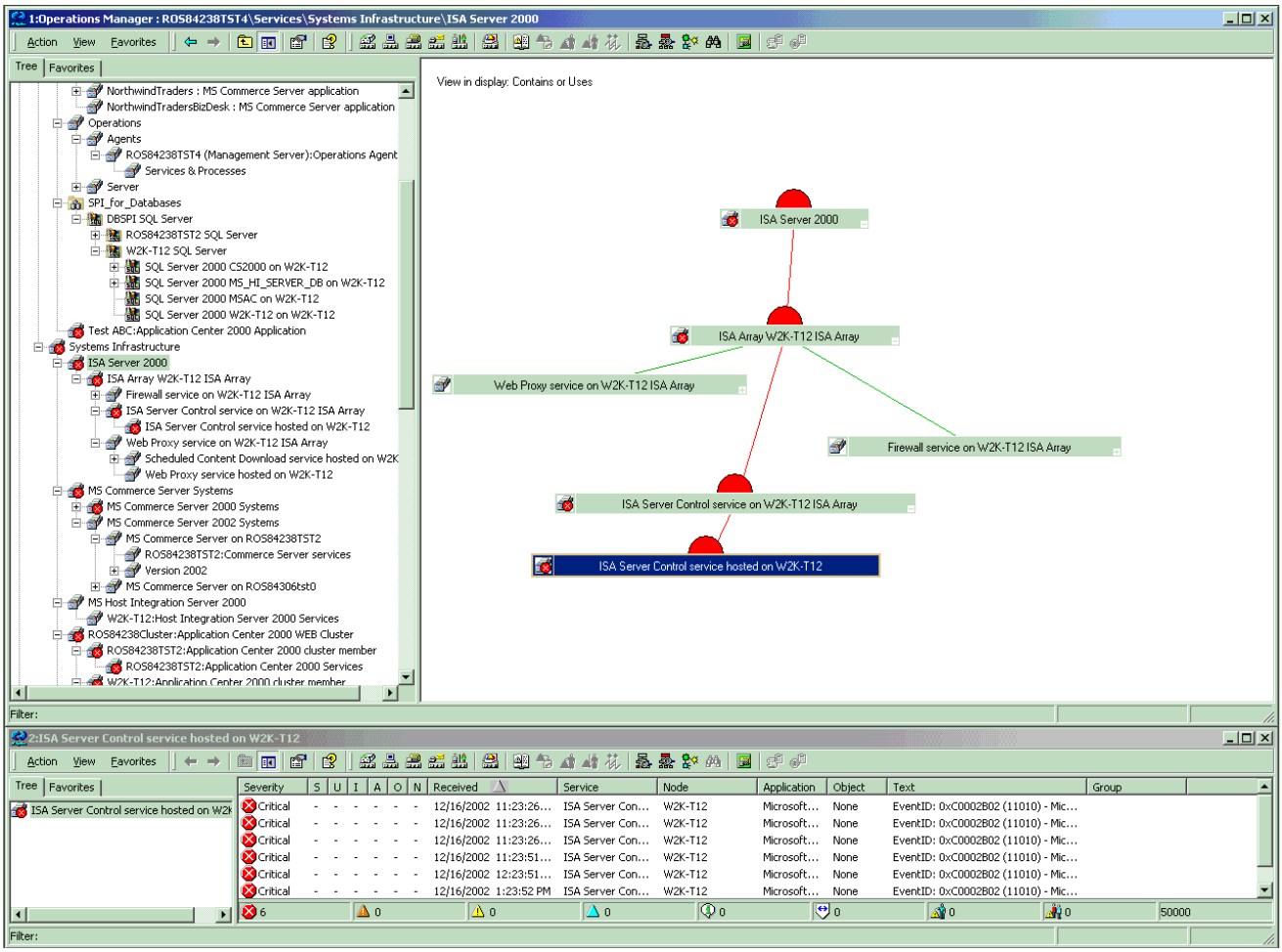
Creating service maps for Microsoft Enterprise Servers

The service maps for Microsoft Enterprise Servers graphically represent the connections between Microsoft Enterprise Servers and their related applications and infrastructure. These maps give you visual information about components and dependencies. At a glance, you can monitor your Microsoft Enterprise Servers. Then, use the Message Browser to gain more detailed troubleshooting information.

Service maps are automatically created after the servers are discovered. Follow the procedure for Discovering Microsoft Enterprise Servers to create the service maps. Do this for each type of Microsoft Enterprise Server you manage.

Additional information about each Microsoft Enterprise Server service map is located within the specific Microsoft Enterprise Server help topic.

The graphic below shows the relationship between the console, the service map, and the message browser. In this instance, the map shows that there is a critical problem (denoted in red) with the Internet Security and Acceleration Server services on the ISA Server Control service hosted on W2k-T12. Detailed information is available by viewing the message browser, displayed in the bottom pane.



Related Topics:

- Getting Started
- Discovering Microsoft Enterprise Servers
- Application Center Server Service Map
- BizTalk Server Service Map
- Commerce Server Service Map
- Content Management Server Service Map
- Internet Security and Acceleration Server Service Map
- SharePoint Portal Server Service Map
- Configuring the Microsoft Enterprise Servers SPI for BizTalk Server

Graphs for Microsoft Enterprise Servers

The Microsoft Enterprise Servers SPI includes a set of pre-defined graphs. Graphs for the Microsoft Enterprise Servers are located in the **Graphs** folder in the console tree.

Deployment of the following policies is required:

1. The Windows OS SPI logging policy WINOSSPI-WINOS_Win2k_Logging
2. The Microsoft Enterprise Server Logging policy, or policies, specific to the Microsoft Enterprise Servers in your environment:
   - Application Server -- **NET_ACServer2000_Logging**
   - BizTalk Server -- **NET_BizTalkServer_Logging** and **NET_BizTalkServer2002_Logging**
   - Commerce Server -- **NET_CommerceServer_Logging** and **NET_CommerceServer2002_Logging**
   - Content Management Server -- **NET_CMS_Logging** **NET_HostIntegrationServer2000_Logging**
   - Internet Security and Acceleration Server: **NET_ISAServer_Logging** and **NET_MobileInformationServer_Logging**
     In addition, for ISA 2006 graphs you must deploy the following policies:
     - ISA2006_Logging_Firewall
     - ISA2006_Logging_Jobscheduler
     - ISA2006_Logging_Servercache
     - ISA2006_Logging_Servercontrol
     - ISA2006_Logging_WebProx
   - SharePoint Portal Server -- **NET_SPS_Logging** and **NET_SPS_WorkspaceLogger**

Refer to the topics below for information about graphs specific to a Microsoft Enterprise Server.

Related Topics:

- Application Center Server Graphs
- BizTalk Server Graphs
- Commerce Server Graphs
- Content Management Server Graphs

- Internet Security and Acceleration Server Graphs
- SharePoint Portal Server Graphs

Policies for Microsoft Enterprise Servers

All policies for the Microsoft Enterprise Servers are located under Policy management, in the SPI for Microsoft Enterprise Servers Policy group.

From the console tree, select **Policy management → Policy groups → SPI for Microsoft Enterprise Servers** .

Each Microsoft Enterprise Server has its own set of three policy groups:

- Auto-Deploy
- Discovery
- Manual-Deploy

The policies contained in the Auto-Deploy policy group and the Manual-Deploy policy group are identical, and contain policies that define the rules for collecting data. The Discovery policy group contains policies that discover your Microsoft Enterprise Servers.

Auto-Deploy

The Auto-Deploy feature automates deployment, saving you time. After the Microsoft Enterprise servers have been discovered, the policies in the Auto-Deploy group are automatically deployed to those servers.

To disable auto-deployment for a particular server, on the HPOM console right-click **Services** , select **Configure → Service Types.** With one of the **Service Types** selected, click **Properties** , in the Application Services Properties dialog, open the **Deployment** tab and check **Disable Automatic Deployment of Policies** . In addition:

- You can delete policies from the Auto-Deploy group if you do not want them deployed automatically after servers are discovered.
- You can modify the policies prior to deployment to customize them for your environment.

If this is the first time the Microsoft Enterprise Servers SPI has been installed, you may want to remove or modify policies prior to configuring your nodes. Policies can be also be modified or removed after they are deployed.

Manual-Deploy The Manual-Deploy feature gives you more control. You choose which policies to deploy and when to deploy them. Polices must be removed from the Auto-Deploy group to avoid auto-deployment of policies.

Discovery The Discovery policy group contains policies that discover your Microsoft Enterprise Servers. For most of the Microsoft Enterprise Servers, the discovery is automatic. For others, deploy the Discovery Policy group manually.

For a list of the policies and their descriptions, see the policy section for each Microsoft Enterprise Server topic.

Related Topics:

- Deploying Policies
- Modifying Policies
- Deleting Policies
- Discovering Microsoft Enterprise Servers
- Deploying Discovery Policies for Microsoft Enterprise Servers
- Application Center Server Policies
- BizTalk Server Policies
- Content Management Server Policies
- Commerce Server Policies
- Internet Security and Acceleration Server 2000 Policies
- Internet Security and Acceleration Server 2006 Policies
- SharePoint Portal Server Policies

Reports for Microsoft Enterprise Servers

The Microsoft Enterprise Servers SPI includes a set of pre-configured, read-only reports for each Microsoft Enterprise Server. These reports provide graphical representations of data that is collected by agents on the managed nodes in your environment.

Reports for the Microsoft Enterprise Servers are located in the **Reports** folder in the console tree.

Deployment of the following policies is required:

1. The Windows OS SPI logging policy WINOSSPI-WINOS_Win2k_Logging
2. The Microsoft Enterprise Server Logging policy, or policies, specific to the Microsoft Enterprise Servers in your environment:
   - Application Server: **NET_ACServer2000_Logging**
   - BizTalk Server: **NET_BizTalkServer_Logging** and **NET_BizTalkServer2002_Logging**
   - Commerce Server: **NET_CommerceServer_Logging** and **NET_CommerceServer2002_Logging**
   - Content Management Server: **NET_CMS_Logging**NET_HostIntegrationServer2000_Logging
   - Internet Security and Acceleration Server: **NET_ISAServer_Logging** and **NET_MobileInformationServer_Logging**
     In addition, for ISA 2006 you must deploy the following policies:
     - ISA2006_Logging_Firewall
     - ISA2006_Logging_Jobscheduler
     - ISA2006_Logging_Servercache
     - ISA2006_Logging_Servercontrol
     - ISA2006_Logging_WebProxy
   - SharePoint Portal Server: **NET_SPS_Logging** and **NET_SPS_WorkspaceLogger**

NOTE:
- Since reports are generated nightly, the current day's information is not immediately available for viewing.
- Reports use the standard international format for dates: *yyyy-mm-dd* , and the 24 hr clock: *hh.mm.*

Refer to the topics below for information about reports specific to any Microsoft Enterprise Server.

Related Topics:

- Installing Microsoft Enterprise Servers Reporter Package into HP Reporter
- Application Center Server Reports
- BizTalk Server Reports
- Commerce Server Reports
- Content Management Server Policies
- Internet Security and Acceleration Server Reports
- SharePoint Portal Server Policies

Installing Microsoft Enterprise Servers SPI reports with Reporter

If you have purchased the HP Reporter product, the Microsoft Enterprise Servers SPI reports must be installed on the system where HPOM resides.

Two components are required to allow Microsoft Enterprise Servers SPI data to be available to HP Reporter.

- Windows OS SPI Reporter package
- Microsoft Enterprise Servers SPI Reporter package

Install Reports

1. Insert the HP Operations Smart Plug-in DVD in the DVD-ROM drive of the HP Reporter system.
2. Run the following programs, in the listed order, to install the reporter packages:
    1. -Windows OS SPI Reporter Package\WINOSSPI-Reporter.msi
    2. -Microsoft Enterprise Servers SPI Reporter Package\Microsoft Enterprise Servers SPI-Reporter.msi
3. Check the Reporter status pane to note changes to Reporter configuration.

Related Topics:

- Using Reports for Microsoft Enterprise Servers

Troubleshoot Microsoft Enterprise Servers SPI

Some troubleshooting information is available in the online help. An additional resource for technical information is the HP Software Support Online support site.

Click this link to open the Software Support Online web site in a separate browser window.

Related Topics:

- Troubleshoot Commerce Server
- Troubleshoot Microsoft Enterprise Servers SPI reports and graphs

Using the Self Healing Info tool

The Self-Healing Info tool gathers system information, and configuration, log, and trace Microsoft Enterprise Servers SPI files, for assisting to troubleshoot problems. Gathered information and files are placed in a pre-defined output directory. The data collector gathers real-time data, which reduces the probability of troubleshooting with stale data.
Whenever you encounter a problem with the Microsoft Enterprise Servers SPI, run the data collector by launching the Self-Healing Info tool in the SPI for Microsoft Enterprise Servers **Tools** group.

To launch the Self-Healing Info tool on the node from which you want to gather data:

1. Right-click the **Self-Healing Info** tool in the **Tools** → **SPI for Microsoft Enterprise Servers** group.
2. Select **All Tasks**, then click **Launch Tool** .
3. Select the node to which the data collector has to be launched, and click **Launch** .
4. You are notified where the output file is placed. Submit this file to HP Support for assistance, or use the file to identify and correct the problem you encountered.

Related Topics:

- Troubleshoot the Microsoft Enterprise Servers SPI

Uninstalling the Microsoft Enterprise Servers SPI

To uninstall the Microsoft Enterprise Servers SPI:

- remove all Microsoft Enterprise Servers SPI policies from the managed nodes
- uninstall Microsoft Enterprise Servers SPI programs from the management server
- delete the Microsoft Enterprise Servers SPI policy group from the management server.

NOTE: If you need to retain the previous install log file, save it to another location before you begin the uninstall process.

Task 1: Remove all SPI for Microsoft Enterprise Servers policies from the managed nodes

1. In the console expand the folder **Policy Management** .
2. Right-click **SPI for Microsoft Enterprise Servers** and select **All tasks** → **Uninstall from...**
3. In the **Uninstall policies on...** window, check the nodes from which the policies should be removed. Click **OK** .
4. To check which policies are installed on any node: in the HPOM console expand the **Nodes** folder, right-click a node, and select **View** → **Policy Inventory** .

Task 2: Uninstall Microsoft Enterprise Servers SPI programs from the HPOM management server

1. Insert the HPOM for Windows disk.
2. Follow the instructions as they appear on screen, and start the uninstall procedure by selecting the **Remove products** radio button.
3. In the **Product Selection Uninstall** window select **Microsoft Enterprise Servers SPI** and click **Next** .
4. In the next window select **Remove** . (You are updated on the progress of the program removal).

5. Click **Finish** to complete.

Task 3: Delete the SPI for Microsoft Enterprise Servers policy group from the management server

1. In the console expand the folder **Policy groups** .
2. Right-click **SPI for Microsoft Enterprise Servers** and select **Delete** .

Related Topics:

- Get Started with Microsoft Enterprise Servers SPI
- The Smart Plug-in for Microsoft Enterprise Servers

Application Center Server

Microsoft's Application Center 2000 is the deployment and management tool for administering high-availability Web applications built on the Microsoft Windows 2000 operating system. Using Application Center 2000, organizations can use software scaling to achieve scalability and availability for their Web applications.

Availability Monitoring

Application Center Server services are monitored to determine whether they are up or down. If the service is not running, and the service in startup is set to "Auto Start", then an attempt is made to restart the service. A console error message is sent to indicate that the service is not running. Monitored services include:

- Application Center Cluster Service (accluster.exe)
- Application Center Name Resolution Service (acnameres.exe)
- Application Center Synchronization Service (acsrepl.exe)

Event Monitoring

Event monitoring of the Windows 2000 Event Log occurs for Application Center Server events. Console messages are sent for all errors, warnings, and information events logged for the following sources:

- Application Center
- Health monitor

WMI Event Monitoring

The Application Center Server monitors WMI (Windows Management Instrumentation) events. Console messages are sent for all errors and warnings logged for the following sources:

- Replication Events
- Cluster Events
- Load Balancing Events
- Request Forwarding Events

Performance Monitoring

Application Center Server performance monitoring includes both specific Application Center Server performance counters and CPU process-related counters. Each policy for performance monitoring has both error and warning thresholds.

Server Logging

Selected process-related data for CPU and memory counters is logged for the Application Center Server.

> **NOTE:**
> For Server Logging, deployment of the Windows OS SPI logging policy, WINOSSPI-WINOS_Win2k_Logging, is required to log process-related data for CPU and memory counters. The counters specific to the Application Center Server are documented in the policy section. Refer to the Windows OS SPI Policies for information about the process-related data for CPU and memory counters.

Related Topics:

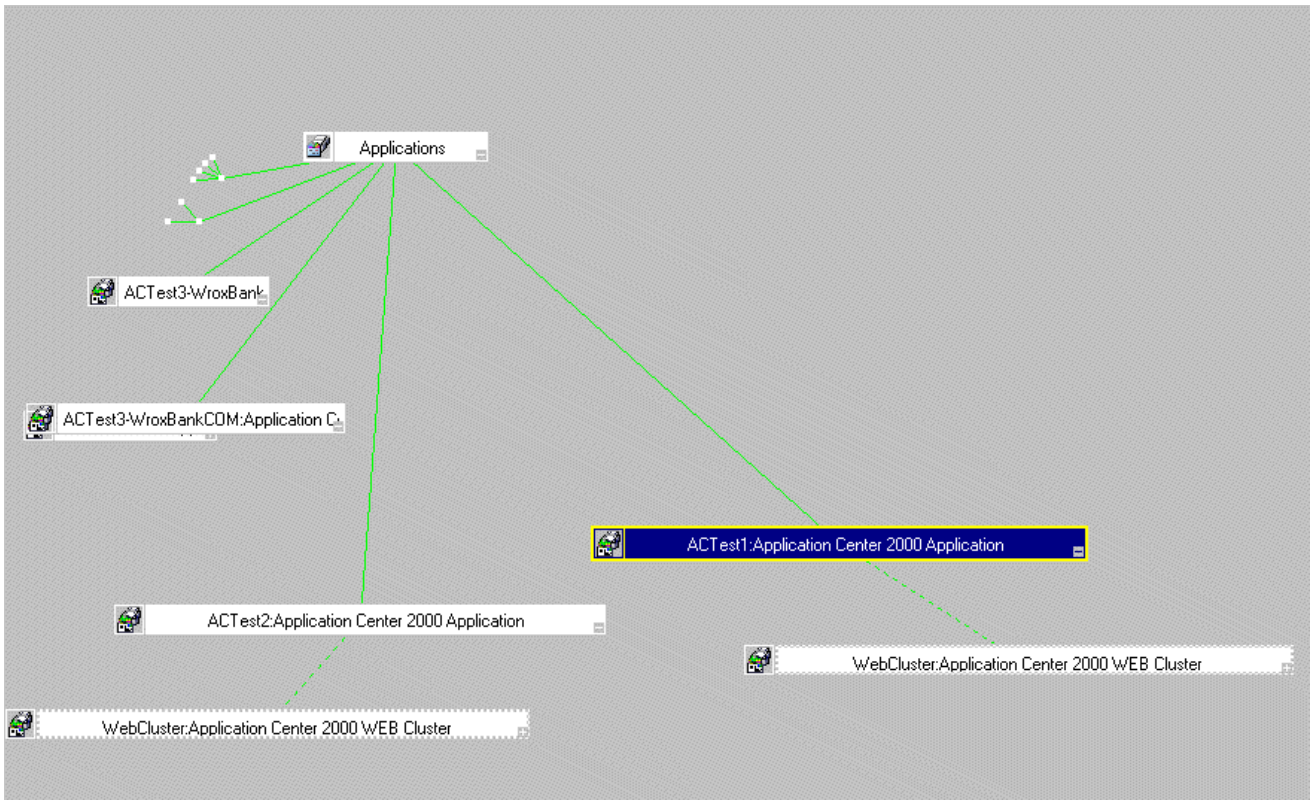
- Application Center Server Policies
- Application Center Server Reports
- Application Center Server Graphs
- Application Center Server Service Map

Application Center Server service map

The Application Center Server service map displays the nodes where Application Center Servers have been installed. The service maps are available under both the Applications and the Systems Infrastructure areas.

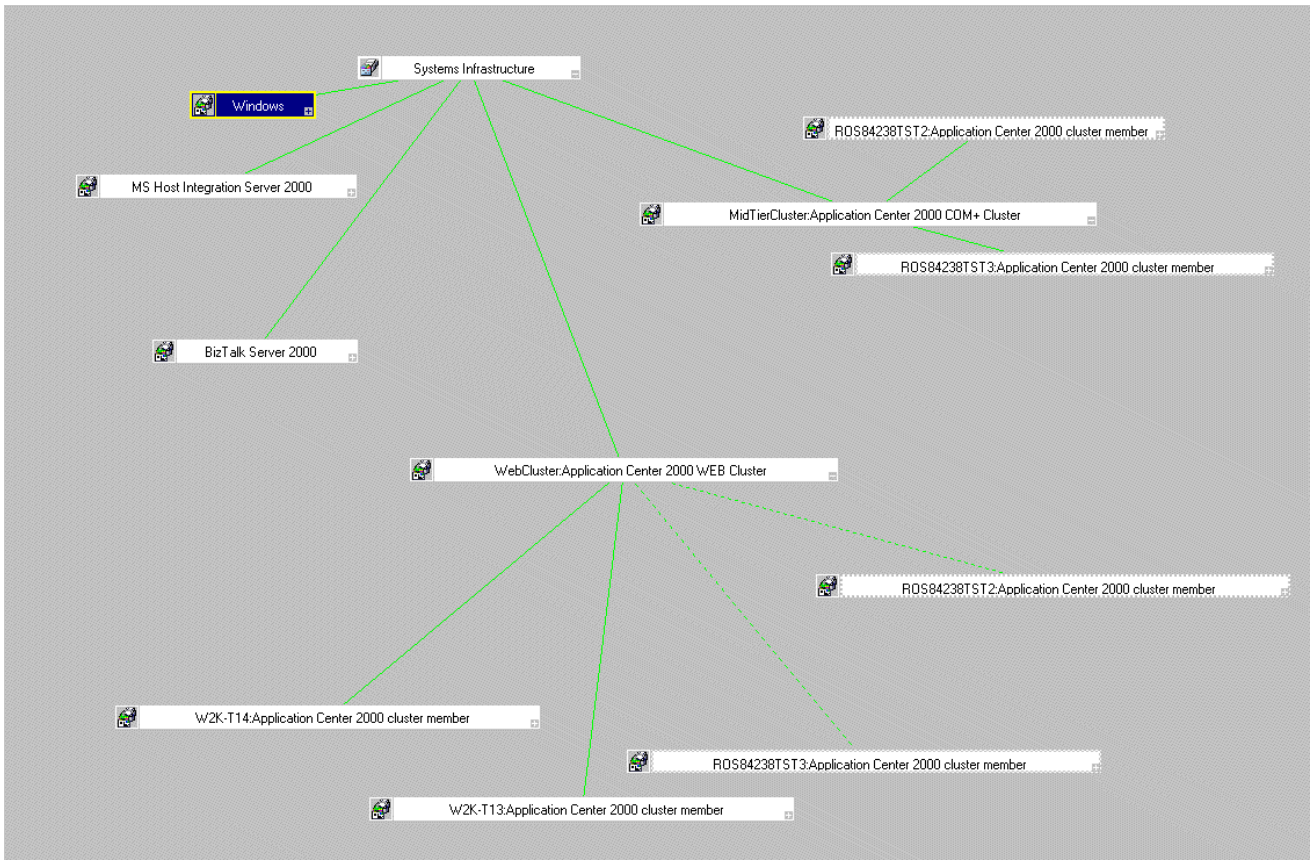
Applications

The service map shows all the applications that are discovered on Application Center 2000 installations. In addition it shows the application's dependencies on the Application Center Cluster (WEB or COM+).



Systems Infrastructure

The service map shows the topology of Application Center 2000 clusters (WEB or COM+) with a node representing the cluster and then each member of the cluster represented as a component of this cluster.



Related Topics:

- Creating Service Maps for Microsoft Enterprise Servers

HP Smart Plug-in for Microsoft Enterprise Servers

Application Center Server policies

Predefined policies for the Application Center Server are available with the Microsoft Enterprise Servers SPI.

- Availability Monitoring
- Windows Event Log Monitoring
- Performance Monitoring
- WMI Event Monitoring
- Server Logging
- Discovery

Availability Monitoring

Policy Descriptions

NET_ACServices

Description: This policy monitors the Application Center Server services: Cluster Service, Name Resolution Service and Synchronization Service. If a service is stopped it is restarted automatically.

Windows Event Log Monitoring

Policy Descriptions

NET_ACFwdApplicationError

Description: Forwards all Application Center Server application log entries with severity 'Error'.

NET_ACFwdApplicationInformation

Description: Forwards all Application Center Server application log entries with severity 'Information'.

NET_ACFwdApplicationWarning

Description: Forwards all Application Center Server application log entries with severity 'Warning'.

Performance Monitoring

Policy Descriptions

NET_AC-PageFaultssec-ClusterService

Description: Checks Process.Page Faults/sec for the Application Center Server 2000 Cluster Service.

NET_AC-PageFaultssec-NameResolutionService

Description: Checks Process.Page Faults/sec for the Application Center Server 2000 Name Resolution Service.

NET_AC-PageFaultssec-SynchronizationService

Description: Checks Process.Page Faults/sec for the Application Center Server 2000 Synchronization Service.

NET_AC-PrivateBytes-ClusterService

Description: Checks Process.Private Bytes for the Application Center 2000 Cluster service.

NET_AC-PrivateBytes-NameResolutionService

Description: Checks Process.Private Bytes for the Application Center 2000 Name Resolution service.

NET_AC-PrivateBytes-SynchronizationService

Description: Checks Process.Private Bytes for the Application Center 2000 Synchronization service.

NET_AC-ProcessorTime-ClusterService

Description: Checks Process.% Processor Time for the Application Center 2000 Cluster service.

NET_AC-ProcessorTime-NameResolutionService

Description: Checks Process.% Processor Time for the Application Center 2000 Name Resolution service.

NET_AC-ProcessorTime-SynchronizationService

Description: Checks Process.% Processor Time for the Application Center 2000 Server Synchronization service.

NET_AC-ThreadCount-ClusterService

Description: Checks Process.Thread Count for the Application Center 2000 Server Cluster service.

NET_AC-ThreadCount-NameResolutionService

Description: Checks Process.Thread Count for the Application Center 2000 Server Name Resolution service.

NET_AC-ThreadCount-SynchronizationService

Description: Checks Process.Thread Count for the Application Center 2000 Server Synchronization service.

NET_AC-WorkingSet-ClusterService

Description: Checks Process.Working Set for the Application Center Server 2000 Cluster service.

NET_AC-WorkingSet-NameResolutionService

Description: Checks Process.Working Set for the Application Center Server 2000 Name Resolution service.

NET_AC-WorkingSet-SynchronizationService

Description: Checks Process.Working Set for the Application Center Server 2000 Synchronization service.

NET_ACReqFwdFailedReqs

Description: Checks Application Center Request Forwarder: Total Failed Requests/sec.

NET_ACTotalReqsFwd

Description: Checks Application Center Request Forwarder: Total Forwarded Requests/sec

NET_ACAdministrationRequests

Description: Checks Application Center Request Forwarder:Total Application Center Administration Requests/sec.

WMI Event Monitoring

Policy Descriptions

NET_ACClusterControllerErrorEvents

Description: Forwards Application Center Cluster Controller Error Events

NET_ACClusterControllerWarningEvents

Description: Forwards Application Center Cluster Controller Warning Events

NET_ACClusterLoadBalancingErrorEvents

Description: Forwards all Application Center Cluster Load Balancing Error Events

NET_ACClusterLoadBalancingInformationEvents

Description: Forwards all Application Center Cluster Load Balancing Information Events

NET_ACClusterMemberDrainEvents

Description: Forwards all Application Center Cluster Server Drain Load Balancing Events

NET_ACClusterMemberOfflineEvent

Description: Forwards all Application Center Cluster Server Offline Load Balancing Events

NET_ACClusterMemberOnlineEvent

Description: Forwards all Application Center Cluster Server Online Load Balancing Events

NET_ACClusterMembershipFailedEvent

Description: Forwards all Application Center Cluster Membership Failed Events due to server not responding to cluster heartbeat from the cluster controller

NET_ACClusterNameResolutionSvcErrorEvents

Description: Forwards Application Center Cluster Name Resolution Service Error Events

NET_ACClusterNetCfgUnsupportedErrorEvents

Description: Forwards Application Center Cluster Loadbalancing Network Configuration Unsupported Error Events

NET_ACClusterServiceErrorEvents

Description: Forwards Application Center Cluster Service Error Events

NET_ACClusterTopologyClusterEvents

Description: Forwards Application Center Cluster Topology Cluster Events

NET_ACClusterTopologyServerEvents

Description: Forwards Application Center Cluster Topology Warning Events

NET_ACReplicationCancelledEvent

Description: Forwards Application Center Replication Session Cancelled Event

NET_ACReplicationInvalidContentDescriptionEvent

Description: Forwards Application Center Replication Session Invalid Content Description Event

NET_ACReplicationServiceStartError

Description: Forwards all Application Center Replication Service Start Error

NET_ACReplicationSessionAcsRestartErrorEvent

Description: Forwards Application Center Replication Session AcsRestart Error Events

NET_ACReplicationSessionAuthFailedEvent

Description: Forwards Application Center Replication Session Authorization Failed Event

NET_ACReplicationSessionComplusErrorEvents

Description: Forwards Application Center Replication Session Complus Error Events

NET_ACReplicationSessionComplusWarningEvents

Description: Forwards Application Center Replication Session Complus Warning Events

NET_ACReplicationSessionConnectionErrorEvents

Description: Forwards Application Center Replication Session Connection Error Events

NET_ACReplicationSessionDriverActionListFailEvent

Description: Forwards Application Center Replication Session Driver Events Action List Failed Error Events

NET_ACReplicationSessionDriverGeneralErrorEvents

Description: Forwards Application Center Replication Session Driver General Error Events

NET_ACReplicationSessionDriverListFailedEvent

Description: Forwards Application Center Replication Session Driver List Failed Event

NET_ACReplicationSessionDriverUpdateListFailEvent

Description: Forwards Application Center Replication Session Driver Events Update Error Events

NET_ACReplicationSessionEnumObjectFailedEvent

Description: Forwards Application Center Replication Session Object Enumeration Failed Event

NET_ACReplicationSessionFailedEvent

Description: Forwards Application Center Replication Session Failed Event

NET_ACReplicationSessionObjectSecurityErrorEvents

Description: Forwards Application Center Replication Session Object Security Error Events

NET_ACReplicationSessionRegDelKeyFailedEvent

Description: Forwards Application Center Replication Session Replication Registry Delete key Failed Event

NET_ACReplicationSessionRegDelValueFailedEvent

Description: Forwards Application Center Replication Session Replication Registry Delete Value Failed Event

NET_ACReplicationSessionRegOpenFailedEvent

Description: Forwards Application Center Replication Session Replication Registry Open Failed Event

NET_ACReplicationSessionResourceAvailErrorEvents

Description: Forwards Application Center Replication Session Resource Availability Events Error Events

NET_ACReplicationSessionSendFileFailedEvents

Description: Forwards Application Center Replication Session Send File Failed Event

NET_ACReplicationSessionStartFailedEvent

Description: Forwards Application Center Replication Session Replication Start Failed Event

NET_ACReplicationSessionUdateListApplyErrorEvents

Description: Forwards Application Center Replication Session Update List Apply Error Events

NET_ACRequestForwardingInitErrorEvents

Description: Forwards Application Center Request Forwarding Initialize Error Events

NET_ACRequestForwardingInitMbChangeErrorEvents

Description: Forwards Application Center Request Forwarding Initialize Metabase Change Notify Error Events

NET_ACRequestForwardingInstExtErrorEvent

Description: Forwards Application Center Request Forwarding Install Extension Error Event.

NET_ACRequestForwardingMbUpdateErrorEvents

Description: Forwards Application Center Request Forwarding Metabase Update Error Events

NET_ACRequestForwardingMbUpdateWarningEvents

Description: Forwards Application Center Request Forwarding Metabase Update Warning Events

NET_ACRequestForwardingSecurityErrorEvent

Description: Forwards Application Center Request Forwarding Security Error Event.

NET_ACRequestFwdInstallPerfCountError

Description: Forwards Application Center Request Forwarding Install Performance Counter Failed Event

NET_ACTimeSyncFailedEvent

Description: Forwards Application Center Time Synchronization Failed Event

Server Logging

Policy Description

NET_ACServer2000_Logging

Description: This policy logs selected performance data for the Application Center Server using the following counters. Deployment of Windows OS SPI logging policy WINOSSPI-WINOS_Win2k_Logging is required to log process-related data for CPU and memory counters.

Counters:

- Application Center Request Forwarder
  - Total Requests/sec
  - Total Failed Requests/sec
  - Total Coherent Session Requests/sec

Discovery

Policy Descriptions

NET_ApplicationCenter2000_Discovery

Description: This policy discovers and adds the infrastructure information to the service map.

NET_ApplicationCenter2000_Apps_Discovery

Description: This policy discovers and adds the application information to the service map. It also adds the dependency information to the service map.

Related Topics:

- Deploying Policies for Microsoft Enterprise Servers
- Application Center Server Overview

Application Center Server reports

Predefined reports for the Application Center Server are available with the Microsoft Enterprise Servers SPI. Each of the following report descriptions includes a list of the performance counters used within the report.

- Application Center 2000 Processes CPU Statistics
- Application Center 2000 Processes Memory Statistics
- Application Center 2000 Web Server Cluster Request Forwarding Trends of Member Systems
- Application Center 2000 Web Server Cluster Request Forwarding Failure Trends of Member Systems
- Application Center 2000 Web Server Cluster Coherent Session Request Trends of Member Systems

Application Center 2000 Processes CPU Statistics (g_ACCPUSummary.rpt) This report shows summary CPU statistics of Application Center 2000 Server processes compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by the Cluster Service, Name Resolution Service, and Synchronization Service compared with the percentage of time the system's CPU was busy.

Counters:

- Process.% Processor Time (accluster.exe, acnameres.exe, acsrepl.exe)
- Process.Thread Count (accluster.exe, acnameres.exe, acsrepl.exe)
- Processor.% Processor Time

Application Center 2000 Processes Memory Statistics (g_ACMemorySummary.rpt) This report shows summary memory statistics of Application Center 2000 Server processes. The summarized process statistics include the page faults per second, private bytes, and working set used by the Cluster Service, Name Resolution Service and Synchronization Service processes.

Counters:

- Process.Private Bytes (accluster.exe, acnameres.exe, acsrepl.exe)
- Process.Working Set (accluster.exe, acnameres.exe, acsrepl.exe)
- Process.Page Faults/sec (accluster.exe, acnameres.exe, acsrepl.exe)

Application Center 2000 Web Server Cluster Request Forwarding Trends of Member Systems. (g_ACRequestForwarder.rpt)

Counters:

- Application Center Request Forwarder Total Requests/sec"

Application Center 2000 Web Server Cluster Request Forwarding Failure Trends of Member Systems (g_ACRequestForwarder.rpt)

Counters:

- Application Center Request Forwarder Total Failed Requests/sec"

Application Center 2000 Web Server Cluster Coherent Session Request Trends of Member Systems (g_ACRequestForwarder.rpt) The Coherent Sessions indicate the requests for pages requiring session coherency.

Counters:

- Application Center Request Forwarder Total Coherent Session Requests/sec

Related Topics:

- Application Center Server Graphs

Application Center Server graphs

Predefined graphs for the Application Center Server graphs are available with the Microsoft Enterprise Servers SPI.

- Application Center Cluster Service CPU
- Application Center Cluster Service Memory
- Application Center Name Resolution Service CPU
- Application Center Name Resolution Service Memory
- Application Center Synchronization Service CPU
- Application Center Synchronization Service Memory

Application Center Cluster Service CPU This graph shows summary CPU statistics of the Application Center Server Cluster Service process.

Application Center Cluster Service Memory This graph shows summary memory statistics of the Application Center Server Cluster Service process.

Application Center Name Resolution Service CPU This graph shows summary CPU statistics of the Application Center Server Name Resolution Service process.

Application Center Name Resolution Service Memory This graph shows summary memory statistics of the Application Center Server Name Resolution Service process.

Application Center Synchronization Service CPU This graph shows summary CPU statistics of the Application Center Server Synchronization Service process.

Application Center Synchronization Service Memory This graph shows summary memory statistics of the Application Center Server Synchronization Service process.

Related Topics:

- Application Center Server Reports

BizTalk Server

Microsoft's BizTalk Server provides distributed application integration services using XML as its primary messaging format. External formats are converted to the Biztalk standards through parsers and Biztalk mapping services, which are components of Biztalk Messaging Services. The Biztalk Orchestration Designer defines the process that a document undergoes.

In BizTalk messaging, channels handle the conversion of external formats, and ports are responsible for transmitting documents. The channels and ports in Biztalk Messaging can be configured to receive and transmit documents in a variety of formats and protocols, such as HTTP, HTTPS, SMTP, COM. In Orchestration services, the ports represent the input and output of a process. The action is defined in the XLANG schedule.

The Microsoft Enterprise Servers SPI monitors the performance of **BizTalk Server 2000** , **BizTalk Server 2002** , **BizTalk Server 2004** and **BizTalk Server 2006** , with policies, tools, graphs and reports.

Concerning versions: Where policies, reports, graphs or tools are only available for particular versions of BizTalk Server this is noted, in all other cases Microsoft Enterprise Servers SPI functionality monitors all versions of BizTalk Server.

> **NOTE:**
> There are special configuration steps required before monitoring BizTalk Server 2004 and BizTalk Server 2006, see Configuring the Microsoft Enterprise Servers SPI for BizTalk 2004 and 2006 for details.

The Microsoft Enterprise Servers SPI offers the following policies for process monitoring and service management, and for logging data used by BizTalk Server graphs and reports.

BizTalk Server Discovery and Service Map

The BizTalk Server discovery policy discovers and maps the service topology for all versions of BizTalk server.

Availability monitoring

BizTalk Server services are monitored to determine whether they are up or down. If the service is not running and the service startup is set to "Auto Start", then an attempt is made to restart the service. A console error message is sent to indicate that service is not running.

Monitored services for all versions of BizTalk Server include:

- BizTalk Messaging Service (MSCIS)
- BizTalk Orchestration Service (WFSVCMGR)

In addition, for **BizTalk 2002** there are policies for monitoring the following services:

- BizTalk COM+ applications (capable of hosting XLANG schedules)
- BizTalk related Databases

For **BizTalk 2004** and **BizTalk Server 2006** there are policies available for monitoring the following additional services:

- BizTalk Server Application Service
- BizTalk RuleEngineUpdate Service
- Enterprise Single Sign-On.

Event Log monitoring

Where errors, warnings, and information entries from BizTalk Server sources are logged to the Windows Event Log, messages are sent to the HPOM console.

Policies monitoring events are grouped in the following way:

- BizTalk Server
- XLANG Scheduler

For **BizTalk 2002** there are additional policies grouped in the following categories:

- **Server** : including General Event, Licensing, Security Failure/Violation, Service, and AICError(COM+,VBScript) policies.
- **Document** : policies monitoring general document handling events including document mapping and parsing.
- **Messaging:** including Channel, Organization, Messaging ports, Application, and ReceiveFunctions policies.
- **XLANG Scheduler**

Performance monitoring

Biztalk Server performance monitoring includes both specific BizTalk Server performance counters and CPU process-related counters. Each policy for performance monitoring has both error and warning thresholds.

For **BizTalk Server 2002** , policies monitoring the following areas of performance are available:

- Activated Schedule Instances
- Dehydrated Schedule Instance
- Failed Schedule Instances
- Running Schedule Instances
- Running Schedule Instances per sec.
- Transactions Aborted
- Transactions Aborted per sec.

In addition, policies monitoring the following areas of performance for **BizTalk Server 2004** and **BizTalk Server 2006** are available:

- CPU Usage
- Memory Usage

Server logging

The NET_BizTalkServer_Logging policy collects selected performance and process-related data for CPU and memory counters.

For **BizTalk Server 2002** , you must deploy the NET_BizTalkServer2002_Logging policy to monitor and collect data on the messaging and orchestration services of BizTalk Server 2002, and a NET_BizTalkServer2002_IntervalCount_Logging policy to log delta values on a number of document, interchange and XLANG counters. These policies require the NET_BizTalk_CreateCodaDataSources policy to create Interval Count datasources.

For **BizTalk Server 2004** and **BizTalk Server 2006** , the Microsoft Enterprise Servers SPI offers the MSES_BizTalkServer_TDDS_Logging, MSES_BizTalk_IntervalCount_Logging and MSES_BizTalkServer_SusDoc_Logging policies.

These policies require the deployment of the MSES_BizTalk_CreateCodaDataSources policy to first create the CODA interval count datasource.

NOTE:

For all versions of BizTalk Server, deployment of the Windows OS SPI logging policy, WINOSSPI-WINOS_Win2k_Logging, is required to log process-related data for CPU and memory counters. The counters specific to the BizTalk Server are documented in the policy section. Refer to the Windows OS SPI Policies for information about the process-related data for CPU and memory counters.

Related Topics:

- BizTalk Server Tools
- BizTalk Server Policies
- BizTalk Server Reports
- BizTalk Server Graphs
- BizTalk Server Service Map
- Configuring the Microsoft Enterprise Servers SPI for BizTalk 2004 and 2006

Configuring the Microsoft Enterprise Servers SPI for BizTalk Server 2004 and 2006

The following steps need to be completed to enable the Microsoft Enterprise Servers SPI to monitor nodes running BizTalk Server 2004 or BizTalk Server 2006:

Open the HPOM console from the management server.

1. Execute the tool **MSES_BTS_DB_Configuration,** in **Tools** → **SPI for Microsoft Enterprise Servers** → **BizTalk Servers** .
2. Database configuration has to be performed for all nodes with BizTalk Server 2004 or 2006 installed, see the procedure for using the BizTalk Server Database Configuration tool. The Database configuration tool should be launched from the management server only, not from a remote console.
3. Right-click the selected node in the HPOM console **Nodes** folder, select **All tasks** → **Deploy Instrumentation** → **BizTalk Server** and **SPI data collector** , and deploy BizTalk and SPI data collector instrumentation.
4. Deploy the Microsoft Enterprise Servers SPI discovery policy on the selected node by right-clicking **Policy Management** → **Policy Groups** → **SPI for Microsoft Enterprise Servers** → **BizTalk Servers** → **BizTalk_Discovery** , and select **Deploy** .

Related Topics:

- BizTalk Server Tools
- BizTalk Server Policies
- BizTalk Server Reports
- BizTalk Server Graphs
- BizTalk Server Service Map

BizTalk Server service map

On discovery of a BizTalk Server the components of the BizTalk system are identified, including the Messaging Management databases, the BizTalk Group to which the managed server belongs, and all components of that group such as other BizTalk servers, Shared Queues, Receive Functions, and the Document Tracking database. A service map is created from this information, located on the console tree under **Services → Systems Infrastructure → BizTalk Server.**

Systems infrastructure

BizTalk Server is the primary node for BizTalk Server systems. The two main groups are the BizTalk Group and the BizTalk Management Databases. The BizTalk Group contains several subgroups as shown below:

BizTalk 2004 Server Group On Server <SERVERNAME>

1. Tracking DB: Dependency on MS SQL SPI On Server <SERVERNAME>
2. SSODb: Dependency on MS SQL SPI On Server <SERVERNAME>
3. Message Box: Dependency on MS SQL SPI On Server <SERVERNAME>
4. Management DB: Dependency on MS SQL SPI On Server <SERVERNAME>
5. DTA DB: Dependency on MS SQL Server On Server <SERVERNAME>
6. Send Port Groups

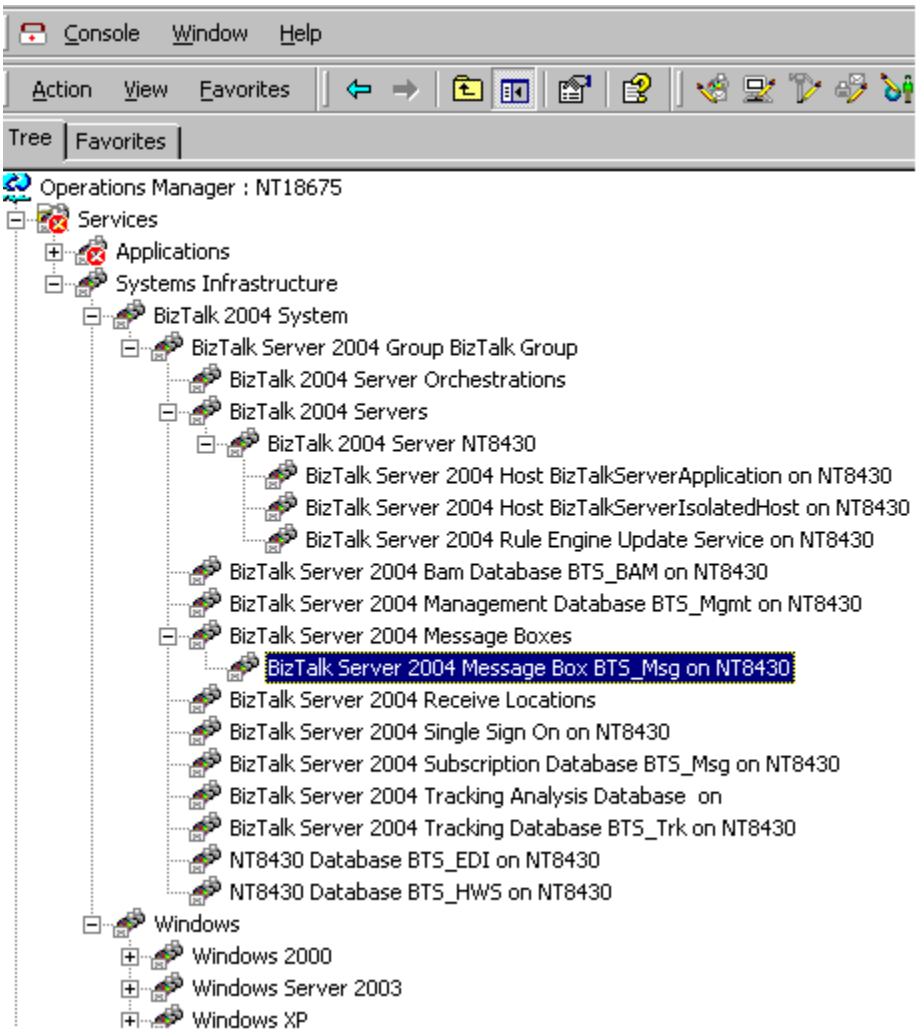
   Send Ports
7. Orchestrations
8. Hosts

   Host: Instance_Hosted_On_Server_<SERVERNAME>

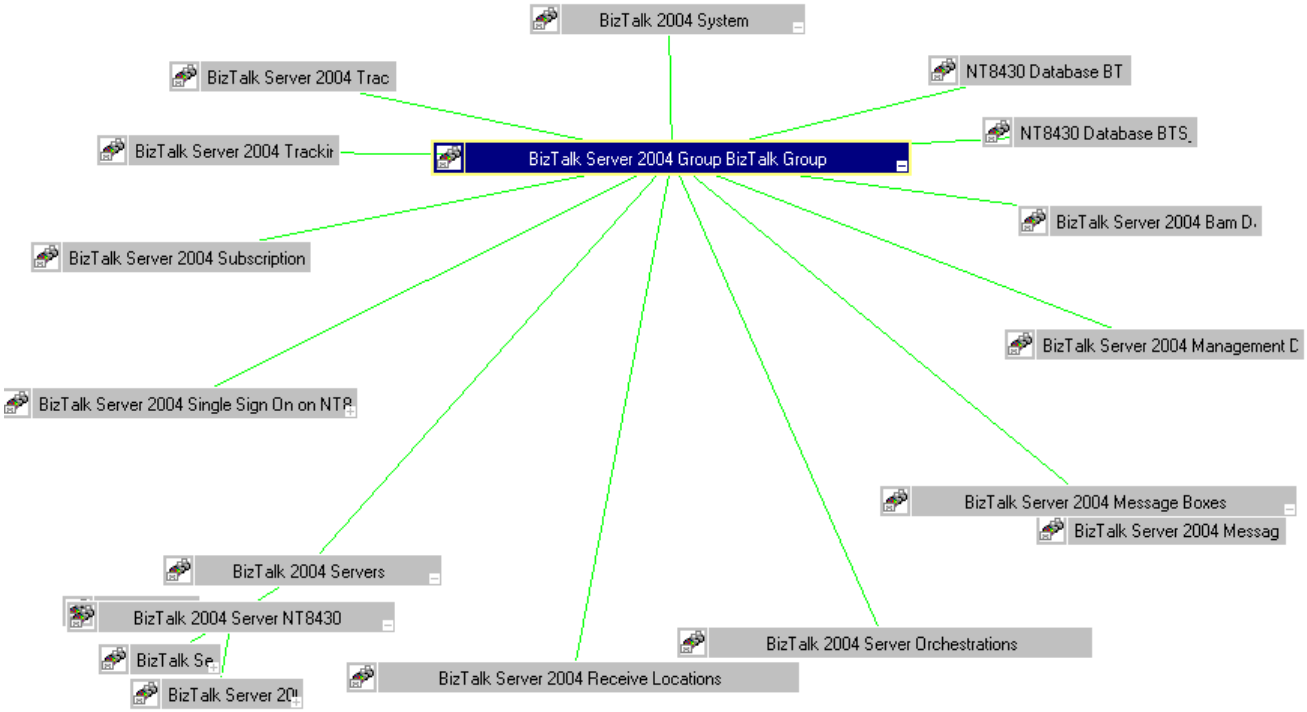
   Isolated Host: Instance_Hosted_On_Server_ <SERVERNAME>

   Rules: Engine_Hosted_On_Server_ <SERVERNAME>

Example BizTalk Server 2004 service tree view:



Example BizTalk Server 2004 service map view:



Related Topics:

- Creating Service Maps for Microsoft Enterprise Servers
- Configuring the Microsoft Enterprise Servers SPI for BizTalk 2004 and 2006

BizTalk Server policies

Many predefined policies for monitoring BizTalk Server are available with the Microsoft Enterprise Servers SPI.

- Policies for monitoring BizTalk Server 2000
- Policies for monitoring BizTalk Server 2002
- Policies for monitoring BizTalk Server 2004
- Policies for monitoring BizTalk Server 2006

Related Topics:

- Deploying policies for Microsoft Enterprise Servers
- BizTalk Server Overview

BizTalk Server 2000 policies

- Availability monitoring policies
- Performance monitoring policies
- Windows event monitoring policies
- WMI event monitoring policies
- Server logging policies
- Discovery policy

Availability monitoring policies

Messaging Service Monitoring

NET_BizTalkCheckMessagingService and NET_BizTalkCheckBizTalkComponents

Description: The policies NET_BizTalkCheckMessagingService and NET_BizTalkCheckBizTalkComponents monitor the BizTalk 2002 Messaging Service. To ensure that this critical service is functioning correctly, this policy verifies that Messaging Service responds to basic API calls. This check provides a deeper check than the basic service check done by NET_BizTalkServerServices policy. Provide the BizTalk Server Admin credentials or the credentials which the BizTalk messaging service is running under to the NET_BizTalkCheckMessagingService policy. NET_BizTalkCheckBizTalkComponents is an auxiliary policy, which forwards messages generated during this check to the console.

Orchestration Service Monitoring

NET_BizTalkCheckOrchestrationComponents and **NET_BizTalkCheckBizTalkComponents**

Description: To ensure that this critical service is functioning correctly, this policy verifies that BizTalk Orchestration components (COM+ applications hosting XLANG schedules) respond to basic API calls. This check provides a deeper check than the basic service check done by the NET_BizTalkServerServices policy. Provide the BizTalk Server Admin credentials or the credentials which the BizTalk messaging service is running under to the NET_BizTalkCheckOrchestrationComponents policy. NET_BizTalkCheckBizTalkComponents is an auxiliary policy, which forwards messages generated during this check to the console.

Performance monitoring policies

NET_BS-Activated ScheduleInstances

Description: Monitors the Activated Schedule Instances perfmon counter and generates the Critical, Major, Minor, and Warning level messages when the number of activated schedule instances reaches above 50,40,30 and 20 mark. The BizTalk administrator can modify these threshold values to suit their needs. This counter indicates the number of schedules started since the last time the XLANG XOM+ process was started. Crossing a level doesn't necessarily indicate that something is wrong with the BizTalk Server, but shows increase in CPU and memory network consumption. The BizTalk server load needs to be assessed and values set appropriately.

NET_BS-DehydratedScheduleInstances

Description: This policy monitors the Dehydrated Schedule Instance perfmon counter, and generates Critical, Major, Minor and Warning level messages when the number of dehydrated schedule instances goes above the 50,40,30 or 20 mark. A BizTalk administrator can modify these threshold values to suit their needs. This counter indicates the number (integer) of schedules dehydrated per server. This number is cumulative across all XLANG COM+ processes running on a particular server. The accumulation for each process begins each time the process is started. This counter can be used to monitor the on-going number of schedules dehydrated on a server, compared to the number of schedules started or failed.

NET_BS-FailedScheduleInstances

Description: This policy monitors the Failed Schedule Instances perfmon counter, and generates Critical, Major, Minor and Warning level messages when the number of failed schedule instances goes above the 50,40,30 or 20 mark. A BizTalk administrator can modify these threshold values to suit their needs. This counter indicates the number (integer) of schedules that have failed for a specified server. This number is cumulative across all XLANG COM+ processes running on a particular server. The accumulation for each process begins each time the process is started. This counter can be used to monitor the on-going number of schedules failing on a server, compared to the number of schedules started. i

NET_BS-RunningScheduleInstances

Description: This policy monitors the Running Schedule Instances perfmon counter, and generates Critical, Major, Minor and Warning level messages when the number of running schedule instances goes above the 50 mark. A BizTalk administrator can modify these threshold values to suit their needs. Crossing the level may not indicate a problem with the server, but indicates the load on the server.

NET_BS-RunningScheduleInstances/sec

Description: This policy monitors the Running Schedule Instances/sec perfmon counter, and generates Critical, Major, Minor and Warning level messages when the number of running schedule instances/sec goes above the 50 mark. This counter indicates the average number of schedules running per second. Set the threshold value to the optimal value which a BizTalk server can handle, if the counter goes above this value a warning message will be generated for future action.

NET_BS-TransactionsAborted

Description: This policy monitors the number of schedule transactions aborted on a given server. This number is cumulative across all XLANG COM+ processes running on a particular server. Accumulation for each process begins each time the process is started. This policy generates Critical and Major level messages when the number of transactions aborted goes above the 50,10 mark. A BizTalk administrator can modify these threshold values to suit their needs.

NET_BS-TransactionsAborted/sec

Description: This policy monitors the number of schedule transactions aborted on a given server per second. This policy generates Critical and Major level messages when the number of transactions aborted per second goes above the 5,1 mark. A BizTalk administrator can modify these threshold values to suit their needs.

Windows event monitoring policies

NET_BizTalkServerFwdApplicationError

Description: Forwards all BizTalk Server application log entries with severity 'Error'.

NET_BizTalkServerFwdApplicationInformation

Description: Forwards all BizTalk Server application log entries with severity 'Information'.

NET_BizTalkServerFwdApplicationWarning

Description: Forwards all BizTalk Server application log entries with severity 'Warning'.

WMI event monitoring policies

NET_BS_DocSuspendedEvent

Description: WMI policy forwards all Document Suspended Events to the console, and logs them into the database.

NET_BS_ReceiveFunctionEvent

Description: WMI policy forwards all Receive Function Disabled Events.

Server logging policies

NET_BizTalkServer_Logging

Description: **This policy logs selected performance data for BizTalk Server 2000. Deployment of Windows OS SPI logging policy WINOSSPI-WINOS_Win2k_Logging is required to log process-related data for CPU and memory counters.**

Counters:

- **Asynchronous Submissions**
- **Asynchronous Submissions/sec**
- **Documents Mapped/sec**
- **Documents Parsed/sec**
- **Documents Processed**
- **Documents Processed/sec**
- **Documents Received**
- **Documents Received/sec**
- **Documents Serialized/sec**
- **Interchanges Decoded/sec**
- **Interchanges Decrypted/sec**
- **Interchanges Encrypted/sec**
- **Interchanges Received**
- **Interchanges Received/sec**
- **Interchanges Transmitted/sec**
- **Items Suspended**
- **Items Suspended/sec**
- **Synchronous Submissions**
- **Synchronous Submissions/sec**

NET_BS_DocSuspendedEvent

Description: **BizTalk triggers the DocSuspendedEvent for each document in a suspended queue. The DocSuspendeEvent contains Destination, Source, DocName/Type and State information. NET_BS_DocSuspendedEvent policy logs this data into the service reporter database for use by some reports.**

BizTalk Server Discovery policy

NET_BizTalkServer_Discovery

Description: **This policy discovers the BizTalk infrastructure information and adds it to the service map.**

Related Topics:

- **BizTalk Server policies**
- **Deploying Policies for Microsoft Enterprise Servers**
- **BizTalk Server Overview**

BizTalk Server 2002 policies

- Availability monitoring policies
- Performance monitoring policies
- Windows event monitoring policies
- WMI event monitoring policies
- Database connectivity monitoring
- Server logging policies
- Discovery policy

Availability monitoring policies

Messaging Service Monitoring

NET_BizTalkCheckMessagingService and NET_BizTalkCheckBizTalkComponents

Description: The policies NET_BizTalkCheckMessagingService and NET_BizTalkCheckBizTalkComponents monitor the BizTalk 2002 Messaging Service. To ensure that this critical service is functioning correctly, this policy verifies that Messaging Service responds to basic API calls. This check provides a deeper check than the basic service check done by NET_BizTalkServerServices policy. Provide the BizTalk Server Admin credentials or the credentials which the BizTalk messaging service is running under to the NET_BizTalkCheckMessagingService policy. NET_BizTalkCheckBizTalkComponents is an auxiliary policy, which forwards messages generated during this check to the console.

Orchestration Service Monitoring

NET_BizTalkCheckOrchestrationComponents and **NET_BizTalkCheckBizTalkComponents**

Description: To ensure that this critical service is functioning correctly, this policy verifies that BizTalk Orchestration components (COM+ applications hosting XLANG schedules) respond to basic API calls. This check provides a deeper check than the basic service check done by the NET_BizTalkServerServices policy. Provide the BizTalk Server Admin credentials or the credentials which the BizTalk messaging service is running under to the NET_BizTalkCheckOrchestrationComponents policy. NET_BizTalkCheckBizTalkComponents is an auxiliary policy, which forwards messages generated during this check to the console.

Performance monitoring policies

NET_BS-Activated ScheduleInstances

Description: Monitors the Activated Schedule Instances perfmon counter and generates the Critical, Major, Minor, and Warning level messages when the number of activated schedule instances reaches above 50,40,30 and 20 mark. The BizTalk administrator can modify these threshold values to suit their needs. This counter indicates the number of schedules activated since the last time the XLANG XOM+ process was started. Crossing a level doesn't necessarily indicate that something is wrong with the BizTalk Server, but shows increase in CPU and memory network consumption. The BizTalk server load needs to be assessed and values set appropriately.

NET_BS-DehydratedScheduleInstances

Description: This policy monitors the Dehydrated Schedule Instance perfmon counter, and generates Critical, Major, Minor and Warning level messages when the number of dehydrated schedule instances goes above the 50,40,30 or 20 mark. A BizTalk administrator can modify these threshold values to suit their needs. This counter indicates the number (integer) of schedules dehydrated per server. This number is cumulative across all XLANG COM+ processes running on a particular server. The accumulation for each process begins each time the process is started. This counter can be used to monitor the on-going number of schedules dehydrated on a server, compared to the number of schedules started or failed.

NET_BS-FailedScheduleInstances

Description: This policy monitors the Failed Schedule Instances perfmon counter, and generates Critical, Major, Minor and Warning level messages when the number of failed schedule instances goes above the 50,40,30 or 20 mark. A BizTalk administrator can modify these threshold values to suit their needs. This counter indicates the number (integer) of schedules that have failed for a specified server. This number is cumulative across all XLANG COM+ processes running on a particular server. The accumulation for each process begins each time the process is started. This counter can be used to monitor the on-going number of schedules failing on a server, compared to the number of schedules started.

NET_BS-RunningScheduleInstances

Description: This policy monitors the Running Schedule Instances perfmon counter, and generates Critical, Major, Minor and Warning level messages when the number of running schedule instances goes above the 50 mark. A BizTalk administrator can modify these threshold values to suit their needs. Crossing the level may not indicate a problem with the server, but indicates the load on the server.

NET_BS-RunningScheduleInstances/sec

Description: This policy monitors the Running Schedule Instances/sec perfmon counter, and generates Critical, Major, Minor and Warning level messages when the number of running schedule instances/sec goes above the 50 mark. This counter indicates the average number of schedules running per second. Set the threshold value to the optimal value which a BizTalk server can handle, if the counter goes above this value a warning message will be generated for future action.

NET_BS-TransactionsAborted

Description: This policy monitors the number of schedule transactions aborted on a given server. This number is cumulative across all XLANG COM+ processes running on a particular server. Accumulation for each process begins each time the process is started. This policy generates Critical and Major level messages when the number of transactions aborted goes above the 50,10 mark. A BizTalk administrator can modify these threshold values to suit their needs.

NET_BS-TransactionsAborted/sec

Description: This policy monitors the number of schedule transactions aborted on a given server per second. This policy generates Critical and Major level messages when the number of transactions aborted per second goes above the 5,1 mark. A BizTalk administrator can modify these threshold values to suit their needs.

Windows event monitoring policies

Server policy group

Description: Handles the BizTalk Server related events. Has the following policy sub groups:

- **General Events (NET_BizTalkGeneral)** : Policies handle any event which cannot be placed in any other group.
- **Licensing (NET_BizTalkLicensing)** : Policies handle events related to Licensing issues.
- **Security Failure/Violation (NET_BizTalkSecurityLogon)** : Policies handle events related to security/logon failure violation events.
- **Service (NET_BizTalkServices)** : Policies handle events for all BizTalk services such as startup failures.
- **AICError(COM+,VBScript) (NET_BizTalkAIC)** : Policies handle events caused by Application integration components such as COM components and scripting components.

Document policy group

Description: Policies under this group handle events related to document mapping, parsing, and general document events:

Forward and Log Document Suspended Event (NET_BS_DocSuspendEvent) : WMI policy forwards Document Suspended Event to console and Logs it into the database.

Forward Document related Event log event (NET_BizTalkDocument) : Forwards all BizTalk Document/Interchange application log entries.

Messaging policy group

Description: Contains the following policy sub groups:

- **Channel (NET_BizTalkMessagingChannel)** : Policies handle any event related to channels.
- **Organization (NET_BizTalkOrganization)** : Policies handle events related to BizTalk Organization.
- **Messaging ports (NET_BizTalkMessagingPorts)** : Policies handle events related to BizTalk Messaging ports.
- **Application (NET_BizTalkApplication)** : Policies handle events related to BizTalk Applications.
- **Receive Functions (NET_BizTalkReceiveFunctionEvent** and **NET_BizTalkReceiveFunctions)** : Policies handle events related to BizTalk receive functions and related application log entries.

XLANG Scheduler policy group (NET_BizTalkXLANGScheduler)

Description: Policies under this group handle events related to XLANG scheduler and orchestration.

WMI event monitoring policies

NET_BS_DocSuspendedEvent

Description: WMI policy forwards all Document Suspended Events to the console, and logs them into the database.

NET_BS_ReceiveFunctionEvent

Description: WMI policy forwards all Receive Function Disabled Events.

Database connectivity monitoring

NET_BizTalkCheckDatabasesConnections and NET_BizTalkCheckBizTalkComponents

Description: **BizTalk Server environment includes Messaging Management (Administration) database, Shared Queue databases, and the Document Tracking database running on Microsoft SQL server. Availability of these databases is essential for the functioning of the BizTalk environment. These database can be installed on separate machines running SQL Servers, so that connectivity between the BizTalk Server machine and the SQL server should be up all the time. To monitor this connection deploy these policies. The policies check connectivity with BizTalk databases from Biztalk server, the default schedule is every hour. Provide the BizTalk Server Admin credentials or the credentials which the BizTalk messaging service is running under to the NET_BizTalkCheckDatabasesConnections policy, checking access to the databases. NET_BizTalkCheckBizTalkComponents is an auxiliary policy, which forwards messages generated during this check to the console.**

Server logging policies

NET_BizTalkServer2002_Logging

Description: **The NET_BizTalkServer2002_Logging policy logs the following rate counters:**

Messaging Service Counters

- **Asynchronous Submissions/sec**
- **Documents Mapped/sec**
- **Documents Parsed/sec**
- **Documents Processed/sec<**
- **Documents Received/sec**
- **Documents Serialized/sec**
- **Interchanges Decrypted/sec**
- **Interchanges Encoded/sec**
- **Interchanges Encrypted/sec**
- **Interchanges Decoded/sec**
- **Interchanges Received/sec**
- **Interchanges Transmitted/sec**

- **Items suspended/sec**
- **Synchronous Submissions/sec**

Xlang Counters

- **Completed Schedule Instances/sec**
- **Failed Schedule Instances/sec**
- **Running Schedule Instances/sec**
- **Schedules Activated/sec**
- **Transactions Aborted/sec**

NET_BizTalkServer2002_IntervalCount_Logging

Description: **This policy logs the delta value between two consecutive accumulative loggings:**

Messaging Service Counters

- **Asynchronous Submissions**
- **Documents Processed**
- **Documents Received**
- **Interchanges Received**
- **Items suspended**
- **Synchronous Submissions**

Xlang Counters

- **Activated Schedule Instances**
- **Completed Schedule Instances**
- **Dehydrated Schedule Instances**
- **Failed Schedule Instances**
- **Running Schedule Instances**
- **Transactions Aborted**

NET_BizTalk_CreateCodaDataSources

Description: **This policy creates the data source and class in coda for the NET_BizTalkServer2002_IntervalCount_Logging policy to insert data into.**

BizTalk Server Discovery policy

NET_BizTalkServer_Discovery

Description: **This policy discovers the BizTalk infrastructure information and adds it to the service map.**

Related Topics:

- **BizTalk Server policies**
- **Deploying Policies for Microsoft Enterprise Servers**
- **BizTalk Server Overview**

BizTalk Server 2004 policies

- Availability monitoring policy
- Performance monitoring policies
- Windows event monitoring policy
- Database connectivity monitoring
- Server logging policies
- Discovery policy

Availability monitoring policy

EBIZ_BizTalkServer2004Services	
Description	This policy monitors the following BizTalk Server 2004 services: BizTalk Server Application Service, BizTalk RuleEngineUpdate Service and Enterprise Single Sign-On. If a service is stopped it is restarted automatically.
Message Text	The Service is not running, but its start mode is 'Auto'. Trying to restart the service.
Instruction Text	Message Severity: Critical Situation: Process not running. Probable Cause: The application has shut down. Potential Impact: System down. Suggested Action: Start up the process. Policy Type: Scheduled Task Polling Interval: 5 min

Performance monitoring policies

EBIZ_BS2004-MEMUsage-BTSSvc

Description: Measures Memory usage of BizTalk Server Application services

EBIZ_BS2004-CPUUsage-BTSSvc

Description: Measures CPU usage of BizTalk Server Application services

EBIZ_BS2004-MEMUsage-ENTSSO

Description: Measures Memory usage of Enterprise Single Sign-On service

EBIZ_BS2004-CPUUsage-ENTSSO

Description: Measures CPU usage of Enterprise Single Sign-On service

MSES_SendPort_Status_Monitoring

Description: Monitors the status of the SendPorts in the BizTalk Server.

MSES_ReceiveLocation_Status_Monitoring

Description: Monitors the status of the ReceiveLocations of BizTalk Server.

MSES_BS2004_ DocumentsProcessed

Description: Average number of documents processed (pulled from the Work queue and sent to a port destination address) per second, since the last time the BizTalk Messaging Service was started.

MSES_BS2004_ DocumentsReceived

Description: Average number of documents received per second by BizTalk Server. This includes all documents that make it into the Work queue, and any that have failed.

MSES_BS2004_DocumentsSuspended

Description: Average number of items suspended per second in the suspended queue.

MSES_BS2004_DatabaseTransactions

Description: Average number of database transactions performed since the host instance started.

MSES_BS2004_ActiveApplicationDomains

Description: The number of application domains currently existing for hosting orchestrations.

MSES_BS2004_DehydrationThreshold

Description: Number in milliseconds that determines how aggressively orchestrations are being dehydrated. If the orchestration engine predicts that an instance will be dehydratable (storing all the instance-specific data in the database and removing the instance from the memory), for an amount of time longer than the threshold value, it will dehydrate the instance.

MSES_BS2004_IdleOrchestrations

Description: Number of idle orchestration instances currently hosted by the host instance. This refers to orchestrations that are not making progress but are not dehydratable, as when the orchestration is blocked waiting for a receive, listen, or delay in an atomic transaction.

MSES_BS2004_MsgBox DBConnFailures

Description: Number of attempted database connections that failed since the host instance started.

MSES_BS2004_OrchestrationsCompleted

Description: Average number of orchestration instances completed per second since the host instance started.

MSES_BS2004_OrchestrationsCreated

Description: Average number of orchestration instances per second created since the host instance started. Measures CPU usage of Enterprise Single Sign-On service.

MSES_BS2004_OrchestrationsDehydrated

Description: Average number of orchestration instances dehydrated per second since the host instance started.

MSES_BS2004_OrchestrationsDiscarded

Description: Average number of orchestration instances discarded from memory since the host instance started. An orchestration can be discarded if the engine fails to persist its state.

MSES_BS2004_OrchestrationsRehydrated

Description: Average number of orchestration instances rehydrated per second (restoring the instance from the database to memory) since the host instance started.

MSES_BS2004_OrchestrationsResidentMemory

Description: Number of orchestration instances currently hosted by the host instance.

MSES_BS2004_OrchestrationsScheduledForDehydration

Description: Number of dehydratable orchestrations for which there is a dehydration request pending.

MSES_BS2004_OrchestrationsSuspended

Description: Average number of orchestration instances suspended per second since the host instance started.

MSES_BS2004_RunningOrchestrations

Description: Number of orchestration instances currently executing.

MSES_BTS2004_Orchestration_Status_Monitoring

Description: Monitors the status of the Orchestrations.

MSES_BS2004_PendingMessages

Description: Number of received messages for which receipt has not yet been acknowledged to the message box.

MSES_BS2004_PendingWorkItems

Description: Number of code execution blocks that are scheduled for execution.

MSES_BS2004_TransactionalScopes aborted

Description: Number of long-running or atomic scopes that have been aborted since the host instance started.

Windows event monitoring policy

EBIZ_BizTalkServer2004FwdApplicationLogEntries

Description: Forwards all BizTalk Server 2004 application log entries with severity 'Critical','Error', 'Warning' and 'Information'.

Database connectivity monitoring

MSES_BS2004_DBMonitor

Description: If an attempt to connect to any of the following databases fails, a message is sent to the HPOM message browser and an OPC message is sent to refresh the service map with this information. Connections to the following BizTalk 2004 databases are monitored:

- BAMPrimaryImport - Business Activity Monitoring DB.
- BAMStarSchema - Business Activity Monitoring DB.
- BAM Analysis - Business Activity Monitoring OLAP Cubes DB.
- BAMArchive - Archives Business Activity Monitoring DB.
- BizTalkHWSDb - Human Workflow Services DB.
- BizTalkDTADb - Tracking DB.
- BizTalkMgmtDB BTS - Configuration Information DB.

- BizTalkMsgBoxDb - DB for storing Messages and subscriptions.
- BizTalkRuleEngineDb - DB for storing Policies and Vocabularies.
- SSODB - Single Sign-On DB.
- TPM - Trading Partner DB for Business Activity Services.
- BizTalkAnalysisdb - DB for storing business and health monitoring OLAP Cubes.
- BizTalkEDIdb - Electronic data interchange DB.

MSES_BizTalk_MessageBox_DatabaseSize

Description: Monitors the percentage of the usage of the BizTalk MessageBox database.

MSES_BizTalk_DTA_DatabaseSize

Description: Monitors the percentage of the usage of the BizTalk DTA database.

Server logging policies

MSES_BizTalk_CreateCodaDataSources

Description: This policy creates the CODA interval count data source for BizTalk 2004 server.

NOTE: Deploy the Microsoft Enterprise Servers SPI Data collector instrumentation for this policy to work.

MSES_BizTalkServer2004_SusDoc_Logging

Description: Collects suspended documents data from the BizTalk Server database and logs it into CODA data source. First, this data source must be created by **MSES_BizTalk_CreateCodaDataSources** .

MSES_BizTalkServer2004_Logging

Description: This policy collects the performance data for the following three BizTalk 2004 objects:

- BizTalk:Messaging
- Enterprise Single Sign On
- XLANG/s Orchestrations

The data is logged as CODA data source. First, this data source must be created by **MSES_BizTalk_CreateCodaDataSources.**

MSES_BizTalkServer_TDDS_Logging

Description: This policy collects the performance data for BizTalk TDDS (Tracking Data Decode Service), and saves it as CODA data source. First, this data source must be created by **MSES_BizTalk_CreateCodaDataSources.**

Discovery policy

EBIZ_BS2004Disc

Description: This policy discovers the BizTalk infrastructure information and adds it to the service map.

Related Topics:

- BizTalk Server policies
- Deploying Policies for Microsoft Enterprise Servers
- BizTalk Server Overview

BizTalk Server 2006 policies

- Availability monitoring policy
- Performance monitoring policies
- Windows event monitoring policy
- Database connectivity monitoring
- Server logging policies
- Discovery policy

Availability monitoring policy

EBIZ_BizTalkServerServices	
Description	This policy monitors the following BizTalk Server 2006 services: BizTalk Server Application Service, BizTalk RuleEngineUpdate Service and Enterprise Single Sign-On. If a service is stopped it is restarted automatically.
Message Text	The Service is not running, but its start mode is 'Auto'. Trying to restart the service.
Instruction Text	Message Severity: Critical Situation: Process not running. Probable Cause: The application has shut down. Potential Impact: System down. Suggested Action: Start up the process. Policy Type: Scheduled Task Polling Interval: 5 min

Performance monitoring policies

EBIZ_BS-MEMUsage-BTSSvc

Description: Measures Memory usage of BizTalk Server Application services

EBIZ_BS-CPUUsage-BTSSvc

Description: Measures CPU usage of BizTalk Server Application services

EBIZ_BS-MEMUsage-ENTSSO

Description: Measures Memory usage of Enterprise Single Sign-On service

EBIZ_BS-CPUUsage-ENTSSO

Description: Measures CPU usage of Enterprise Single Sign-On service

MSES_SendPort_Status_Monitoring

Description: Monitors the status of the SendPorts in the BizTalk Server.

MSES_ReceiveLocation_Status_Monitoring

Description: Monitors the status of the ReceiveLocations of BizTalk Server.

MSES_BS_ DocumentsProcessed

Description: Average number of documents processed (pulled from the Work queue and sent to a port destination address) per second, since the last time the BizTalk Messaging Service was started.

MSES_BS_ DocumentsReceived

Description: Average number of documents received per second by BizTalk Server. This includes all documents that make it into the Work queue, and any that have failed.

MSES_BS_DocumentsSuspended

Description: Average number of items suspended per second in the suspended queue.

MSES_BS_DatabaseTransactions

Description: Average number of database transactions performed since the host instance started.

MSES_BS_ActiveApplicationDomains

Description: The number of application domains currently existing for hosting orchestrations.

MSES_BS_DehydrationThreshold

Description: Number in milliseconds that determines how aggressively orchestrations are being dehydrated. If the orchestration engine predicts that an instance will be dehydratable (storing all the instance-specific data in the database and removing the instance from the memory), for an amount of time longer than the threshold value, it will dehydrate the instance.

MSES_BS_IdleOrchestrations

Description: Number of idle orchestration instances currently hosted by the host instance. This refers to orchestrations that are not making progress but are not dehydratable, as when the orchestration is blocked waiting for a receive, listen, or delay in an atomic transaction.

MSES_BS_MsgBox DBConnFailures

Description: Number of attempted database connections that failed since the host instance started.

MSES_BS_OrchestrationsCompleted

Description: Average number of orchestration instances completed per second since the host instance started.

MSES_BS_OrchestrationsCreated

Description: Average number of orchestration instances per second created since the host instance started. Measures CPU usage of Enterprise Single Sign-On service.

MSES_BS_OrchestrationsDehydrated

Description: Average number of orchestration instances dehydrated per second since the host instance started.

MSES_BS_OrchestrationsDiscarded

Description: Average number of orchestration instances discarded from memory since the host instance started. An orchestration can be discarded if the engine fails to persist its state.

MSES_BS_OrchestrationsRehydrated

Description: Average number of orchestration instances rehydrated per second (restoring the instance from the database to memory) since the host instance started.

MSES_BS_OrchestrationsResidentMemory

Description: Number of orchestration instances currently hosted by the host instance.

MSES_BS_OrchestrationsScheduledForDehydration

Description: Number of dehydratable orchestrations for which there is a dehydration request pending.

MSES_BS_OrchestrationsSuspended

Description: Average number of orchestration instances suspended per second since the host instance started.

MSES_BS_RunningOrchestrations

Description: Number of orchestration instances currently executing.

MSES_Orchestration_Status_Monitoring

Description: Monitors the status of the Orchestrations.

MSES_BS_PendingMessages

Description: Number of received messages for which receipt has not yet been acknowledged to the message box.

MSES_BS_PendingWorkItems

Description: Number of code execution blocks that are scheduled for execution.

MSES_BS_TransactionalScopes aborted

Description: Number of long-running or atomic scopes that have been aborted since the host instance started.

Windows event monitoring policy

EBIZ_BizTalkServerFwdApplicationLogEntries

Description: Forwards all BizTalk Server 2006 application log entries with severity 'Critical','Error', 'Warning' and 'Information'.

Database connectivity monitoring

MSES_BS_DBMonitor

Description: If an attempt to connect to any of the following databases fails, a message is sent to the HPOM message browser and an OPC message is sent to refresh the service map with this information. Connections to the following BizTalk 2006 databases are monitored:

- BAMPrimaryImport - Business Activity Monitoring DB.
- BAMStarSchema - Business Activity Monitoring DB.
- BAM Analysis - Business Activity Monitoring OLAP Cubes DB.
- BAMArchive - Archives Business Activity Monitoring DB.
- BizTalkHWSDb - Human Workflow Services DB.
- BizTalkDTADb - Tracking DB.
- BizTalkMgmtDB BTS - Configuration Information DB.

- BizTalkMsgBoxDb - DB for storing Messages and subscriptions.
- BizTalkRuleEngineDb - DB for storing Policies and Vocabularies.
- SSODB - Single Sign-On DB.
- TPM - Trading Partner DB for Business Activity Services.
- BizTalkAnalysisdb - DB for storing business and health monitoring OLAP Cubes.
- BizTalkEDIdb - Electronic data interchange DB.

MSES_BizTalk_MessageBox_DatabaseSize

Description: Monitors the percentage of the usage of the BizTalk MessageBox database.

MSES_BizTalk_DTA_DatabaseSize

Description: Monitors the percentage of the usage of the BizTalk DTA database.

Server logging policies

MSES_BizTalk_Create_Coda_DataSources

Description: This policy creates the CODA interval count data source for BizTalk 2006 server.

NOTE: Deploy the Microsoft Enterprise Servers SPI Data collector instrumentation for this policy to work.

MSES_BizTalkServer_SusDoc_Logging

Description: Collects suspended documents data from the BizTalk Server database and logs it into CODA data source. First, this data source must be created by **MSES_BizTalk_CreateCodaDataSources** .

MSES_BizTalk_IntervalCount_Logging

Description: This policy collects the performance data for the following three BizTalk 2006 objects:

- BizTalk:Messaging
- Enterprise Single Sign On
- XLANG/s Orchestrations

The data is logged as CODA data source. First, this data source must be created by **MSES_BizTalk_CreateCodaDataSources.**

MSES_BizTalkServer_TDDS_Logging

Description: This policy collects the performance data for BizTalk TDDS (Tracking Data Decode Service), and saves it as CODA data source. First, this data source must be created by **MSES_BizTalk_CreateCodaDataSources.**

Discovery policy

BizTalk_Discovery

Description: This policy discovers the BizTalk infrastructure information and adds it to the service map.

Related Topics:

- BizTalk Server policies
- Deploying Policies for Microsoft Enterprise Servers
- BizTalk Server Overview

BizTalk Server reports

Predefined reports for BizTalk Server are available with the Microsoft Enterprise Servers SPI. Each report description includes a list of the performance counters used within the report.

- Reports for **BizTalk 2000 and 2002**
- Reports for **BizTalk 2002 only**
- Reports for **BizTalk 2004 only**
- Reports for **BizTalk 2006 only**

Reports for **BizTalk 2000 and 2002**

All reports in the groupings listed below are available for BizTalk 2000 and BizTalk 2002 Servers:

- BizTalk Services Statistics
- BizTalk Messaging Service and Orchestration Service Process CPU Statistics
- BizTalk Messaging Service and Orchestration Service Process Memory Statistics

BizTalk Services Statistics (g_BSServiceSummary.rpt): This report summarizes the usage patterns of BizTalk 2000 Server's services.

Counters:

- Asynchronous Submissions/sec
- Documents Processed/sec
- Documents Received/sec
- Items Suspended/sec
- Synchronous Submissions/sec

BizTalk Messaging Service and Orchestration Service Process CPU Statistics (g_BSCPUSummary.rpt): This report shows summary CPU statistics of BizTalk Server processes compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by the Messaging Service and Orchestration Service processes, compared with the percentage of time the system's CPU was busy.

Counters:

- System % Processor Time
- Messaging Service % Processor Time
- Messaging Service Thread Count
- Orchestration Service % Processor Time
- Orchestration Service Thread Count

BizTalk Messaging Service and Orchestration Service Process Memory Statistics (g_BSMemorySummary.rpt): This report shows summary memory statistics of BizTalk Server processes.

Counters:

- PageFaults/sec
- Private Bytes
- Working Set

Related Topics:

- BizTalk Server 2002 reports
- BizTalk Server 2004 reports
- BizTalk Server 2006 reports
- BizTalk Server Graphs

BizTalk Server 2002 reports

The following predefined reports for the BizTalk Server 2002 are available with the Microsoft Enterprise Servers SPI:

BizTalk Messaging and Xlang CPU Report (g_BSCPUSummaryReport.rpt): This report shows summary CPU statistics of BizTalk Server processes compared with overall CPU statistics of the system, in graphical and tabular format. The summarized process statistics include the percentage of CPU time used by the Messaging Service and Orchestration Service processes, compared with the percentage of time the system's CPU was busy.

BizTalk Messaging and Xlang Memory Report (g_BSMemorySummaryReport.rpt): This report shows summary memory statistics of BizTalk Server processes in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes and working set used by the Messaging and Orchestration Service processes.

BizTalk Messaging Service and Xlang Service Reports:

BizTalk Server 2002 provides a number of performance counters to monitor the messaging and orchestration service. Logging policies log data from these counters into the service reporter database. This data is later used to generate the BizTalk messaging reports.

Cumulative counter reports

The following reports, using the various Messaging Service and Xlang counters, can be helpful in many administrative and service management tasks, including capacity planning and the debugging of performance and scalability problems. For each of them there is a **weekly** report and a **monthly** report available:

- **BizTalk Messaging Statistics Report** (g_BizTalkMessagingIntervalCountsWeekly.rpt and g_BizTalkMessagingIntervalCountsMonthly.rpt): These reports give the total number of the Documents Processed, Documents Received, Interchanges Received, Asynchronous Submissions, Synchronous Submissions and Items Suspended of BizTalk messaging counters, either every 12 hours for the last seven days (weekly) or each day for the last 30 days (monthly). Using the reports BizTalk administrators can customize their BizTalk messaging service.
- **Xlang Statistics Report** (g_BizTalkXlangStatsIntervalCountsWeekly.rpt and g_BizTalkXlangStatsIntervalCountsMonthly.rpt): These reports give the average of Completed Schedule Instances/sec, Failed Schedule Instances/sec, Running Schedule Instances/sec, Dehydrated Schedule Instances/sec of BizTalk Orchestration, either every 12 hours for last seven days (weekly) or

each day for last 30 days (monthly).

Per/Sec counter reports

- **Documents Statistics Report** (g_BizTalkDocsStatsWeekly.rpt and g_BizTalkDocsStatsMonthly.rpt): These reports give the average of Documents Mapped/sec, Documents Parsed/sec, Documents Processed/sec, Documents Received/sec, Documents Serialized/sec of BizTalk messaging counters, either weekly or monthly. Weekly report collects these counters for every hour in each day for the last seven days. Monthly report collects the counters every day for the past 30 days. Chart is plotted showing these counters for each included day.
- **General Statistics Report** (g_BizTalkGeneralStatsWeekly.rpt and g_BizTalkGeneralStatsMonthly.rpt): These reports give the average of Asynchronous Submissions, Synchronous Submissions, Transactions Aborted, Items Suspended of BizTalk messaging and Xlang counters, either weekly or monthly. Weekly report collects these counters for every hour in each day for the last seven days. Monthly report collects the counters every day for the past 30 days. Chart is plotted showing these counters for each included day.
- **Interchange Statistics Report** (g_BizTalkInterchangesStatsWeekly.rpt and g_BizTalkInterchangesStatsMonthly.rpt): These reports give the average of Interchanges Decrypted/sec, Interchanges Encoded/sec, Interchanges Encrypted/sec, Interchanges Received/sec, Interchanges Transmitted/sec, Interchanges Decoded/sec of BizTalk messaging counters, either weekly or monthly. Weekly report collects these counters for every hour in each day for the last seven days. Monthly report collects the counters every day for the past 30 days. Chart is plotted showing these counters for each included day.
- **Xlang Statistics Report** (g_BizTalkXlangStatsWeekly.rpt and g_BizTalkXlangStatsMonthly.rpt): These reports give the average of Completed Schedule Instances/sec, Failed Schedule Instances/sec, Running Schedule Instances/sec and Activated Schedule Instances/sec of BizTalk Orchestration, either weekly or monthly. Weekly report collects these counters for every hour in each day for the last seven days. Monthly report collects the counters every day for the past 30 days. Chart is plotted showing these counters for each included day.

Suspended queue reports:

The Suspended Queue contains work items that have failed processing for a variety of reasons including parsing errors, serialization errors, failed transmissions, or the inability to find a channel configuration. Suspended Queue state can be any of these Initial, Custom component, Parsing, Document, Validation, Channel selection, Field Tracking, Correlating, Mapping, Serializing, Encoding, Signing, Encryption, or Transmitting.

BizTalk triggers the DocSuspendedEvent for each document in a suspended queue. The DocSuspendeEvent contains Destination, Source, DocName/Type and State information. The

NET_BS_DocSuspendedEvent policy logs this data into the service reporter database and generates the following reports:

- **Document Suspended Report based on Source** (g_BizTalkSuspendedSource.rpt): This report generates a chart and report for each BizTalk server on the managed node. It gives details about the number of documents in a suspended queue for each source organization and for each BizTalk server. BizTalk admin can use this report to find out how many documents from the source organization have ended up in the suspended queue.
- **Document Suspended Report based on Destination** (g_BizTalkSuspendedDestination.rpt): This report generates a chart and report for each BizTalk server on the managed node. It gives details about the number of documents in a suspended queue for each destination organization and for each BizTalk server. BizTalk admin can use this report to find out how many documents from the source organization have ended up in the suspended queue.
- **Document Suspended Report based on State** (g_BizTalkSuspendedState.rpt): This report generates a chart and report for each BizTalk server on the managed node. It gives details about the number of documents in a suspended queue based on the suspended queue state for each BizTalk server. BizTalk admin can use this report to find out how many documents are in the suspended queue for each of the above mentioned states.
- **Document Suspended Report based on Document Type** (g_BizTalkSuspendedDocType.rpt): This report generates a chart and report for each BizTalk server on the managed node. It gives details about the number of documents in a suspended queue based on document type and for each BizTalk server. BizTalk admin can use this report to find out how many documents are in the suspended queue for each document type.

Related Topics:

- BizTalk Server reports
- BizTalk Server 2004 reports
- BizTalk Server Graphs

BizTalk Server 2004 reports

The Microsoft Enterprise Servers SPI offers the following reports for BizTalk Server 2004:

BizTalk Document Process Rate Monthly/BizTalk Document Process Rate Weekly

These reports give the summarization of the following monthly/weekly statistics related to BizTalk Documents:

- **Documents processed/sec** : Integer representing the average number of documents processed per second, that is, pulled from the Work queue and sent to a port destination address.
- **Documents received/sec** : Integer representing the average number of documents that have been received by BizTalk Server per second. This includes all documents that make it into the Work queue and any that have failed.
- **Documents suspended/sec** : Integer representing the average number of items suspended in the Suspended queue per second.

BizTalk Processes CPU Statistics

This report shows a summary of CPU statistics of BizTalk Server processes, compared with overall CPU statistics of the system, in graphical and tabular format. The summarized process statistics include the percentage of CPU time used by BTSHatApp, BTSNTSvc, ENTSSO and RuleEngineUpdateService processes, compared with the percentage of time the system's CPU was busy.

BizTalk Processes Memory Statistics

This report shows summary memory statistics of BizTalk Server processes in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by BTSHatApp, BTSNTSvc, ENTSSO and RuleEngineUpdateService processes.

BizTalk Orchestration Statistics Monthly/BizTalk Orchestration Statistics Weekly

These reports give the summarization of the following statistics related to orchestrations:

- **Orchestrations completed/sec** : Average number of orchestrations completed per second.

- **Orchestrations created/sec** : Average number of orchestrations created per second.
- **Orchestrations dehydrated/sec** : Average number of orchestrations dehydrated per second.
- **Orchestrations discarded/sec** : Average number of orchestrations discarded per second.
- **Orchestrations rehydrated/sec** : Average number of orchestrations rehydrated per second.
- **Orchestrations suspended/sec** : Average number of orchestrations suspended per second.
- **Database transactions/sec** : Average number of database transactions per second.

BizTalk Transactional Rate Monthly/BizTalk Transactional Rate Weekly

A **scope** is a framework for grouping actions, primarily used for transactional execution and exception handling. **Compensation** is a process where a piece of code gets executed to undo or reverse the effects of a successfully committed transaction.

These reports give the monthly/weekly summarization of the following statistics related to transactions:

- **Transactional scopes aborted/sec** : Average number of long-running or atomic scopes that have been aborted.
- **Transactional scopes committed/sec** : Average number of long-running or atomic scopes that have successfully completed.
- **Transactional scopes compensated/sec** : Average number of long-running or atomic scopes that have successfully completed compensation scopes.

BizTalk Suspended Documents Monthly/BizTalk Suspended Documents Weekly

These reports give the weekly suspended document statistics, segregated by the following attributes:

- **State** : Documents that are in resumable and non-resumable states.
- **Server Name** : Processing server name.
- **Priority** : Document Priority.

BizTalk TDDS (Tracking Data Decode Service) Statistics

TDDS is also known as the BAM Event Bus Service. This report gives the monthly summarization of the following statistics related to TDDS:

- **Events being processed** : The number of events the BAM Event Bus Service is currently processing.

- **Batches being processed** : The number of batches the BAM Event Bus Service is currently processing.
- **Events Committed** : The number of events the BAM Event Bus Service has committed to SQL Server in the last second.
- **Records Committed** : The number of records the BAM Event Bus Service has committed to SQL Server in the last second.
- **Batches Committed** : The number of batches the BAM Event Bus Service has committed to SQL Server in the last second.

Enterprise Single Sign-on - Monthly

This report gives the monthly summarization of the following statistics related to enterprise SSO:

- **GetConfigInfo** : Total number of config info accessed.
- **IssueTicket/sec** : Total number of tickets issued.
- **GetCredentials/sec** : Total number of credentials accessed.
- **RedeemTicket/sec** : Total number of tickets redeemed.
- **ValidateAndRedeemTicket/sec** : Total number of tickets validated and redeemed.

Related Topics:

- BizTalk Server reports
- BizTalk Server 2002 only reports
- BizTalk Server Graphs

BizTalk Server 2006 reports

The Microsoft Enterprise Servers SPI offers the following reports for BizTalk Server 2006:

BTS Document Process Rate Monthly/BTS Document Process Rate Weekly

These reports give the summarization of the following monthly/weekly statistics related to BizTalk Documents:

- **Documents processed/sec** : Integer representing the average number of documents processed per second, that is, pulled from the Work queue and sent to a port destination address.
- **Documents received/sec** : Integer representing the average number of documents that have been received by BizTalk Server per second. This includes all documents that make it into the Work queue and any that have failed.
- **Documents suspended/sec** : Integer representing the average number of items suspended in the Suspended queue per second.

BTS Processes CPU Statistics

This report shows a summary of CPU statistics of BizTalk Server processes, compared with overall CPU statistics of the system, in graphical and tabular format. The summarized process statistics include the percentage of CPU time used by BTSHatApp, BTSNTSvc, ENTSSO and RuleEngineUpdateService processes, compared with the percentage of time the system's CPU was busy.

BTS Processes Memory Statistics

This report shows summary memory statistics of BizTalk Server processes in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by BTSHatApp, BTSNTSvc, ENTSSO and RuleEngineUpdateService processes.

BTS Orchestration Statistics Monthly/BizTalk Orchestration Statistics Weekly

These reports give the summarization of the following statistics related to orchestrations:

- **Orchestrations completed/sec** : Average number of orchestrations completed per second.
- **Orchestrations created/sec** : Average number of orchestrations created per second.
- **Orchestrations dehydrated/sec** : Average number of orchestrations dehydrated per second.

- **Orchestrations discarded/sec** : Average number of orchestrations discarded per second.
- **Orchestrations rehydrated/sec** : Average number of orchestrations rehydrated per second.
- **Orchestrations suspended/sec** : Average number of orchestrations suspended per second.
- **Database transactions/sec** : Average number of database transactions per second.

BizTalk Transactional Rate Monthly/BizTalk Transactional Rate Weekly

A **scope** is a framework for grouping actions, primarily used for transactional execution and exception handling. **Compensation** is a process where a piece of code gets executed to undo or reverse the effects of a successfully committed transaction.

These reports give the monthly/weekly summarization of the following statistics related to transactions:

- **Transactional scopes aborted/sec** : Average number of long-running or atomic scopes that have been aborted.
- **Transactional scopes committed/sec** : Average number of long-running or atomic scopes that have successfully completed.
- **Transactional scopes compensated/sec** : Average number of long-running or atomic scopes that have successfully completed compensation scopes.

BTS Suspended Documents Monthly/BizTalk Suspended Documents Weekly

These reports give the weekly suspended document statistics, segregated by the following attributes:

- **State** : Documents that are in resumable and non-resumable states.
- **Server Name** : Processing server name.
- **Priority** : Document Priority.

BTS TDDS (Tracking Data Decode Service) Statistics

TDDS is also known as the BAM Event Bus Service. This report gives the monthly summarization of the following statistics related to TDDS:

- **Events being processed** : The number of events the BAM Event Bus Service is currently processing.
- **Batches being processed** : The number of batches the BAM Event Bus Service is currently processing.
- **Events Committed** : The number of events the BAM Event Bus Service has committed to SQL Server

in the last second.

- **Records Committed** : The number of records the BAM Event Bus Service has committed to SQL Server in the last second.
- **Batches Committed** : The number of batches the BAM Event Bus Service has committed to SQL Server in the last second.

BTS Enterprise Single Sign-on - Monthly

This report gives the monthly summarization of the following statistics related to enterprise SSO:

- **GetConfigInfo** : Total number of config info accessed.
- **IssueTicket/sec** : Total number of tickets issued.
- **GetCredentials/sec** : Total number of credentials accessed.
- **RedeemTicket/sec** : Total number of tickets redeemed.
- **ValidateAndRedeemTicket/sec** : Total number of tickets validated and redeemed.

Related Topics:

- BizTalk Server reports
- BizTalk Server 2006 policies
- BizTalk Server Graphs

BizTalk Server graphs

The following Microsoft Enterprise Servers SPI predefined graphs for BizTalk Server are offered:

- Messaging Service CPU Statistics
- Messaging Service Memory Statistics
- Orchestration Service CPU Statistics
- Orchestration Service Memory Statistics
- BizTalk Services Statistics
- Graphs for **BizTalk Server 2002** only
- Graphs for **BizTalk Server 2004 and 2006** only

Messaging Service CPU Statistics This graph shows a summary of the Messaging Service CPU statistics of BizTalk Server processes compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by the Messaging Service process, compared with the percentage of time the system's CPU was busy.

Messaging Service Memory Statistics This graph shows a summary of the Messaging Service Memory statistics including the page faults per second, private bytes, and working set used by the Messaging Service.

Orchestration Service CPU Statistics This graph shows a summary of the Orchestration Service CPU statistics of BizTalk Server processes compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by Orchestration Service processes, compared with the percentage of time the system's CPU was busy.

Orchestration Service Memory Statistics This graph shows a summary of the Orchestration Service Memory statistics including the page faults per second, private bytes, and working set used by Orchestration Service processes.

BizTalk Services Statistics This graph shows a summary of the usage patterns of BizTalk Server's services, including Asynchronous Submissions/sec, Documents Received/sec, Synchronous Submissions/sec, Documents Processed/sec, Item Suspended/sec.

Graphs for BizTalk Server 2002 only :

- **BizTalk Document Interval Counts:** this graph shows the actual count of Documents Processed,

Received and Items Suspended, during the selected time interval.

- **BizTalk Submissions Interval Counts:** this graph shows the actual count of all Submissions (Synchronous and Asynchronous) and Interchanges Received in the selected time interval.
- **BizTalk Document Statistics:** this graph shows rates per second of all BizTalk Document related statistics for the selected time interval. Uses the Documents Mapped/sec, Documents Parsed/sec, Documents Processed/sec, Documents Received/sec, Documents Serialized/sec, Asynchronous Submissions/sec, Synchronous Submissions/sec counters.
- **BizTalk Schedules Interval Counts:** this graph shows the actual count of BizTalk XLANG schedule instances, using the Activated, Running, Completed, Dehydrated, Failed and Transactions Aborted counters for the selected time interval.
- **BizTalk Interchange Statistics:** this graph shows the rates per second of all BizTalk interchange related statistics. Uses the Interchanges Decoded/sec, Interchanges Decrypted/sec, Interchanges Encoded/sec, Interchanges Encrypted/sec, Interchanges Received/sec, and Interchanges Transmitted/sec counters.
- **BizTalk Schedule Statistics:** this graph shows rates per second of all BizTalk XLANG Schedule related statistics for the selected time interval. Uses the Schedules Activated/sec, Completed Schedule Instances/sec, Failed Schedule Instances/sec, Running Schedule Instances/sec, and Transactions Aborted/sec counters.

Graphs for BizTalk Server 2004 and 2006 only :

- BizTalk Server Application Service CPU
- Enterprise Single Sign-On Service CPU
- Rule Engine Update Service CPU

These graphs represent the percentage of time spent by the processors executing threads for the BizTalk Server Application Service, Enterprise Single Sign-On Service and Rule Engine Update Service processes. This counter can be compared to System Processor Time to determine to what extent these processes are utilizing processor time.

- **BizTalk Server Application Service Memory**
- **Enterprise Single Sign-On Service Memory**
- **Rule Engine Update Service Memory**

Page Faults/sec represents the rate page faults occur in the threads executing in the BizTalk Server Application Service, Enterprise Single Sign-On Service and Rule Engine Update process.
A **page fault** occurs when a thread refers to a virtual memory page that is not in its working set in main

memory. The graph shows the average rate at which page faults occur, by the threads executing in these processes.

Working Set represents the number of bytes in the working set of the BizTalk Server Application Service, Enterprise Single Sign-On Service and Rule Engine Update Service process. The Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a certain threshold, pages are left in the working set of a process even if they are not in use. When free memory falls below a certain threshold, pages are trimmed from working sets. If they are needed, they are then soft-faulted back into the working set before they leave main memory.

Private Bytes is the current number of bytes the BizTalk Server Application Service, Enterprise Single Sign-On Service and Rule Engine Update process has allocated that cannot be shared with other processes.

Related Topics:

- BizTalk Server Reports

BizTalk Server tools

- BizTalk Server 2002 Suspended Document Viewer tool
- BizTalk Server 2002 Document Tracking tool
- BizTalk Server 2004 and 2006 Database Configuration tool
- Using the Microsoft Enterprise Servers SPI Self Healing Info tool for troubleshooting

BizTalk Server 2002 Suspended Document Viewer

The BizTalk suspended queue contains work items that have failed to process for a variety of reasons, including parsing errors, serialization errors, failed transmissions, or the inability to find a channel configuration.

The Microsoft Enterprise Servers SPI Suspended Document Viewer tool displays all documents in the BizTalk suspended queue, for a targeted BizTalk Server. It allows users to browse, resubmit or delete any document or interchange in the suspended queue. (Interchanges are collections of one or more document instances that consist of a single transmission, that are exchanged from application to application within an organization, or from one trading partner to another).

The Suspended Document Viewer shows the Server name and the Server Group to which the server belongs, the Document/Interchange name, the State (a brief description In addition there is a detailed description of what error caused the document to be held in the suspended queue, and the entire contents of the interchange/document are displayed in the Content field.

This tool can also be used for resubmitting documents in the suspended queue. There is a **Resubmit** and a **Resubmit All** button on the viewer. When clicked they resubmit selected, or all, documents in the queue.

This tool can be launched in either of the following ways:

- operator initiated command
- standalone tool

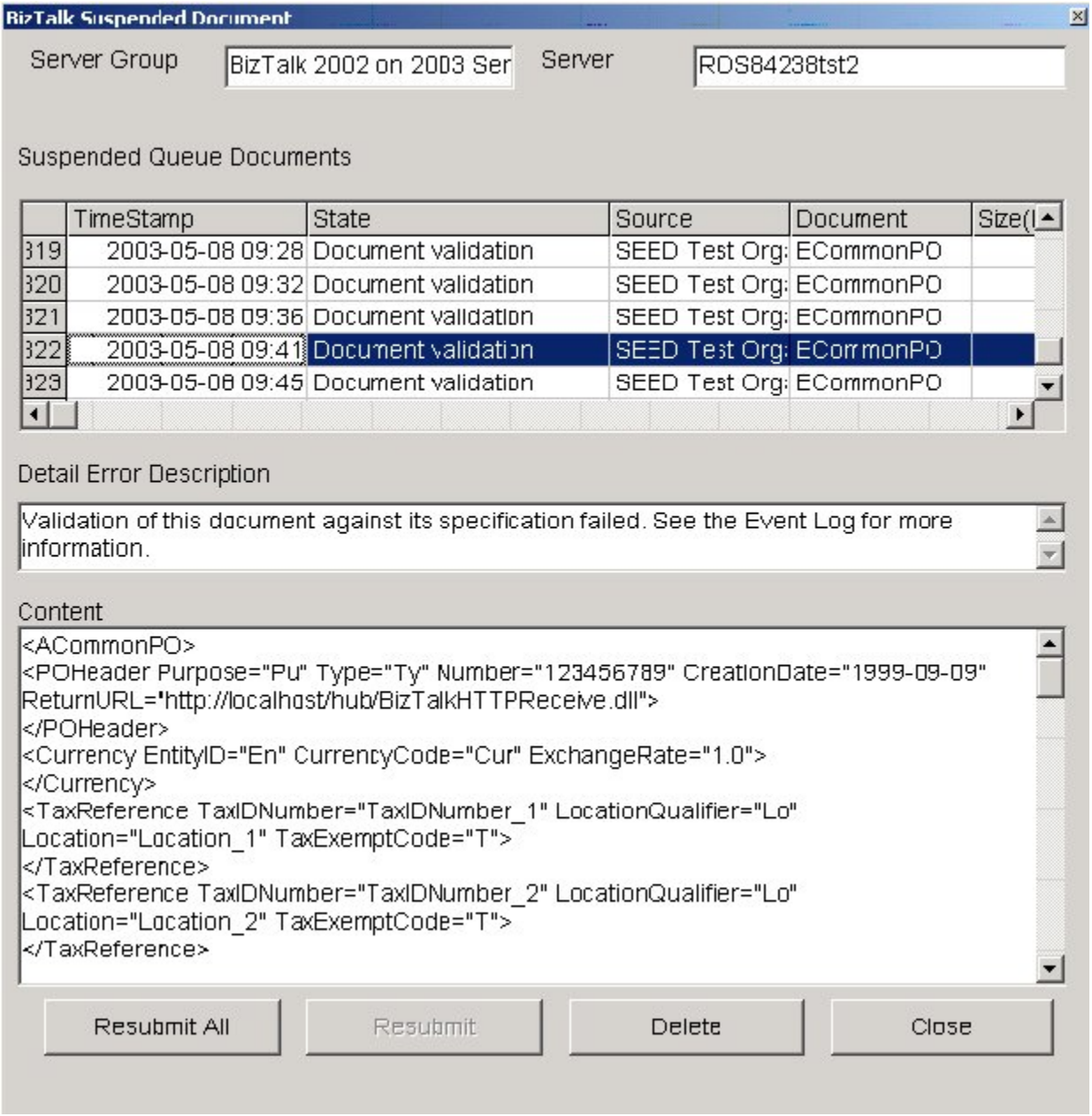
To launch as an operator initiated command:

1. Deploy the policy **NET_BS_DocSuspendedEvent** located in **Policy Management** → **Policy groups** → **SPI for Microsoft Enterprise Servers** → **Biztalk Server 2002** → **Manual-Deploy** → **Document** group.

2. After deploying this policy, when a document goes into the suspended queue, a message will be sent to the HPOM management console. The operator must right-click the message, select **Commands → Start** and click **Operator initiated command**. This opens the Suspended Document Viewer.

To launch as a standalone tool:

1. Go to **Tools → SPI for Microsoft Enterprise Servers → BizTalk Server.**
2. Double-click **BizTalk Suspended Document Viewer**. This tool takes the hostname of the Biztalk server as the parameter, so before the tool launches you are prompted to provide the correct Biztalk server hostname.
3. Next a dialog for server Login Information displays. This information is used to access the BizTalk Suspended Document data on the WM repository where the BizTalk server is running, so the user must have the required permissions. (If the user has the required credentials you can click **OK** without entering the information).
4. The BizTalk Suspended Document viewer opens.



BizTalk Server 2002 Document Tracking

BizTalk Document Tracking is a stand-alone web application that you can use to view the progress of documents processed by Microsoft BizTalk Server 2002. You can create queries or advanced queries to extract essential information from the Tracking database in an easy-to-view format. For example, in BizTalk Document Tracking you can view captured information about the document source and destination, the document name and document type, and relevant date and time parameters. You can also create queries that display standard and custom-search fields so that you can analyze your business practices. For example, a Purchase Order Total field can be stored for every purchase order sent to

suppliers.

In the Microsoft Enterprise Servers SPI this application is integrated with HPOM, so that this BizTalk tool can be easily launched from the HPOM console.

To launch as a standalone tool:

1. Go to **Tools** → **SPI for Microsoft Enterprise Servers** → **BizTalk Server.**
2. Double-click **BizTalk Document Tracking** . This tool takes the hostname of the Biztalk server as the parameter, so before the tool launches you are prompted to provide the correct Biztalk server hostname.
3. Next a dialog for server Login Information displays. This information is used to access the BizTalk document tracking data on the WM repository where the BizTalk server is running, so the user must have the required permissions. (If the user has the required credentials you can click **OK** without entering the information).
4. The BizTalk Document Tracking tool opens.

BizTalk Server 2004 and 2006 Database Configuration tool

(MSES_BTS_DB_Configuration)

> **NOTE:**
> The Database Configuration tool must be launched from the management server only, not from a remote console. If you use Windows authentication, do not run the MSES_BTS_DB_Configuration tool.

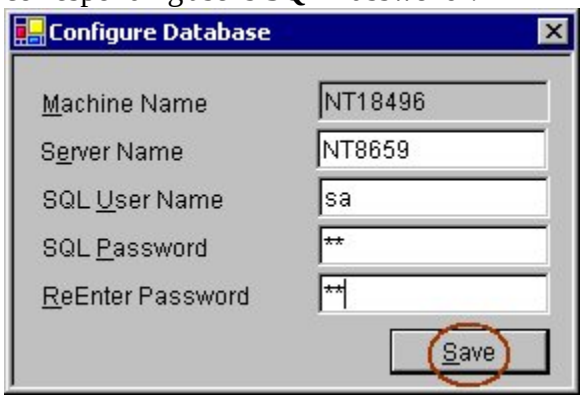
Unlike BizTalk Server 2002, BizTalk Server 2004 and 2006 store data in SQL server instead of the WMI CIMV2 database. For the Microsoft Enterprise Servers SPI to fetch related data it needs to connect to BizTalk Server's SQL database.

Before running Discovery, the HPOM administrator needs to configure the SQL database for all nodes with BizTalk Server installed. Windows integrated security (SSPI mode) does not work if the SQL authentication mode is set for SQL server. If SQL authentication is "*users /*", the HPOM console needs to know the SQL user name and password. To connect to SQL server even when it is in SQL authentication mode, the HPOM administrator can use the MSES_BTS_DB_Configuration tool to store the corresponding SQL server name, and the SQL user name and password. If this configuration is not done for BizTalk Server 2004 or 2006 nodes, the SQL user name and password's value will be considered as the default.

Launching the tool:

1. In the HPOM console, locate **Tools→ SPI for Microsoft Enterprise Server→ BizTalk Server** .

- Double-click the **MSES_BTS_DB_Configuration** tool.
- The **Edit Parameters** window opens. Select all nodes containing BizTalk Server and launch the tool.
- A **Configure Database** window opens for each node selected. The **Machine Name** field is read only, and the user needs to enter **Server Name** (for BizTalk Database), **SQL User Name** and corresponding user's **SQL Password** .



> **NOTE:**
> Use the database user name and password with administrative privileges.

- **Save** the configuration.

Related Topics:

- Using the Microsoft Enterprise Servers SPI Self Healing Info tool for troubleshooting
- Configuring the Microsoft Enterprise Servers SPI for BizTalk 2004 and 2006
- BizTalk Server Policies
- BizTalk Server Reports
- BizTalk Server Graphs
- BizTalk Server Service Map

Commerce Server

Microsoft's Commerce Server is a tool for building highly sophisticated, scalable, business-to-consumer and business-to-business e-commerce applications, on the Microsoft Windows operating system. Using Commerce Server, business managers can configure, manage, and analyze their Web site usage and productivity, with features such as customer profiling and targeted marketing campaigns. Web site developers can use Commerce Server to provide merchandising, catalog display, customer service, and order capture and receipt to e-commerce applications.

The Microsoft Enterprise Servers SPI monitors Commerce Server 2000 and Commerce Server 2002 in the following ways:

Availability Monitoring

Commerce Server services are monitored to determine whether they are up or down. If the service is not running, and the service in startup is set to "Auto Start", then an attempt is made to restart the service. A console error message is sent to indicate that the service is not running. Monitored services include:

- Commerce Server Direct Mailer (DMLService)
- Commerce Server List Manager (listmanager)
- Commerce Server Predictor (PredServ)

Event Monitoring

Event monitoring of the Windows 2000 Event Log occurs for Commerce Server events. Console messages are sent for all errors, warnings, and information events logged for the following sources:

- Commerce Server 2000
- Commerce Server 2002
- Commerce Server Direct Mailer

Performance Monitoring

Commerce Server performance monitoring includes both specific Commerce Server performance counters and CPU process-related counters. Each policy for performance monitoring has both error and warning thresholds.

Server Logging

Selected performance data for CPU and memory counters is logged for the Commerce Server.

> **NOTE:**
> For Server Logging, deployment of the Windows OS SPI logging policy, WINOSSPI-WINOS_Win2k_Logging, is required to log process-related data for CPU and memory counters. The counters specific to Commerce Server are documented in the policy section. Refer to the Windows OS SPI Policies for information about the process-related data for CPU and memory counters.

Related Topics:

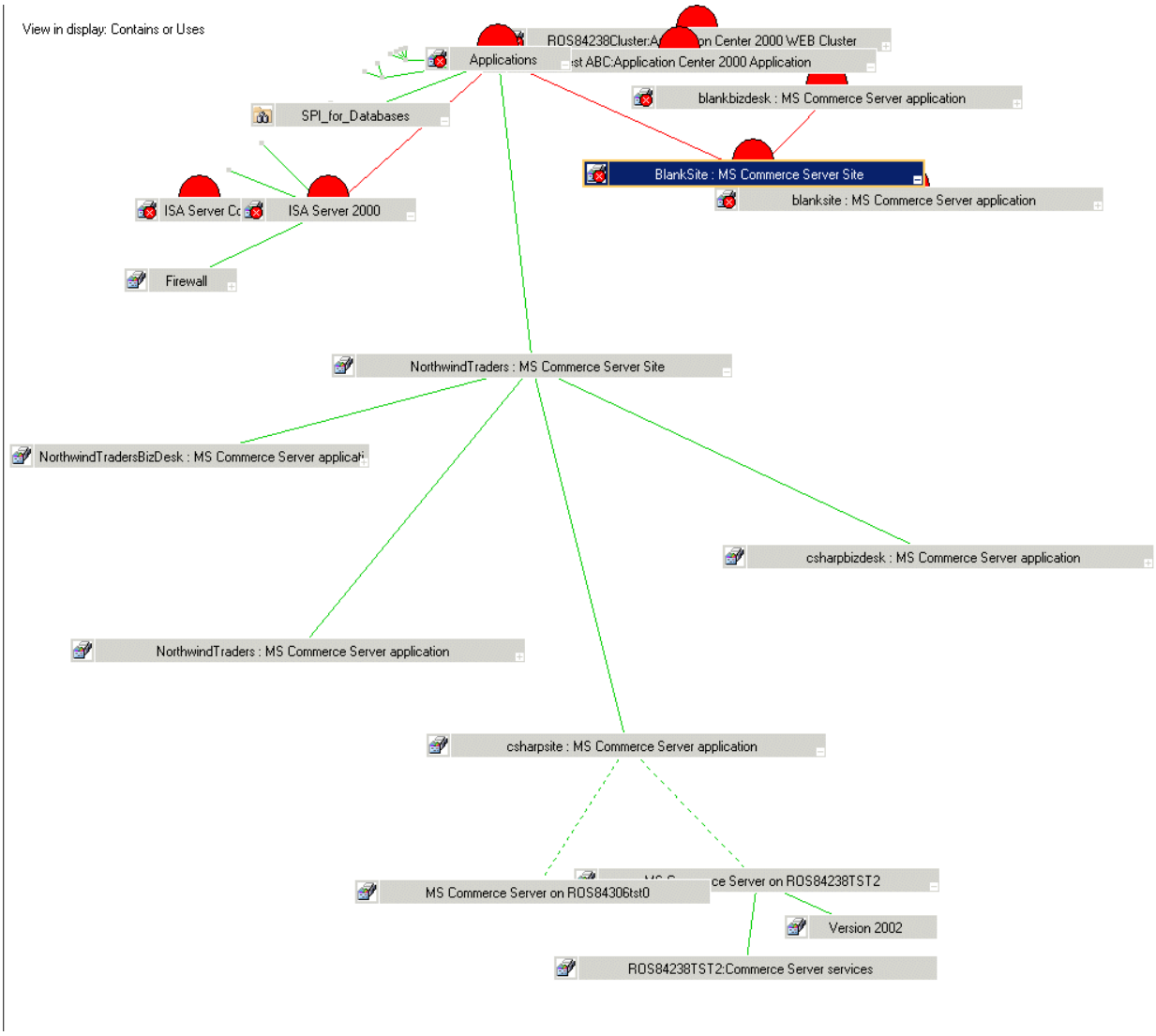
- Commerce Server Policies
- Commerce Server Reports
- Commerce Server Graphs
- Commerce Server Service Map

Commerce Server service map

The Commerce Server service map displays the nodes where Commerce servers have been installed. The service maps are available under both the Applications and the Systems Infrastructure sections on the HPOM console.

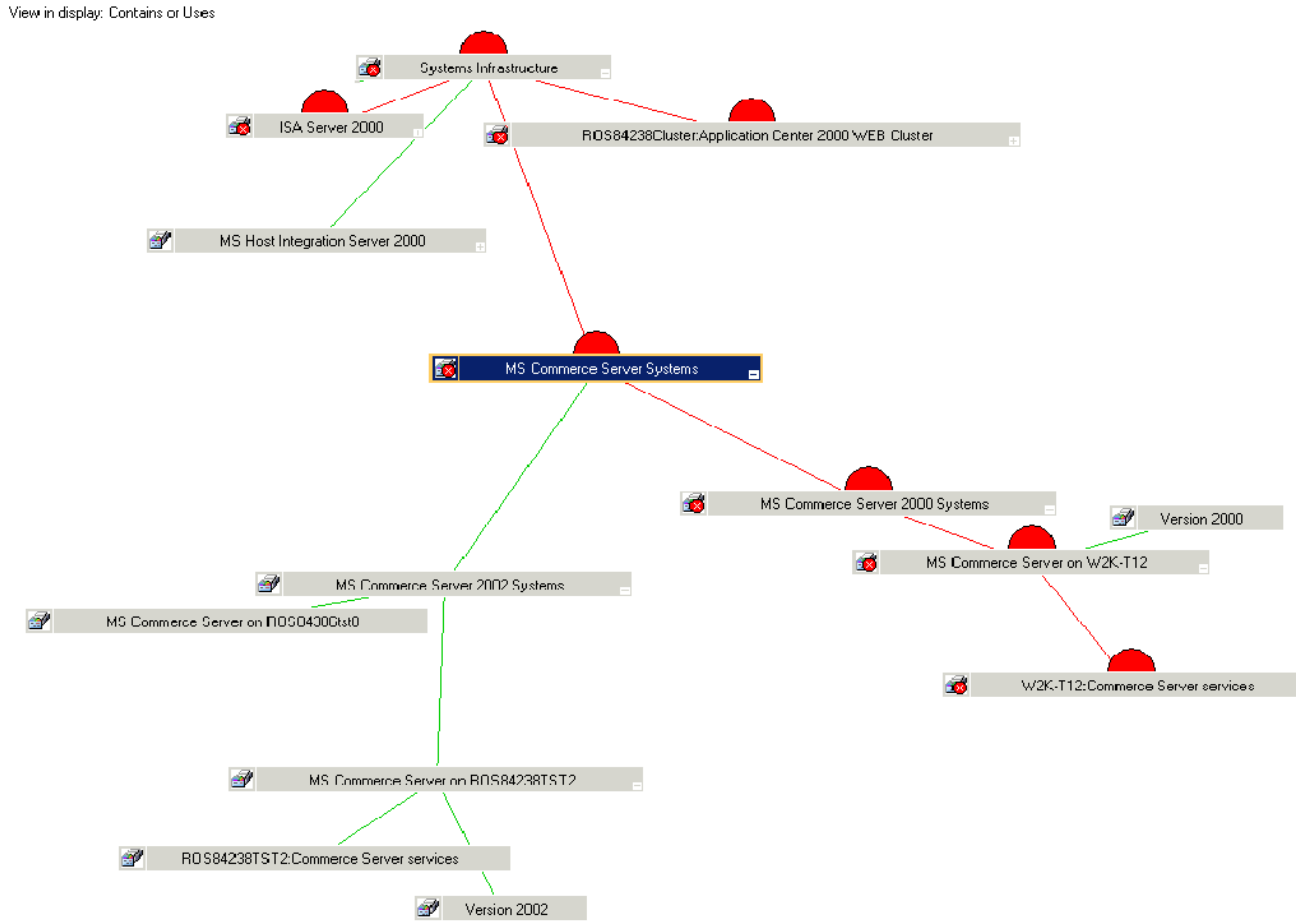
Applications

The service map shows the Commerce Server sites and the applications running under them. It also shows where the applications are hosted by showing all dependencies on servers.



Systems Infrastructure

The Systems Infrastructure service map shows all Commerce Server machines, grouped by version (2000 and 2002).



Related Topics:

- Creating Service Maps for Microsoft Enterprise Servers

Commerce Server policies

The following predefined policies for monitoring Microsoft Commerce Server (versions 2000 and 2002), are available with the Microsoft Enterprise Servers SPI:

- Availability Monitoring
- Windows Event Log Monitoring
- Performance Monitoring
- Server Logging
- Discovery

Availability Monitoring

Policy Descriptions

NET_CommerceServerServices

Description: This policy monitors the Commerce Server services: DMLService, ListManager, and Predictor Service. If a service is stopped it is restarted automatically.

Windows Event Log Monitoring

Policy Descriptions

NET_CommerceServerFwdApplicationError

Description: Forwards all Commerce Server application log entries with severity 'Error'

NET_CommerceServerFwdApplicationInformation

Description: Forwards all Commerce Server application log entries with severity 'Information'

NET_CommerceServerFwdApplicationWarning

Description: Forwards all Commerce Server application log entries with severity 'Warning'

Performance Monitoring

Policy Descriptions

NET_CS-AuthChecksFailedsec/NET_CS2002-AuthChecksFailedsec

Description: Checks the number of failed authentication checks per second at a particular commerce site, for Commerce Server 2000 or 2002.

NET_CS-CatalogQueriessec/NET_CS2002-CatalogQueriessec

Description: Checks the number of queries made to the catalog system per second, for Commerce Server 2000 or 2002.

NET_CS-DirectMailErrorssec/NET_CS2002-DirectMailErrorssec

Description: Checks the number of Direct Mailer errors per second during mail generation, for Commerce Server 2000 or 2002.

NET_CS-NumberofCachePurges

Description: Checks the number of times the foreground thread purged entries from the profile object cache to search for a free block of memory.

NET_CS-PageFaultssec-DirectMailer

Description: Checks Process.Page Faults/sec for the Commerce Server Direct Mailer service.

NET_CS-PageFaultssec-ListManager

Description: Checks Process.Page Faults/sec for the Commerce Server List Manager service.

NET_CS-PageFaultssec-Predictor

Description: Checks Process.Page Faults/sec for the Commerce Server Predictor service.

NET_CS-PipelineErrorssec/NET_CS2002-PipelineErrorssec

Description: Checks the number of errors generated by the particular pipeline component per second, for Commerce Server 2000 or 2002.

NET_CS-PrivateBytes-DirectMailer

Description: Checks Process.Private Bytes for the Commerce Server Direct Mailer service.

NET_CS-PrivateBytes-ListManager

Description: Checks Process.Private Bytes for the Commerce Server List Manager service.

NET_CS-PrivateBytes-Predictor

Description: Checks Process.Private Bytes for the Commerce Server Predictor service.

NET_CS-ProcessorTime-DirectMailer

Description: Checks Process.% Processor Time for the Commerce Server Direct Mailer service.

NET_CS-ProcessorTime-ListManager

Description: Checks Process.% Processor Time for the Commerce Server List Manager service.

NET_CS-ProcessorTime-Predictor

Description: Checks Process.% Processor Time for the Commerce Server Predictor service.

NET_CS-ThreadCount-DirectMailer

Description: Checks Process.Thread Count for the Commerce Server Direct Mailer service.

NET_CS-ThreadCount-ListManager

Description: Checks Process.Thread Count for the Commerce Server List Manager service.

NET_CS-ThreadCount-Predictor

Description: Checks Process.Thread Count for the Commerce Server Predictor service.

NET_CS-WorkingSet-DirectMailer

Description: Checks Process.Working Set for the Commerce Server Direct Mailer service.

NET_CS-WorkingSet-ListManager

Description: Checks Process.Working Set for the Commerce Server List Manager service.

NET_CS-WorkingSet-Predictor

Description: Checks Process.Working Set for the Commerce Server Predictor service.

Server Logging

Policy Descriptions

NET_CommerceServer_Logging/NET_CommerceServer2002_Logging

Description: This policy logs selected performance data for Commerce Server. Deployment of Windows OS SPI logging policy WINOSSPI-WINOS_Win2k_Logging is required to log process-related data for CPU and memory counters.

Counters:

- **CS2000/CS2002: Marketing and Catalog**
  - Catalog
    - Catalog Queries/sec
  - DML
    - Direct Mail Errors/sec

    - Direct Mail Jobs Running
    - Mail Messages Sent/sec
    - Total Direct Mail Errors
    - Total Messages Sent
  - LRUCache
    - Cache Size
    - Flushes/sec
    - Hits/sec
    - Misses/sec
  - Predictor
    - Client Avg Prediction Time
    - Client Model Loads From File
    - Total Client Model Loads
    - Total Client Predictions
- **CS 2000/CS2002 Pipelines**
  - Average execution time
  - Executions per second o
  - Errors per second
  - Warnings per second
  - Executions total
  - Errors total
  - Warnings total
- **CS2000/CS2002: User Profile Management**
  - AuthFilter
    - AutoCookies/sec
    - TotalAutoCookies
    - Total Requests Failed

- AuthMgr
  - AnonTickets/sec
  - TotalAnonTickets
  - AuthTickets/sec
  - TotalAuthTickets
  - AuthChecks Failed/sec
  - TotalAuthChecks Failed
  - AuthChecks Succeeded/sec
  - TotalAuthChecks Succeeded
  - AuthMgr Objects/sec
  - Total AuthMgr Objects Created
- UPM
  - Cache Objects
  - Cache Hit Rate
  - Cache Miss Rate

Discovery

Policy Descriptions

NET_CommerceServer_Discovery_Application

Description: This policy discovers the service topology for Commerce Server 2000 and 2002, adds Commerce Server sites and applications in a site to the service map, and shows on the service map what systems the applications are hosted on, with dependencies indicated from the application to the system.

NET_CommerceServer_Discovery_System

Description: On running this policy, the Commerce Server systems and dependencies on other services (Windows OS, IIS and Commerce Server services) are added to the service map.

Related Topics:

- Deploying Policies for Microsoft Enterprise Servers
- Commerce Server Overview

Commerce Server reports

Predefined reports for Commerce Server 2000 and 2002 are available with the Microsoft Enterprise Servers SPI. Each report description includes a list of the performance counters used within the report.

- AuthFilter Statistics
- AuthManager Statistics
- Catalog Queries Statistics
- Direct Mailer, List Manager, and Predictor Process CPU Statistics
- Direct Mailer Message, Job, and Error Statistics
- LRUCache Statistics
- Direct Mailer, List Manager, and Predictor Process Memory Statistics
- Pipelines Statistics
- Predictor Statistics
- Profile Object Cache Statistics

AuthFilter Statistics (g_CSAuthFilter.rpt) Commerce Server provides two tools to implement user authentication and identification: the AuthManager object and AuthFilter. AuthFilter is an Internet Server API (ISAPI) filter that is used at the IIS Commerce Server application level.

Counters:

- CS2000/CS2002: User Profile Management.AuthFilter
  - AutoCookies/sec
  - TotalAutoCookies
  - Total Requests Failed

AuthManager Statistics (g_CSAuthManager.rpt) Commerce Server provides two tools to implement user authentication and identification: the AuthManager object and AuthFilter. AuthManager is a COM object that exposes methods for identifying users and controlling access to dynamically generated content.

Counters:

- CS2000/CS2002: User Profile Management.AuthMgr

- AnonTickets/sec
- TotalAnonTickets
- AuthTickets/sec
- TotalAuthTickets
- AuthChecks Failed/sec
- TotalAuthChecks Failed
- AuthChecks Succeeded/sec
- TotalAuthChecks Succeeded
- AuthMgr Objects/sec
- Total AuthMgr Objects Created

Catalog Queries Statistics (g_CSCatalogQueries.rpt) This report shows summary statistics of Commerce Server catalog queries.

Counters:

- CS2000/CS2002: Marketing and Catalog.Catalog: Catalog Queries/sec.

Direct Mailer, List Manager, and Predictor Process CPU Statistics (g_CSCPUSummary.rpt) This report shows summary CPU statistics of Commerce Server processes compared with overall CPU statistics of the system.

Counters:

- Process.% Processor Time (DMLService, listmanager, PredServ)
- Process.Thread Count(DMLService, listmanager, PredServ)
- Processor:% Processor Time

Direct Mailer Message, Job, and Error Statistics (g_CSDirectMailer.rpt) This report examines Commerce Server Direct Mailer usage patterns, including messages sent, occurrence of errors, and jobs running.

Counters:

- CS2000/CS2002: Marketing and Catalog.DML:
  - Direct Mail Errors/sec
  - Direct Mail Jobs Running
  - Mail Messages Sent/sec

- Total Direct Mail Errors
- Total Messages Sent

LRUCache Statistics (g_CSLRUCache.rpt) This report examines Commerce Server Least Recently Used Cache (LRUCache) usage patterns, including flushes per second, hits per second, and misses per second.

- CS2000/CS2002: Marketing and Catalog.LRUCache
  - Cache Size
  - Flushes/sec
  - Hits/sec
  - Misses/sec

Direct Mailer, List Manager, and Predictor Process Memory Statistics (g_CSMemorySummary.rpt) This report shows summary memory statistics of Commerce Server processes.

- Process.Private Bytes (DMLService, listmanager, PredServ)
- Process.Working Set (DMLService, listmanager, PredServ)
- Process.Page Faults/sec (DMLService, listmanager, PredServ)

Pipelines Statistics (g_CSPipelines.rpt) This report examines Commerce Server Pipeline usage patterns, including average execution time, number of executions per second, number of warnings per second, and number of errors per second.

- CS2000/CS2002: Pipelines.Average execution time
- CS2000/CS2002: Pipelines.Errors per second
- CS2000/CS2002: Pipelines.Errors total
- CS2000/CS2002: Pipelines.Executions per second
- CS2000/CS2002: Pipelines.Executions total
- CS2000/CS2002: Pipelines.Warnings per second
- CS2000/CS2002: Pipelines.Warnings total

Predictor Statistics (g_CSPredictor.rpt) This report examines Commerce Server Predictor usage patterns, including average prediction time, analysis model loads, and number of client predictions.

- CS2000/CS2002: Marketing and Catalog.Predictor

- Client Avg Prediction Time
- Client Model Loads From File
- Total Client Model Loads
- Total Client Predictions

Profile Object Cache Statistics (g_CSUPMCache.rpt) This report examines Commerce Server profile object cache usage patterns, including rate of hits, rate of misses, and number of cache purges.

- CS2000/CS2002: User Profile Management.UPM
  - Cache Objects
  - Cache Hit Rate
  - Cache Miss Rate
  - No. of Cache Purges

Related Topics:

- Commerce Server Graphs

Commerce Server graphs

The following predefined graphs for Commerce Server 2000 and 2002 are available with the Microsoft Enterprise Servers SPI:

- AuthFilter Statistics
- AuthManager Anon/Auth Tickets Statistics
- AuthManager Authentication Checks Statistics
- AuthManager Object Statistics
- Catalog Queries/sec
- Direct Mailer CPU
- Direct Mailer Memory
- Direct Mailer Statistics
- List Manager CPU
- List Manager Memory
- LRUCache Statistics
- Pipeline Error and Warning Statistics
- Pipeline Execution Statistics
- Predictor CPU
- Predictor Memory
- Predictor Statistics
- Profile Object Cache Statistics

AuthFilter Statistics This graph shows summary statistics relating to the Commerce Server AuthFilter.

AuthManager Anon/Auth Tickets Statistics This graph shows summary statistics relating to Commerce Server AuthManager, and the number of anonymous and authenticated tickets.

AuthManager Authentication Checks Statistics This graph shows summary statistics relating to Commerce Server AuthManager, and the number of successful and failed authentication checks.

AuthManager Object Statistics This graph shows summary statistics relating to Commerce Server AuthManager, and the number of Authentication Manager objects created.

Catalog Queries/sec This graph shows summary statistics of Commerce Server catalog queries.

Direct Mailer CPU This graph shows summary CPU statistics of the Commerce Server Direct Mailer process.

Direct Mailer Memory This graph shows summary memory statistics of the Commerce Server Direct Mailer process.

Direct Mailer Statistics This graph examines Commerce Server Direct Mailer usage patterns, including messages sent, and occurrence of errors.

List Manager CPU This graph shows summary CPU statistics of the Commerce Server List Manager process.

List Manager Memory This graph shows summary memory statistics of the Commerce Server List Manager process.

LRUCache Statistics This graph examines Commerce Server Least Recently Used Cache (LRUCache) usage patterns, including flushes per second, hits per second, and misses per second.

Pipeline Error and Warning Statistics This graph examines Commerce Server Pipeline usage patterns, including number of warnings per second, and number of errors per second.

Pipeline Execution Statistics This graph examines Commerce Server Pipeline usage patterns, including average execution time, and number of executions per second.

Predictor CPU This graph shows summary CPU statistics of the Commerce Server Predictor process.

Predictor Memory This graph shows summary memory statistics of the Commerce Server Predictor process.

Predictor Statistics This graph examines Commerce Server Predictor usage patterns, including average prediction time.

Profile Object Cache Statistics This graph examines Commerce Server profile object cache usage patterns, including rate of hits, and rate of misses.

Related Topics:

- Commerce Server Reports

Commerce Server troubleshooting

This section covers troubleshooting tips for Commerce Server.

Initialization of Policies Failed

Occasionally a warning occurs in the Message Browser stating that the initialization of policies has failed. This happens when the Commerce Server performance counters are not available and you are using the policy NET_CommerceServer_Logging.

Error messages appear as follows:

```
Initialization of policy NET_CommerceServer_Logging failed. (OpC30-727)
```

```
Initialization of Real Time Performance Measurement source MarketingAndCatalog.Catalog
Queries/sec failed. (OpC30-725)
```

Solution

Re-register the DLL files so that logging can continue.

For more information, refer to Microsoft's support web site. Enter the Knowledge Base Article Number Q277211.

Related Topics:

- Troubleshooting Microsoft Enterprise Servers

Content Management Server

Microsoft's Content Management Server (CMS) is the packaged tool-set to support frequently updated web sites. Using CMS, organizations can run a dynamic updated web site without the day to day care of IT personnel. Content providers such as authors, editors, and site content managers, can simply update content automatically through web browsers without the involvement of a web master, IT or other technical staff. CMS is built on the Microsoft Windows 2000 operating system, IIS and SQL server (7.0 and 2000).

The Microsoft Enterprise Servers SPI covers both Content Management Server 2001 and 2002 versions. CMS 2002 offers improved features for web site developers, in particular due to its application specific performance counters, which enable improved Microsoft Enterprise Servers SPI graphs and reports. In the following list, items labeled **For CMS 2002 only** depend on these performance counters and are only available for Content Management Server 2002 and later versions.

The following policies are available to monitor Content Management Servers:

- **Content Management Server - NT Service Check:** this policy checks to see if the service is running, if it is not and the service in startup is set to "Auto Start", then an attempt is made to restart the service. A console error message is sent to indicate that the service is not running.
- **Service Map Dependencies on IIS, SQL Server and Windows OS:** shows the dependencies on components monitored by other SPIs (Windows OS, Microsoft SQL Server) to reflect the overall availability of the environment.
- Policies that notify on all **Error, Warning, Information Entries in the Windows 2000 Event Log** .
- Policies to check Process.Page Faults/sec, Process.%Processor Time, and Process.Working Set for the **Active Enterprise Security Service** .
- The Content Management Server **logging policy** serves as a dummy policy to distinguish CMS computers from other computers, it logs the Process.%Processor Time for instance AESecurityServi.

The following reports are available:

- **Active Enterprise Security Service CPU Statistics** (g_CMSCPUSummary.rpt) : This report shows summary CPU statistics of the Active Enterprise Security process compared with overall CPU statistics of the system, in graphical and tabular format. The summarized process statistics include the percentage of CPU time used by the document manager compared with the percentage of time the system's CPU was busy.
- **Active Enterprise Security Service Memory Statistics** (g_CMSMemorySummary.rpt) : This report

shows summary memory statistics of the Access Entity Security process, in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the document manager.

- **Active Enterprise Node Count Monthly Statistics (For CMS 2002 only)** (g_CmsAENodesMonthly.rpt): This report shows summary Active Enterprise Nodes count monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters.Active Enterprise Node objects (_Total) for the last 30 days.
- **Active Enterprise Node Count Weekly Statistics (For CMS 2002 only)** (g_CmsAENodesWeekly.rpt): This report shows summary Active Enterprise Nodes count monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show the average hourly value of the counter: CMS Performance Counters.AE Node objects (_Total) for the last 7 days.
- **Master Cache Hits and Misses Rate Monthly Statistics (For CMS 2002 only)** (g_CmsCacheHitMissRateMonthly.rpt): This report shows summary Cache hits/sec and Cache misses/sec monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. Cache hits/sec (_Total) and CMS Performance Counters. Cache misses/sec (_Total) for the last 30 days.
- **Master Cache Hits and Misses Rate Weekly Statistics (For CMS 2002 only)** (g_CmsCacheHitMissRateMWeekly.rpt): This report shows summary Cache hits/sec and Cache misses/sec weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. Cache hits/sec (_Total) and CMS Performance Counters. Cache misses/sec (_Total) for the last 7 days.
- **Cache Nodes count Monthly Statistics (For CMS 2002 only)** (g_CmsCacheNodesMonthly.rpt): This report shows summary Master cache nodes and Shared nodes monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. Master cache nodes (_Total) and CMS Performance Counters. Shared nodes (_Total) for the last 30 days.
- **Cache Nodes count Weekly Statistics (For CMS 2002 only)** (g_CmsCacheNodesWeekly.rpt): This report shows summary Master cache nodes and Shared nodes weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. Master cache nodes (_Total) and CMS Performance Counters. Shared nodes (_Total) for the last 7 days.
- **CMS Connection Rate Monthly Statistics (For CMS 2002 only)** (g_CmsConnectionCreationRateMonthly.rpt): This report shows summary CMS connections/sec monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. CMS connections/sec (_Total) for the last 30 days.

- **CMS Connection Rate Weekly Statistics (For CMS 2002 only)** (g_CmsConnectionCreationRateWeekly.rpt): This report shows summary CMS connections/sec weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. CMS connections/sec (_Total) for the last 7 days.
- **Data Access Operation rates Monthly Statistics (For CMS 2002 only)** (g_CmsDataAccessOperationRateMonthly.rpt): This report shows summary Data access operations/sec monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. Data access operations/sec (_Total) for the last 30 days.
- **Data Access Operation rates Weekly Statistics (For CMS 2002 only)** (g_CmsDataAccessOperationRateWeekly.rpt): This report shows summary Data access operations/sec weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. Data access operations/sec (_Total) for the last 7 days.
- **Server Exception Thrown Monthly Statistics (For CMS 2002 only)** (g_CmsExceptionThrownMonthly.rpt): This report shows summary Exceptions thrown monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. Exceptions thrown (_Total) for the last 30 days.
- **Server Exception Thrown Weekly Statistics (For CMS 2002 only)** (g_CmsExceptionThrownWeekly.rpt): This report shows summary Exceptions thrown weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. Exceptions thrown (_Total) for the last 7 days.
- **Shared Node Creation Rate Monthly Statistics (For CMS 2002 only)** (g_CmsSharedNodeCreationRateMonthly.rpt): This report shows summary Shared nodes/sec monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. Shared nodes/sec (_Total) for the last 30 days.
- **Shared Node Creation Rate Weekly Statistics (For CMS 2002 only)** (g_CmsSharedNodeCreationRateWeekly.rpt): This report shows summary Shared nodes/sec Weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. Shared nodes/sec (_Total) for the last 7 days.

The following graphs are available:

- **AESecurityService CPU** : This graph shows summary CPU statistics of the Active Enterprise Security process. This data can be compared with System Processor Time to determine to what extent the Active Enterprise Security process is utilizing processor time.
- **AESecurityService Memory** : This graph shows summary memory statistics of the Active Enterprise Security process. The summarized process statistics include the page faults per second, private bytes, and working set used by the process.
- **User Sessions (For CMS 2002 only):** This graph shows summary statistics for different type of user sessions. The summarized user session statistics include Authenticated Sessions, Guest Sessions, and Edit Sessions.
- **Authenticated Session Creation Rate (For CMS 2002 only):** This graph shows summary statistics for new user logon rate.
- **CMS Connections (For CMS 2002 only):** This graph shows summary statistics for CMS Connections Trend.
- **Cache Nodes Count (For CMS 2002 only):** This graph shows summary statistics for changes in CMS cache nodes count.
- **Shared Nodes Creation Rate (For CMS 2002 only):** This graph shows summary statistics for shared nodes creation rate.
- **AE Node Objects Count (For CMS 2002 only):** This graph shows summary statistics for number of active enterprise COM objects in the server.
- **AE Node Object Creation Rate (For CMS 2002 only):** This graph shows summary statistics for AE node object creation rate.
- **Exception Thrown (For CMS 2002 only):** This graph shows summary statistics for number of exceptions thrown by the server.
- **Cache Hit and Miss Rate (For CMS 2002 only):** This graph shows summary statistics for CMS internal cache hits and misses rate.

Related Topics:

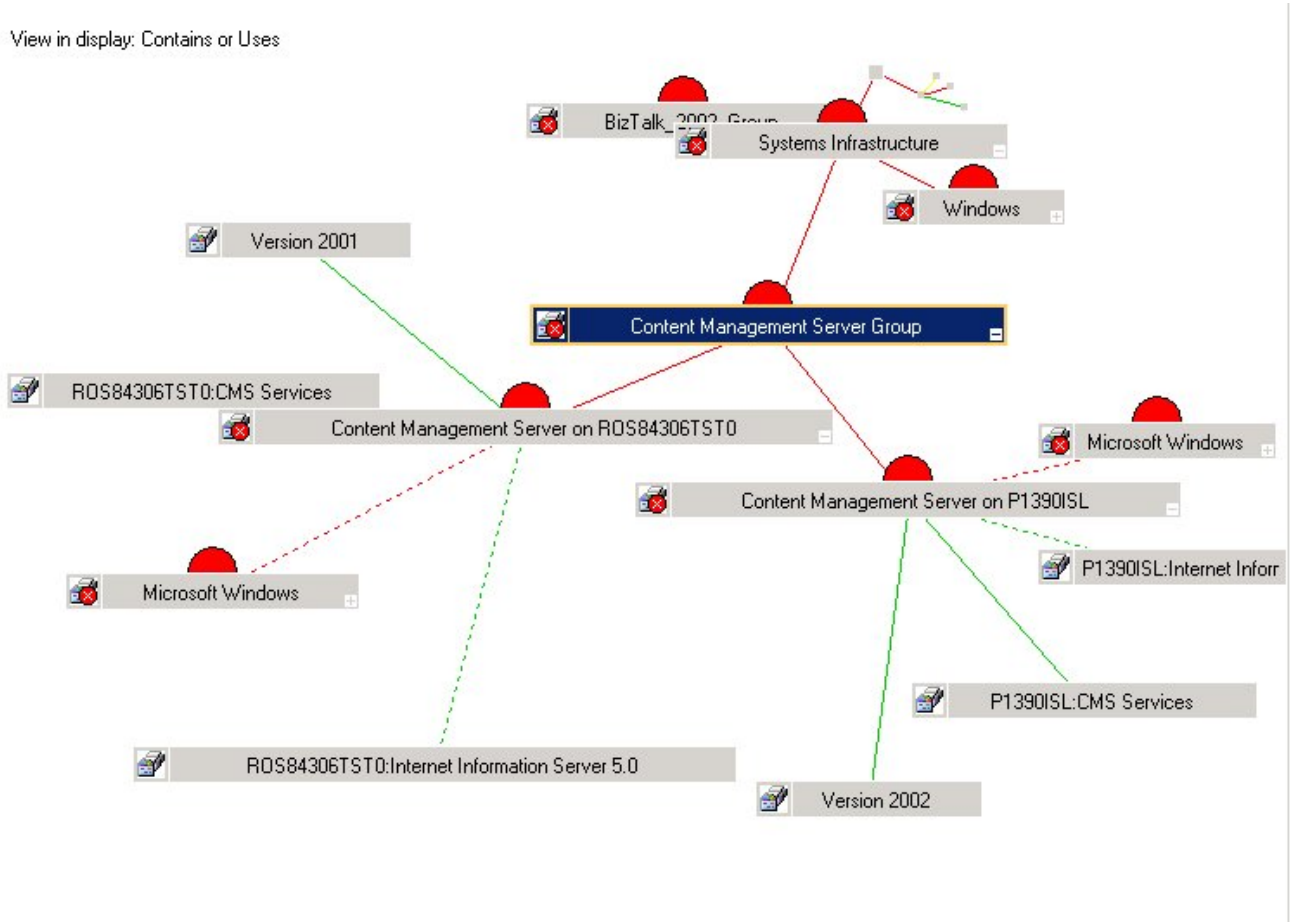
- Content Management Server Policies
- Content Management Server Reports
- Content Management Server Graphs
- Content Management Server Service Map

Content Management Server service map

The Content Management Server service map displays the nodes where Content Management Servers have been installed.

Systems Infrastructure

The service map shows the Content Manager Server services, their dependent SQL servers, IIS, and Windows 2000 servers.



Related Topics:

- Creating Service Maps for Microsoft Enterprise Servers

Content Management Server policies

The Microsoft Enterprise Servers SPI covers both MSCMS (Microsoft Content Management Server) 2001 and MSCMS 2002 versions. MSCMS 2002 offers improved features for web site developers, in particular due to MSCMS specific performance counters, which also enable improved Microsoft Enterprise Servers SPI graphs and reports. In the following list, policies labeled **For CMS 2002 only** depend on these performance counters and are only available for Content Management Server 2002 and later versions.

Availability Monitoring

Policy Description

NET_CMSServices

Description: This policy monitors the Active Enterprise Security Service (AESecurityService.exe). If a service stops an attempt is made to restart the service and an error message is sent to the console.

Server Logging

Policy Descriptions

NET_CMS_Logging

Description: This policy serves as a dummy policy to distinguish CMS computers from other computers. It logs the Process.% Processor Time for instance AESecurityServi.

NET_CMS_PerfRate_Logging (For CMS 2002 only)

Description: This policy logs the following counters: Authenticated sessions/sec; AE Node objects/sec; Cache hits/sec; Cache misses/sec; CMS connections/sec; Data access operations/sec; Shared nodes/sec.

NET_CMS_PerfStatus_Logging (For CMS 2002 only)

Description: This policy logs the following counters: AE Node objects; Authenticated sessions; Edit sessions; Exceptions thrown; Guest sessions; Master cache nodes; Number of CMS connections; Shared nodes.

Windows Event Log Monitoring

Policy Descriptions

NET_CMSFwdApplicationError

Description: Forwards all Content Management Server application entries with severity 'Error' that are logged to the Windows 2000 Event Log.

NET_CMSFwdApplicationWarning

Description: Forwards all Content Management Server application entries with severity 'Warning' that are logged to the Windows 2000 Event Log.

NET_CMSFwdApplicationInfo

Description: Forwards all Content Management Server application entries with severity 'Information' that are logged to the Windows 2000 Event Log.

Performance Monitoring

Policy Descriptions

NET_CMS-PageFaultssec-AESecurityService

Description: Checks Process.Page Faults/sec for the Active Enterprise Security Service.

NET_CMS-ProcessorTime-AESecurityService

Description: Checks Process.% Processor Time for the Active Enterprise Security Service.

NET_CMS-WorkingSet-AESecurityService

Description: Checks Process. Working Set for the Active Enterprise Security Service.

NET_CMS-CmsConnectionsPerSec (For CMS 2002 only)

Description: This policy checks counter [CMS Performance Counters.CMS connections/sec] for the instance_Total. The counter shows the number of open CMS application connections/sec.

NET_CMS-DataAccessOpsPersec (For CMS 2002 only)

Description: This policy checks counter [CMS Performance Counters.Data access operations/sec] for the instance_Total. The counter shows the number of data access operations executed per second.

NET_CMS-MasterCacheMissesPerSec (For CMS 2002 only)

Description: This policy checks counter [CMS Performance Counters. Cache misses/sec] for the instance_Total. The counter shows the rate of cache misses on the master cache.

NET_CMS-MasterCacheNodes (For CMS 2002 only)

Description: This policy checks counter [CMS Performance Counters. Master cache nodes] for the instance_Total. The counter shows the number of items in the internal CMS master cache.

NET_CMS-SharedNodes (For CMS 2002 only)

Description: This policy checks counter [CMS Performance Counters.Shared nodes] for the instance_Total. The counter shows the number of items/nodes referenced by the server (includes master cache items).

Discovery

Policy Descriptions

NET_ContentMgmtSvr_Discovery

Description: This policy discovers the Content Manager Server services, its dependent SQL server, IIS, and Windows 2000 server.

NET_CMS_ForwardDiscoveryError

Description: This Log File policy is deployed every time the discovery policy is deployed, to track and report to the management console all discovery errors logged to the Javaagent.log.

Related Topics:

- Deploying Policies for Microsoft Enterprise Servers
- Content Management Server Overview

Content Management Server reports

The Microsoft Enterprise Servers SPI covers both MSCMS (Microsoft Content Management Server) 2001 and MSCMS 2002 versions. MSCMS 2002 offers improved features for web site developers, in particular due to MSCMS specific performance counters, which also enable improved Microsoft Enterprise Servers SPI graphs and reports. In the following list, reports labeled **For CMS 2002 only** depend on these performance counters and are only available for Content Management Server 2002 and later versions.

The following predefined reports for Content Management Servers are available with the Microsoft Enterprise Servers SPI:

Active Enterprise Security Service CPU Statistics (g_CMSCPUSummary.rpt)

This report shows summary CPU statistics of the Active Enterprise Security process compared with overall CPU statistics of the system, in graphical and tabular format. The summarized process statistics include the percentage of CPU time used by the document manager compared with the percentage of time the system's CPU was busy.

Counters:

- Process.% Processor Time (AESecurityServi)
- Process.Thread Count (AESecurityServi)
- Processor.% Processor Time

Active Enterprise Security Service Memory Statistics (g_CMSMemorySummary.rpt)

This report shows summary memory statistics of the Active Enterprise Security process, in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the document manager.

Counters:

- Process.Private Bytes (AESecurityServi)
- Process.Working Set (AESecurityServi)
- Process.Page Faults/sec (AESecurityServi)

Active Enterprise Node Count Monthly Statistics (For CMS 2002 only) (g_CmsAENodesMonthly.rpt)

This report shows summary Active Enterprise Nodes count monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the

counter: CMS Performance Counters.Active Enterprise Node objects (_Total) for the last 30 days.

Active Enterprise Node Count Weekly Statistics (For CMS 2002 only) (g_CmsAENodesWeekly.rpt)

This report shows summary Active Enterprise Nodes count monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show the average hourly value of the counter: CMS Performance Counters.AE Node objects (_Total) for the last 7 days.

Master Cache Hits and Misses Rate Monthly Statistics (For CMS 2002 only)
(g_CmsCacheHitMissRateMonthly.rpt)

This report shows summary Cache hits/sec and Cache misses/sec monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. Cache hits/sec (_Total) and CMS Performance Counters. Cache misses/sec (_Total) for the last 30 days.

Master Cache Hits and Misses Rate Weekly Statistics (For CMS 2002 only)
(g_CmsCacheHitMissRateMWeekly.rpt)

This report shows summary Cache hits/sec and Cache misses/sec weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. Cache hits/sec (_Total) and CMS Performance Counters. Cache misses/sec (_Total) for the last 7 days.

Cache Nodes count Monthly Statistics (For CMS 2002 only) (g_CmsCacheNodesMonthly.rpt)

This report shows summary Master cache nodes and Shared nodes monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. Master cache nodes (_Total) and CMS Performance Counters. Shared nodes (_Total) for the last 30 days.

Cache Nodes count Weekly Statistics (For CMS 2002 only) (g_CmsCacheNodesWeekly.rpt)

This report shows summary Master cache nodes and Shared nodes weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. Master cache nodes (_Total) and CMS Performance Counters. Shared nodes (_Total) for the last 7 days.

CMS Connection Rate Monthly Statistics (For CMS 2002 only)
g_CmsConnectionCreationRateMonthly.rpt)

This report shows summary CMS connections/sec monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. CMS connections/sec (_Total) for the last 30 days.

CMS Connection Rate Weekly Statistics (For CMS 2002 only)
(g_CmsConnectionCreationRateWeekly.rpt)

This report shows summary CMS connections/sec weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. CMS connections/sec (_Total) for the last 7 days.

Data Access Operation Rates Monthly Statistics (For CMS 2002 only)
(g_CmsDataAccessOperationRateMonthly.rpt)

This report shows summary Data access operations/sec monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. Data access operations/sec (_Total) for the last 30 days.

Data Access Operation rates Weekly Statistics (For CMS 2002 only)
g_CmsDataAccessOperationRateWeekly.rpt)

This report shows summary Data access operations/sec weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. Data access operations/sec (_Total) for the last 7 days.

Server Exception Thrown Monthly Statistics (For CMS 2002 only)
(g_CmsExceptionThrownMonthly.rpt)

This report shows summary Exceptions thrown monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. Exceptions thrown (_Total) for the last 30 days.

Server Exception Thrown Weekly Statistics (For CMS 2002 only)
(g_CmsExceptionThrownWeekly.rpt)

This report shows summary Exceptions thrown weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. Exceptions thrown (_Total) for the last 7 days.

Shared Node Creation Rate Monthly Statistics (For CMS 2002 only)
(g_CmsSharedNodeCreationRateMonthly.rpt)

This report shows summary Shared nodes/sec monthly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average daily value of the counter: CMS Performance Counters. Shared nodes/sec (_Total) for the last 30 days.

Shared Node Creation Rate Weekly Statistics (For CMS 2002 only)
(g_CmsSharedNodeCreationRateWeekly.rpt)

This report shows summary Shared nodes/sec Weekly statistics of Content Management Server, in graphical and tabular format. The summarized statistics show average hourly value of the counter: CMS Performance Counters. Shared nodes/sec (_Total) for the last 7 days.

Related Topics:

- Content Management Server Graphs

Content Management Server graphs

The Microsoft Enterprise Servers SPI covers both Microsoft CMS 2001 and 2002 versions. Content Management Server 2002 offers improved features for web site developers due to Content Management Server specific performance counters, which enable improved Microsoft Enterprise Servers SPI graphs and reports. In the following list, graphs labeled **For CMS 2002 only** depend on these performance counters and are only available for Content Management Server 2002 and later versions.

The following predefined graphs for the Content Management Server are available with the Microsoft Enterprise Servers SPI:

AESecurityService CPU : This graph shows summary CPU statistics of the Active Enterprise Security process. This data can be compared with System Processor Time to determine to what extent the Active Enterprise Security process is utilizing processor time.

Counters: Process.% Processor Time (AESecurityService).

AESecurityService Memory : This graph shows summary memory statistics of the Active Enterprise Security process. The summarized process statistics include the page faults per second, private bytes, and working set used by the process.

Counters: Process.Private Bytes (AESecurityService), Process.Working Set (AESecurityService), Process.Page Faults/sec (AESecurityService).

User Sessions (For CMS 2002 only): This graph shows summary statistics for different type of user sessions. The summarized user session statistics include Authenticated Sessions, Guest Sessions, and Edit Sessions.

Counters: CMS Performance Counters.Authenticated Sessions(_Total), CMS Performance Counters. Guest Sessions (_Total) and CMS Performance Counters. Edit Sessions (_Total).

Authenticated Session Creation Rate (For CMS 2002 only): This graph shows summary statistics for new user logon rate.

Counters: CMS Performance Counters. Authenticated Session/sec (_Total).

CMS Connections (For CMS 2002 only): This graph shows summary statistics for CMS Connections Trend.

Counters: CMS Performance Counters. Number CMS Connections (_Total).

CMS Connections Creation Rate (For CMS 2002 only): This graph shows summary statistics for CMS Connections opened per second.

Counters: CMS Performance Counters. CMS Connections/sec (_Total).

Cache Nodes Count (For CMS 2002 only): This graph shows summary statistics for changes in CMS cache nodes count.

Counters: CMS Performance Counters. Master Cache Nodes (_Total) and CMS Performance Counters. Shared Nodes (_Total).

Shared Nodes Creation Rate (For CMS 2002 only): This graph shows summary statistics for shared nodes creation rate.

Counters: CMS Performance Counters. Shared Nodes/sec (_Total).

AE Node Objects Count (For CMS 2002 only): This graph shows summary statistics for number of active enterprise COM objects in the server.

Counters: CMS Performance Counters. AE Node Objects (_Total).

AE Node Object Creation Rate (For CMS 2002 only) : This graph shows summary statistics for AE node object creation rate.

Counters: CMS Performance Counters AE Node Object/sec (_Total).

Exception Thrown (For CMS 2002 only): This graph shows summary statistics for number of exceptions thrown by the server.

Counters: CMS Performance Counters. Exception Thrown (_Total).

Cache Hit and Miss Rate (For CMS 2002 only): This graph shows summary statistics for CMS internal cache hits and misses rate.

Counters: CMS Performance Counters. Cache Hits/sec (_Total) and CMS Performance Counters. Cache Misses/sec(_Total). Content Management Server Discovery and Service Map

Related Topics:

- Content Management Server Reports

Internet Security and Acceleration Server

Microsoft's Internet Security and Acceleration (ISA) Server is a tool that integrates security (firewall) with acceleration (Web proxy cached pages.) This secures your site and speeds up Web access.

Availability Monitoring

ISA Server services are monitored to determine whether they are up or down. Services are not automatically restarted, because they may have been shut down intentionally.

Monitored ISA 2000 services include:

- Microsoft Firewall (wspsrv)
- Microsoft Web Proxy (w3proxy)
- Microsoft ISA Server Control (mspadmin)
- Microsoft Scheduled Cache Content Download (w3prefch)

Monitored ISA 2006 services include:

- Microsoft Firewall (wspsrv)
- Microsoft ISA Server Control (mspadmin)
- Microsoft ISA Server Job Scheduler (w3prefch)
- Routing and Remote Access (svchost)
- Network Load Balancing
- Microsoft Data Engine (sqlservr)
- Microsoft ISA Server Storage (isastg)
- Firewall Engine
- ISA Storage Configuration (dsadmin)

Event Monitoring

Event monitoring of the Windows 2000/2003 Event Log (application log) occurs for ISA Server events. Console messages are sent for all errors, warnings, and information events logged for the following

sources:

- Microsoft Firewall
- Microsoft Web Proxy
- Microsoft ISA Server Control
- Microsoft Scheduled Cache Content Download

Performance Monitoring

ISA performance monitoring includes both specific ISA Server performance counters and CPU process-related counters. Each policy for performance monitoring has both error and warning thresholds.

Server Logging

Selected process-related data for CPU and memory counters is logged for the ISA Server.

> **NOTE:**
> For Server Logging, deployment of the Windows OS SPI logging policy, WINOSSPI-WINOS_Win2k_Logging, is required to log process-related data for CPU and memory counters. The counters specific to the Internet Security and Acceleration Server are documented in the policy section. Refer to the Windows OS SPI Policies for information about the process-related data for CPU and memory counters.

Related Topics:

- Internet Security and Acceleration Server 2000 policies
- Internet Security and Acceleration Server 2006 policies
- Internet Security and Acceleration Server reports
- Internet Security and Acceleration Server graphs
- Internet Security and Acceleration Server Service Map

Internet Security and Acceleration Server service map

The Internet Security and Acceleration Server service map displays the nodes where Internet Security and Acceleration Servers have been installed. The service maps are available under both the Applications and the Systems Infrastructure areas.

Applications

The service map has two levels. One is the root node for all ISA Server installations within the enterprise. The other is a node corresponding to each main component of the ISA Server. These components of ISA 2000 are:

- Firewall
- Web Proxy
- Scheduled Content Download
- ISA Server Control

These components of ISA 2006 include:

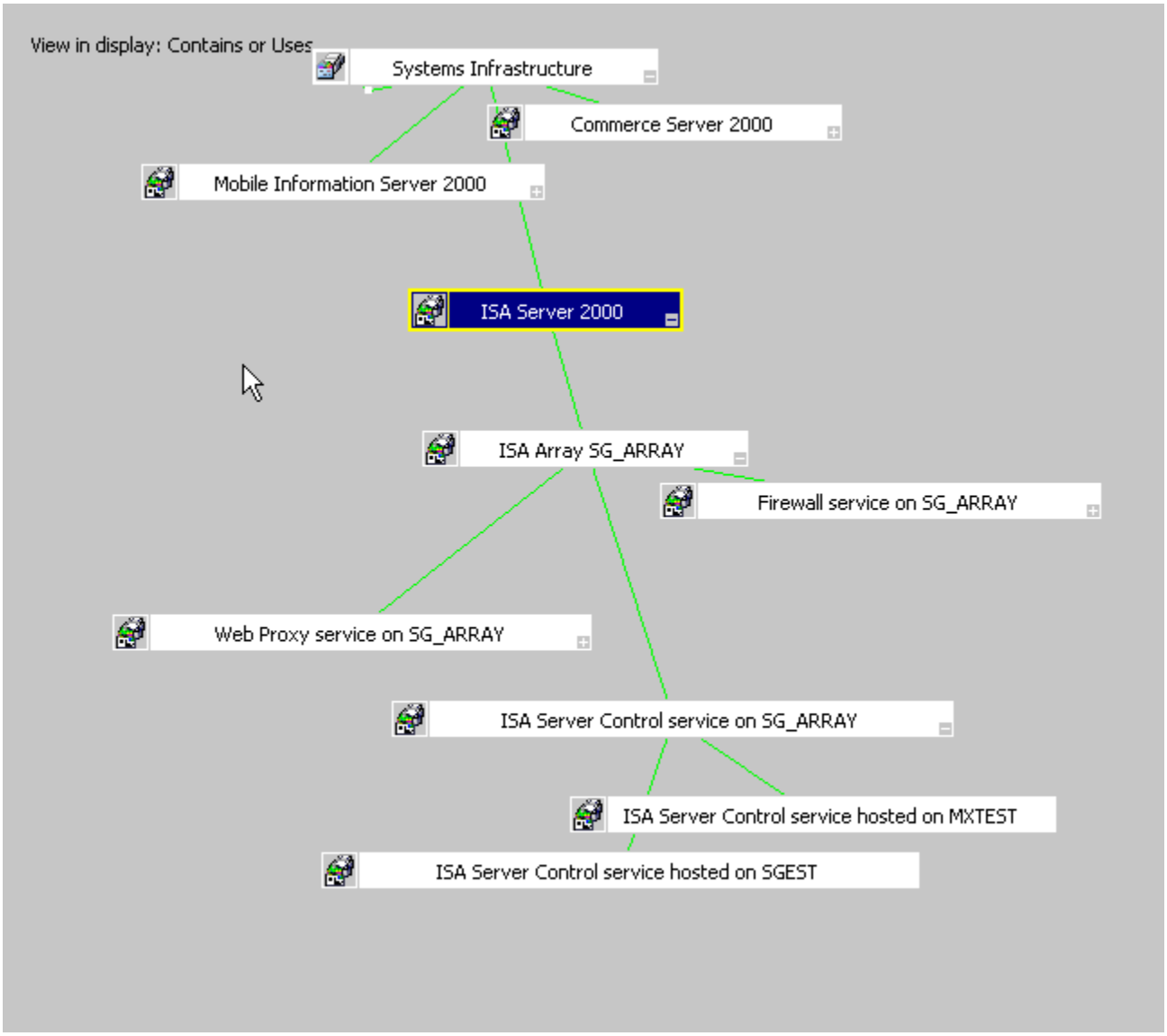
- Microsoft Firewall (wspsrv)
- Microsoft ISA Server Control (mspadmin)
- Microsoft ISA Server Job Scheduler (w3prefch)
- Routing and Remote Access (svchost)
- Network Load Balancing
- Microsoft Data Engine (sqlservr)
- Microsoft ISA Server Storage (isastg)
- Firewall Engine
- ISA Storage Configuration (dsadmin)

Systems Infrastructure

The Systems Infrastructure service map has four levels:

- The root node for all ISA Server installations within the enterprise
- A node corresponding to each ISA server array (standalone server array or enterprise array) that has been setup within the enterprise
- A node corresponding to each of the main services comprising the respective ISA Server array installation.
- A node corresponding to each system within the respective server array that is hosting one of the ISA Server services. The nodes at this level are represented by the caption "Firewall service hosted on *system* " where system is the name of a system within the ISA server array running the firewall service

The following graphic shows an example ISA Server 2000 Systems Infrastructure map.



Related Topics:

- Creating Service Maps for Microsoft Enterprise Servers

Internet Security and Acceleration Server 2000 policies

See the policies for monitoring ISA 2000 under the following categories:

- Availability Monitoring
- Windows Event Log Monitoring
- Performance Monitoring
- Server Logging
- Discovery

See ISA 2006 policies for a complete listing of ISA 2000 policies.

Availability Monitoring

NET_ISAServerServices

Description: This policy monitors the ISA Server services: Firewall, Web Proxy, Scheduled Cache Content Download, ISA Server Control. If a service is stopped it is not restarted automatically, due to possible shutdown resulting from intrusion detection.

Windows Event Log Monitoring

NET_ISAServerFwdApplicationError

Description: Forwards all ISA Server application log entries with severity 'Error'

NET_ISAServerFwdApplicationInformation

Description: Forwards all ISA Server application log entries with severity 'Information'

NET_ISAServerFwdApplicationWarning

Description: Forwards all ISA Server application log entries with severity 'Warning'

Performance Monitoring

NET_ISA-CacheHitRatio

Description: Checks the percentage of Web proxy client requests that have been served using cached data, out of the total number of Web proxy client requests to the ISA Server.

NET_ISA-CacheRunningHitRatio

Description: Checks the percentage of Web proxy client requests that have been served using cached data out of the total number of Web proxy client requests to the ISA Server, for the last 10,000 requests serviced.

NET_ISA-DiskFailureRatesec

Description: Checks the number of I/O failures per second to the disk cache.

NET_ISA-FailingRequestssec

Description: Checks the rate per second that Web proxy client requests have failed with some type of error.

NET_ISA-PageFaultssec-Firewall

Description: Checks Process.Page Faults/sec for the ISA Server 2000 Firewall service.

NET_ISA-PageFaultssec-ISAServerControl

Description: Checks Process.Page Faults/sec for the ISA Server 2000 ISA Server Control service.

NET_ISA-PageFaultssec-ScheduledCacheContentDownload

Description: Checks Process.Page Faults/sec for the ISA Server 2000 Scheduled Cache Content Download service.

NET_ISA-PageFaultssec-WebProxy

Description: Checks Process.Page Faults/sec for the ISA Server 2000 Web Proxy service.

NET_ISA-PrivateBytes-Firewall

Description: Checks Process.Private Bytes for the ISA Server 2000 Firewall service.

NET_ISA-PrivateBytes-ISAServerControl

Description: Checks Process.Private Bytes for the ISA Server 2000 ISA Server Control service.

NET_ISA-PrivateBytes-ScheduledCacheContentDownload

Description: Checks Process.Private Bytes for the ISA Server 2000 Scheduled Cache Content Download service.

NET_ISA-PrivateBytes-WebProxy

Description: Checks Process.Private Bytes for the ISA Server 2000 Web Proxy process.

NET_ISA-ProcessorTime-Firewall

Description: Checks Process.% Processor Time for the ISA Server 2000 Firewall service.

NET_ISA-ProcessorTime-ISAServerControl

Description: Checks Process.% Processor Time for the ISA Server 2000 ISA Server Control service.

NET_ISA-ProcessorTime-ScheduledCacheContentDownload

Description: Checks Process.% Processor Time for the ISA Server 2000 Scheduled Cache Content Download service.

NET_ISA-ProcessorTime-WebProxy

Description: Checks Process.% Processor Time for the ISA Server 2000 Web Proxy service.

NET_ISA-ThreadCount-Firewall

Description: Checks Process.Thread Count for the ISA Server 2000 Firewall service.

NET_ISA-ThreadCount-ISAServerControl

Description: Checks Process.Thread Count for the ISA Server 2000 ISA Server Control service.

NET_ISA-ThreadCount-ScheduledCacheContentDownload

Description: Checks Process.Thread Count for the ISA Server 2000 Scheduled Cache Content Download service.

NET_ISA-ThreadCount-WebProxy

Description: Checks Process.Thread Count for the ISA Server 2000 Web Proxy service.

NET_ISA-WorkingSet-Firewall

Description: Checks Process.Working Set for the ISA Server 2000 Firewall service.

NET_ISA-WorkingSet-ISAServerControl

Description: Checks Process.Working Set for the ISA Server 2000 ISA Server Control service.

NET_ISA-WorkingSet-ScheduledCacheContentDownload

Description: Checks Process.Working Set for the ISA Server 2000 Scheduled Cache Content Download service.

Server Logging

NET_ISAServer_Logging

Description: This policy logs selected performance data for the ISA Server using the following counters. Deployment of Windows OS SPI logging policy WINOSSPI-WINOS_Win2k_Logging is required to log process-related data for CPU and memory counters.

Discovery

NET_ISAServer_Discovery_System

Description: This policy discovers and adds the infrastructure information to the service map.

NET_ISAServer_Discovery_Application

Description: This policy discovers and adds the application information to the service map. It also adds the dependency information to the service map.

Related Topics:

- ISA 2006 policies
- Deploying Policies for Microsoft Enterprise Servers
- Internet Security and Acceleration Server Overview

Internet Security and Acceleration Server 2006 policies

See the policies for monitoring ISA 2006 under the following categories:

- Availability Monitoring
- Windows Event Log Monitoring
- Performance Monitoring
- Server Logging
- Discovery

See ISA 2000 policies for a complete listing of ISA 2000 policies.

Availability Monitoring

ISA2006_Availability_Config-storage-service

Description: This policy checks if ISA Configuration Storage Server service is running, if not, it tries to restart the service.

ISA2006_Availability_DataEngine-Service

Description: This policy checks if ISA Data Engine service is running, if not, it tries to restart the service.

ISA2006_Availability_Firewall-Engine-Service

Description: This policy checks if ISA Firewall Engine service is running, if not, it tries to restart the service.

ISA2006_Availability_Firewall-Service

Description: This policy checks if ISA Server Control service is running, if not, it tries to restart the service.

ISA2006_Availability_JobScheduler-Service

Description: This policy checks if ISA Job Scheduler service is running, if not, it tries to restart the service.

ISA2006_Availability_Network-Load-Balancing-Service

Description: This policy checks if ISA Network Load Balancing service is running, if not, it tries to restart the service.

ISA2006_Availability_RemoteAccess-Service

Description: This policy checks if ISA Routing and Remote Access service is running, if not, it tries to restart the service.

ISA2006_Availability_ServerControl-Service

Description: This policy checks if ISA Job Scheduler service is running, if not, it tries to restart the service.

ISA2006_Availability_Storage-Service

Description: This policy checks if ISA Server Storage service is running, if not, it tries to restart the service.

Windows Event Log Monitoring

ISA2006_FwdApplicationError

Description: Forwards all ISA Server application log entries with severity 'Error'

ISA2006_FwdApplicationInformation

Description: Forwards all ISA Server application log entries with severity 'Information'

ISA2006_FwdApplicationWarning

Description: Forwards all ISA Server application log entries with severity 'Warning'

Performance Monitoring

Service based performance monitoring policies are located in the following folders:

- Firewall Service
- Firewall Engine
- Job Scheduler
- Network Load Balancing
- Microsoft Data Engine
- Remote Access
- Server Control
- Server Storage
- Storage Configuration

Firewall Service

ISA2006_Firewall_PageFaults

Description: Monitors Page Faults of Firewall process.

ISA2006_Firewall_PrivateBytes

Description: Monitors Private Bytes of Firewall process.

ISA2006_Firewall_ProcessorTime

Description: Monitors Processor Time of Firewall process.

ISA2006_Firewall_ThreadCount

Description: Monitors Thread Count of Firewall process.

ISA2006_Firewall_WorkingSet

Description: Monitors Working Set of Firewall process.

Firewall Engine

ISA2006_FirewallEngine_PageFaults

Description: Monitors Page Faults of Firewall Engine.

ISA2006_FirewallEngine_PrivateBytes

Description: Monitors Private Bytes of Firewall Engine.

ISA2006_FirewallEngine_ProcessorTime

Description: Monitors Processor Time of Firewall Engine.

ISA2006_FirewallEngine_ThreadCount

Description: Monitors Thread Count of Firewall Engine.

ISA2006_FirewallEngine_WorkingSet

Description: Monitors Working Set of Firewall Engine.

Job Scheduler

ISA2006_JobScheduler_PageFaults

Description: Monitors Page Faults of Job Scheduler process.

ISA2006_JobScheduler_PrivateBytes

Description: Monitors Private Bytes of Job Scheduler process.

ISA2006_JobScheduler_ProcessorTime

Description: Monitors Processor Time of Job Scheduler process.

ISA2006_JobScheduler_ThreadCount

Description: Monitors Thread Count of Job Scheduler process.

ISA2006_JobScheduler_WorkingSet

Description: Monitors Working Set of Job Scheduler process.

Network Load Balancing

ISA2006_LoadBalancing_PageFaults

Description: Monitors Page Faults of Load Balancing process.

ISA2006_LoadBalancing_PrivateBytes

Description: Monitors Private Bytes of Load Balancing process.

ISA2006_LoadBalancing_ProcessorTime

Description: Monitors Processor Time of Load Balancing process.

ISA2006_LoadBalancing_ThreadCount

Description: Monitors Thread Count of Load Balancing process.

ISA2006_LoadBalancing_WorkingSet

Description: Monitors Working Set of Load Balancing process.

Microsoft Data Engine

ISA2006_Mssqlmsfw_PageFaults

Description: Monitors Page Faults of ISA Data Engine process.

ISA2006_Mssqlmsfw_PrivateBytes

Description: Monitors Private Bytes of ISA Data Engine process.

ISA2006_Mssqlmsfw_ProcessorTime

Description: Monitors Processor Time of ISA Data Engine process.

ISA2006_Mssqlmsfw_ThreadCount

Description: Monitors Thread Count of ISA Data Engine process.

ISA2006_Mssqlmsfw_WorkingSet

Description: Monitors Working Set of ISA Data Engine process.

Remote Access

ISA2006_Remoteaccess_PageFaults

Description: Monitors Page Faults of Remote Access process.

ISA2006_Remoteaccess_PrivateBytes

Description: Monitors Private Bytes of Remote Access process.

ISA2006_Remoteaccess_ProcessorTime

Description: Monitors Processor Time of Remote Access process.

ISA2006_Remoteaccess_ThreadCount

Description: Monitors Thread Count of Remote Access process.

ISA2006_Remoteaccess_WorkingSet

Description: Monitors Working Set of Remote Access process.

Server Control

ISA2006_Servercontrol_PageFaults

Description: Monitors Page Faults of Server Control process.

ISA2006_Servercontrol_PrivateBytes

Description: Monitors Private Bytes of Server Control process.

ISA2006_Servercontrol_ProcessorTime

Description: Monitors Processor Time of Server Control process.

ISA2006_Servercontrol_ThreadCount

Description: Monitors Thread Count of Server Control process.

ISA2006_Servercontrol_WorkingSet

Description: Monitors Working Set of Server Control process.

Server Storage

ISA2006_Serverstorage_PageFaults

Description: Monitors Page Faults of Server Storage process.

ISA2006_Serverstorage_PrivateBytes

Description: Monitors Private Bytes of Server Storage process.

ISA2006_Serverstorage_ProcessorTime

Description: Monitors Processor Time of Server Storage process.

ISA2006_Serverstorage_ThreadCount

Description: Monitors Thread Count of Server Storage process.

ISA2006_Serverstorage_WorkingSet

Description: Monitors Working Set of Server Storage process.

Storage Configuration

ISA2006_Storageconfig_PageFaults

Description: Monitors Page Faults of Storage Configuration process.

ISA2006_Storageconfig_PrivateBytes

Description: Monitors Private Bytes of Storage Configuration process.

ISA2006_Storageconfig_ProcessorTime

Description: Monitors Processor Time of Storage Configuration process.

ISA2006_Storageconfig_ThreadCount

Description: Monitors Thread Count of Storage Configuration process.

ISA2006_Storageconfig_WorkingSet

Description: Monitors Working Set of Storage Configuration process.

Server Logging

ISA2006_Logging_Firewall

Description: This policy logs selected performance data for ISA Server 2006 Firewall service.

ISA2006_Logging_Jobscheduler

Description: This policy logs selected performance data for ISA Server 2006 Job Scheduler.

ISA2006_Logging_Servercache

Description: This policy logs selected performance data for ISA Server 2006 Cache.

ISA2006_Logging_Servercontrol

Description: This policy logs selected performance data for ISA Server 2006 Server Control.

ISA2006_Logging_WebProxy

Description: This policy logs selected performance data for ISA Server 2006 Web Proxy service.

Discovery

ISA2006_discovery_System

Description: This policy discovers and adds infrastructure information to the service map.

ISA2006_discovery_Application

Description: This policy discovers and adds application and dependency information to the service map.

ISA2006_CheckDiscovery_Error

Description: This policy forwards discovery script errors to the console.

ISA2006_AutoDiscover_Delete

Description: Service deletion message.

Related Topics:

- ISA 2000 policies
- Deploying Policies for Microsoft Enterprise Servers
- Internet Security and Acceleration Server Overview

Internet Security and Acceleration Server reports

The Microsoft Enterprise Servers SPI offers a number of reports to help your monitoring of Internet Security and Acceleration Server activity. The following report descriptions include listings of performance counters used.

NOTE:
Report files for ISA 2000 begin with *g_ISA* , and for ISA 2006 with *g_ISA2006* .

- Firewall, Web Proxy, Scheduled Cache Content Download, and ISA Server Control Process CPU Statistics
- Dropped Packets Statistics
- Firewall Statistics
- Firewall, Web Proxy, Scheduled Cache Content Download, and ISA Server Control Process Memory Statistics
- ISA Server Cache Statistics
- Web Proxy Statistics
- Web Proxy Request Statistics
- Web Proxy Sites Allowed and Denied Statistics

Firewall, Web Proxy, Scheduled Cache Content Download, and ISA Server Control Process CPU Statistics
(g_ISACPUSummary.rpt OR g_ISA2006_CPUStatistics.rpt)

This report shows summary CPU statistics of ISA Server processes compared with overall CPU statistics of the system.

Counters:

- Process.% Processor Time (wspsrv, mspadmin, w3prefch, w3proxy)
- Process.Thread Count(wspsrv, mspadmin, w3prefch, w3proxy)
- Processor:% Processor Time.

NOTE:
This report requires that the Windows OS SPI Reports package is installed on your reporter machine, as it accesses tables created and populated by the Windows OS SPI. The Windows OS SPI tables used are: WINOSSPI_PROCESS and WINOSSPI_PROCESSOR.

Dropped Packets Statistics
(g_ISADroppedPackets.rpt OR g_ISA2006_DroppedPackets.rpt)

This report shows summary statistics of ISA Server total dropped packets resulting from packet filtering.

Counters:

- ISA Server Packet Filter.Total Dropped Packets.

Firewall Statistics
(g_ISAFirewall.rpt OR g_ISA2006_FirewallStatistic.rpt)

This report shows summary statistics of the ISA Server firewall, including the number of active sessions, the number of kernel mode data pumps, and the number of worker threads.

Counters:

- ISA Server Firewall Service.Active Sessions
- ISA Server Firewall Service.Active TCP Connections
- ISA Server Firewall Service.Active UDP Connections
- ISA Server Firewall Service.SecureNAT Mappings
- ISA Server Firewall Service.Available Worker Threads
- ISA Server Firewall Service.Worker Threads
- ISA Server Firewall Service.Bytes Read/sec
- ISA Server Firewall Service.Bytes Written/sec
- ISA Server Firewall Service.Kernel Mode Data Pumps.

Firewall, Web Proxy, Scheduled Cache Content Download, and ISA Server Control Process Memory Statistics
(g_ISAMemorySummary.rpt OR g_ISA2006_MemoryStatistics.rpt)

This report shows summary memory statistics of ISA Server processes.

Counters:

- Process.Private Bytes (wspsrv, mspadmin, w3prefch, w3proxy)
- Process.Working Set (wspsrv, mspadmin, w3prefch, w3proxy)
- Process.Page Faults/sec (wspsrv, mspadmin, w3prefch, w3proxy).

> **NOTE:**
> This report requires that the Windows OS SPI Reports package is installed on your reporter machine, as it accesses a table created and populated by the Windows OS SPI. The Windows OS SPI table used is WINOSSPI_PROCESS.

ISA Server Cache Statistics
(g_ISAServerCache.rpt OR g_ISA2006_ServerCacheStatistics.rpt)

This report shows summary statistics of the ISA Server memory and disk cache, including the memory cache usage ratio percentage, and the disk cache failure rate.

Counters:

- ISA Server Cache.Memory Bytes Retrieved Rate (KB/sec)
- ISA Server Cache.Memory Cache Allocated Space (KB)
- ISA Server Cache.Memory Usage Ratio Percent (%)
- ISA Server Cache.Disk Bytes Retrieved Rate (KB/sec)
- ISA Server Cache.Disk Cache Allocated Space (KB)
- ISA Server Cache.Disk Failure Rate (Fail/sec)
- ISA Server Cache.Total Disk Failures
- ISA Server Cache.URL Commit Rate (URL/sec)
- ISA Server Cache.URLs in Cache
- ISA Server Cache.Max URLs Cached

Web Proxy Statistics
(g_ISAWebProxy.rpt OR g_ISA2006_WebProxyStatistics.rpt)

This report shows summary statistics of the ISA Server Web Proxy, including the cache hit ratio percentage, the current number of Web proxy users, and the rate at which data bytes have been sent and received by the Web proxy service to and from Web Proxy clients.

Counters:

- ISA Server Web Proxy.Cache Hit Ratio (%
- ISA Server Web Proxy.Cache Running Hit Ratio (%)
- ISA Server Web Proxy.Total Cache Fetches
- ISA Server Web Proxy.Client Bytes Received/sec
- ISA Server Web Proxy.Client Bytes Sent/sec
- ISA Server Web Proxy.Client Bytes Total/sec
- ISA Server Web Proxy.Current Users
- ISA Server Web Proxy.Maximum Users

Web Proxy Request Statistics
(g_ISAWebProxyRequests.rpt OR g_ISA2006_WebProxyRequests.rpt)

This report shows summary statistics of the ISA Server Web Proxy including the number of failing client requests per second, and the total number of successful and failing client requests that have been made to the Web Proxy service.

Counters:

- ISA Server Web Proxy.Failing Requests/sec
- ISA Server Web Proxy.Requests/sec
- ISA Server Web Proxy.Current Average Milliseconds/request
- ISA Server Web Proxy.Total Failing Requests
- ISA Server Web Proxy.Total Requests
- ISA Server Web Proxy.Total Successful Requests
- ISA Server Web Proxy.Ftp Requests
- ISA Server Web Proxy.Http Requests

Web Proxy Sites Allowed and Denied Statistics
(g_ISAWebProxySites.rpt OR g_ISA2006_WebProxySites.rpt)

This report shows summary statistics of the ISA Server Web Proxy including the number of Web sites allowed access to client and the number of Web sites denied access to clients.

Counters:

- ISA Server Web Proxy.Sites Denied
- ISA Server Web Proxy.Sites Allowed

Related Topics:

- Internet Security and Acceleration Server Graphs

Internet Security and Acceleration Server graphs

The Microsoft Enterprise Servers SPI offers a number of graphs for monitoring Internet Security and Acceleration Server performance. They are listed here in alphabetical order, with links to their descriptions.
NOTE: Graphs for ISA 2006 have the prefix *ISA2006* .

- Cache URL Statistics
- Disk Cache Statistics
- Disk Failure Statistics
- Dropped Packets Statistics
- Firewall CPU
- Firewall Data Pump Statistics
- Firewall Memory
- Firewall Session / Connection Statistics
- Firewall Worker Threads Statistics
- ISA Server Control CPU
- ISA Server Control Memory
- Memory Cache Ratio Percent
- Memory Cache Statistics
- Scheduled Cache Content Download CPU
- Scheduled Cache Content Download Memory
- Sites Allowed/Denied Statistics
- Web Proxy Average Milliseconds/request
- Web Proxy Cache Hit Ratio Statistics
- Web Proxy Client Bytes Statistics

- Web Proxy CPU (ISA 2000 only)
- Web Proxy Memory (ISA 2000 only)
- Web Proxy Requests Statistics
- Web Proxy Users Statistics

Cache URL Statistics : This graph shows summary statistics relating to URLs of the ISA Server cache.

Disk Cache Statistics : This graph shows summary statistics of the ISA Server disk cache, including the disk cache failure rate.

Disk Failure Statistics : This graph shows summary statistics of the ISA Server disk cache failure rate.

Dropped Packets Statistics : This graph shows summary statistics of ISA Server total dropped packets resulting from packet filtering.

Firewall CPU : This graph shows summary CPU statistics of the ISA Server Firewall process.

Firewall Data Pump Statistics : This graph shows summary statistics of the ISA Server firewall, including the number of kernel mode data pumps.

Firewall Memory : This graph shows summary memory statistics of the ISA Server Firewall process.

Firewall Session / Connection Statistics : This graph shows summary statistics of the ISA Server firewall, including the number of active sessions.

Firewall Worker Threads Statistics : This graph shows summary statistics of the ISA Server firewall, including the number of worker threads.

ISA Server Control CPU : This graph shows summary CPU statistics of the ISA Server Control process.

ISA Server Control Memory : This graph shows summary memory statistics of the ISA Server Control process.

Memory Cache Ratio Percent : This graph shows summary statistics of the ISA Server memory cache, including the memory cache usage ratio percentage.

Memory Cache Statistics : This graph shows summary statistics of the ISA Server memory cache, including the memory bytes retrieved rate.

Scheduled Cache Content Download CPU : This graph shows summary CPU statistics of the ISA Server Scheduled Cache Content Download process.

Scheduled Cache Content Download Memory : This graph shows summary memory statistics of the ISA Server Scheduled Cache Content Download process.

Sites Allowed/Denied Statistics : This graph shows summary statistics of the ISA Server Web Proxy, including the number of Web sites allowed access to client and the number of Web sites denied access to clients.

Web Proxy Average Milliseconds/request : This graph shows summary statistics of the ISA Server Web Proxy, including the average milliseconds per client request that has been made to the Web Proxy service.

Web Proxy Cache Hit Ratio Statistics : This graph shows summary statistics of the ISA Server Web Proxy, including the cache hit ratio percentage.

Web Proxy Client Bytes Statistics : This graph shows summary statistics of the ISA Server Web Proxy, including the rate at which data bytes have been sent and received by the Web proxy service to and from Web Proxy clients.

Web Proxy CPU : This graph shows summary CPU statistics of the ISA Server Web Proxy process.

Web Proxy Memory : This graph shows summary memory statistics of the ISA Server Web Proxy process.

Web Proxy Requests Statistics : This graph shows summary statistics of the ISA Server Web Proxy, including the number of failing client requests per second that have been made to the Web Proxy service.

Web Proxy Users Statistics : This graph shows summary statistics of the ISA Server Web Proxy, including the current number of Web proxy users.

Related Topics:

- Internet Security and Acceleration Server Reports

SharePoint Portal Server

Microsoft's SharePoint Portal Server is a document repository system accessed through both a web and native client. SharePoint provides formal processes for authoring and approval, to allow simple but reliable document versioning.

SharePoint Portal Server enables enterprises to develop an intelligent portal that seamlessly connects users, teams, and knowledge so that people can use information and work efficiently across business processes. This is made possible by integrating information from various systems into one solution, through single sign-on and enterprise application integration capabilities, and with flexible deployment options and management tools. The portal facilitates end-to-end collaboration by enabling aggregation, organization, and search capabilities for people, teams, and information. Users can find relevant information quickly through customization and personalization of portal content and layout, as well as by audience targeting. Organizations can target information, programs, and updates to audiences based on their organizational role, team membership, interest, security group, or any other membership criteria that can be defined.

Related Topics:

- SharePoint Portal Server 2001
- SharePoint Portal Server 2003

SharePoint Portal Server services map

The **NET_SPS_Discovery** policy discovers and maps the service topology for SharePoint Portal servers. The **NET_SPSSitesDiscovery** policy discovers the site structure. The services map is generated from all this collected data, offering an efficient and effective way for administrators to manage SharePoint Portal server (SPS) services.

> **NOTE:**
> The NET_SPS_Discovery policy requires the user-id and password of a service account which has permission to access the SharePoint topology configuration database. Open the NET_SPS_Discovery policy and provide the proper user-id/password before deploying the policy to SharePoint nodes.

Microsoft Enterprise Servers SPI discovers and indicates on the service map:

SharePoint Portal 2001 services:

- Search services
- Document Manager
- Workspaces.

SharePoint Portal 2003 services:

- Search services
- Web services
- Team Web services
- Indexing services
- Alert services.

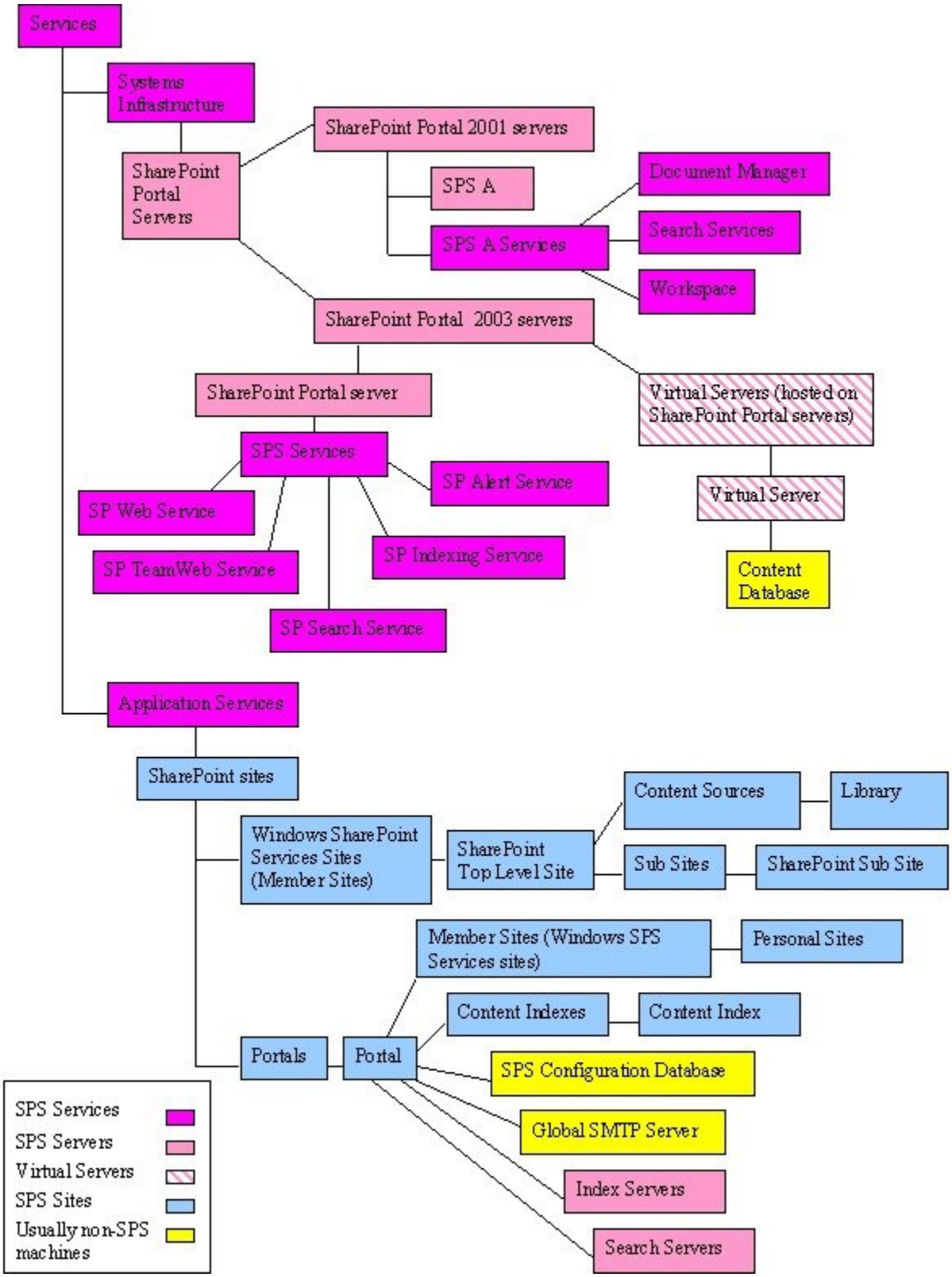
In addition, the following SharePoint Portal Server components:

- all the systems on which SharePoint Portal Server is installed
- all components enabled on each machine
- SharePoint Portal Server Extended Virtual Servers and the machines which they are hosted on
- the virtual server on which any site is hosted, (allows you to see the sites affected when a virtual server is unavailable)

- Content Databases, Configuration Databases, and SMTP servers and the dependency of these services on other components like IIS and Windows OS
- all WSS sites and their content sources hosted by SharePoint Portal Server, and their sub web (child) sites
- SharePoint Portal Server Portal sites and the hierarchy of their member sites

Systems Infrastructure information is gathered by the **NET_SPS_Discovery** policy, and Application Services data from the **NET_SPSSitesDiscovery** policy.

In a Web Farm scenario, the service map clearly identifies a Portals distributed environment: its web-front-end servers, search servers, indexing servers and its content and configuration databases. See the diagram below of the hierarchy of the SPS features discovered by the Microsoft Enterprise Servers SPI, and their dependencies:



Related Topics:

- Creating Service Maps for Microsoft Enterprise Servers

SharePoint Portal Server 2001

Microsoft's SharePoint Portal Server is a document repository system accessed through both a web and native client. SharePoint provides formal processes for authoring and approval, to allow simple but reliable document versioning.

The following policies are available to monitor SharePoint Portal Server services:

- **NET_SPSServices** : monitors Microsoft SharePoint Portal Service (msdmserv) and Microsoft Search Services (mssearch).
- Policies for forwarding all SharePoint Portal Server application Windows 2000 event log entries with severity 'Error', 'Information' and 'Warning'.
- **NET_SPS_Discovery** : a group of policies to discover and map the service topology for SharePoint Portal Server.
- **NET_SPSSitesDiscovery** : discovers the SharePoint Portal Server site structure.
- **NET_SPS_Logging** : logs selected performance data for SharePoint Portal Server.
- **NET_SPS_PageFaultssec-SearchServices** : monitors page faults of the Microsoft search service.
- **NET_SPS_ProcessorTime-SearchServices** : monitors processor utilization of the Microsoft search service.
- **NET_SPS_WorkingSet-SearchServices** : monitors the working set of the Microsoft search service.
- **NET_SPS_ResponseTime** : monitors the workspace response time.

The following SharePoint Portal Server reports are available:

- **Document Manager CPU Statistics** : this report shows the summary CPU statistics of SharePoint Portal Server processes, compared with overall CPU statistics of the system, in both graphical and tabular format. The summarized process statistics include the percentage of CPU time used by the document manager compared with the percentage of time the system's CPU was busy.
- **Document Manager Process Memory Statistics** : this report shows summary memory statistics of SharePoint Portal Server processes, in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the document manager.
- **Top Resource Download Statistics** : this report shows top download statistics from the SharePoint workspaces by user, resource and machine.

- **Workspace Response Time Statistics** : this report shows response time and availability information for all SharePoint workspaces.

The following SharePoint Portal Server graphs are available:

- **Document Manager CPU** : this graph shows summary CPU statistics of the SharePoint Portal Server document manager process. This data can be compared with System Processor Time to determine to what extent the document manager process is utilizing processor time.
- **Document Manager Memory:** this graph shows summary memory statistics of the SharePoint Portal Server document manager process. The summarized process statistics include the page faults per second, private bytes, and working set used by the process.
- **Index Service CPU:** this graph shows summary CPU statistics for the Microsoft index service. This data can be compared with System Processor Time to determine to what extent the indexer is utilizing processor time.
- **Index Service Memory:** this graph shows summary memory statistics of the Microsoft index service. The summarized process statistics include the page faults per second, private bytes, and working set used by the process.
- **Search Service CPU:** this graph shows summary CPU statistics of the Microsoft search service. This data can be compared with System Processor Time to determine to what extent the search service is utilizing processor time.
- **Service Memory** : this graph shows summary memory statistics of the Microsoft search service. The summarized process statistics include the page faults per second, private bytes, and working set used by the process.

Related Topics:

- SharePoint Portal Server Policies
- SharePoint Portal Server Reports
- SharePoint Portal Server Graphs
- SharePoint Portal Server Service Map

SharePoint Portal Server 2001 policies

The following predefined policies for the SharePoint Portal Server are available with the Microsoft Enterprise Servers SPI.

Availability Monitoring

NET_SPSServices

Description: This policy monitors the following Windows 2000 services:

- Microsoft SharePoint Portal Service (msdmserv)
- Microsoft Search Services (mssearch)

If a service is not running and the service startup is set to "Auto Start", then Microsoft Enterprise Servers SPI attempts to restart the service and an error message is sent to the console to indicate that the service is not running.

NET_SPS-PageFaultssec-SearchServices

Description: This policy monitors page faults of the Microsoft search services.

NET_SPS-ProcessorTime-SearchServices

Description: This policy monitors processor utilization of the Microsoft search services.

NET_SPS-WorkingSet-SearchServices

Description: This policy monitors the working set of the Microsoft search services.

NET_SPS-IISResponseTime

Description: This policy monitors workspace response time queried through the Internet Information Server (IIS).

NET_SPS-WSSResponseTime

Description: This policy monitors workspace response time queried through the Web Storage System (WSS).

Event Monitoring

NET_SPSFwdApplicationError

Description: Forwards all SharePoint Portal Server application entries in the Windows 2000 event log with severity 'Error'.

NET_SPSFwdApplicationInformation

Description: Forwards all SharePoint Portal Server application entries in the Windows 2000 event log with severity 'Information'.

NET_SPSFwdApplicationWarning

Description: Forwards all SharePoint Portal Server application entries in the Windows 2000 event log with severity 'Warning'.

Logging

NET_SPS_Logging

Description: This policy logs selected performance data for SharePoint Portal Server.

NET_SPS_Errors

Description: This policy captures and formats errors generated by the SharePoint SPI policies.

NOTE:
Deploy the Windows OS SPI logging policy (WINOSSPI-WINOS_Win2k_Logging) to log SharePoint Portal Server process-related data for CPU and memory counters. In addition, the WINOSSPI-IISCollector is also required to log SharePoint web usage statistics.

Discovery

NET_SPS_Discovery

Description: This policy discovers and maps workspaces and service topology for SharePoint Portal Server.

NET_SPS_ForwardDiscoveryError

Description: This Log File policy is deployed automatically every time the discovery policy is deployed, to track and report to the management console any discovery errors logged to the Javaagent log.

NET_SPS-AutoDiscover_Delete

Description: This policy will remove the service node entries in the service map when the SharePoint product is uninstalled from the target machine.

Related Topics:

- Deploying Policies for Microsoft Enterprise Servers
- SharePoint Portal Server 2001 overview

SharePoint Portal Server 2001 reports

The following predefined reports for SharePoint Portal Server are available with the Microsoft Enterprise Servers SPI:

CPU Summary (g_SPSCPUSummary.rpt)

This report shows summary CPU statistics of SharePoint Portal Server processes, compared with overall CPU statistics of the system, in graphical and tabular format. The summarized process statistics include the percentage of CPU time used by the document manager compared with the percentage of time the system's CPU was busy.

> **NOTE:**
> Deploy the WINOSSPI-WINOS_Win2k_Logging policy for this report to function correctly.

Counters:

- Process.% Processor Time (msdmserv)
- Process.Thread Count (msdmserv)
- Processor.% Processor Time (msdmserv)

Memory Summary (g_SPSMemorySummary.rpt)

This report shows summary memory statistics of SharePoint Portal Server processes, in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the document manager.

> **NOTE:**
> Deploy the WINOSSPI-WINOS_Win2k_Logging policy for this report to function correctly.

Counters:

- Process.Private Bytes (msdmserv)
- Process.Working Set (msdmserv)
- Process.Page Faults/sec (msdmserv)

Documents Summary (g_SPSDocuments.rpt)

This report displays document summaries for SharePoint workspaces.

> **NOTE:**
> Deploy the WINOSSPI-IISCollector and NET_SPS_Logging policies for this report to function correctly.

Top Downloads (g_SPSTopDownloads.rpt)

This report shows top download statistics from the SharePoint workspaces by resource and user.

> **NOTE:**
> Deploy the WINOSSPI-IISCollector and NET_SPS_Logging policies for this report to function correctly.

Response Time Summary (g_SPSResponseTime.rpt)

This report summarizes response time and availability information for all SharePoint workspaces.

Related Topics:

- SharePoint Portal Server 2001 graphs

SharePoint Portal Server 2001 graphs

The following predefined graphs for SharePoint Portal Server 2001 are available with the Microsoft Enterprise Servers SPI:

Document Manager CPU

This graph shows summary CPU statistics of the SharePoint Portal Server document manager process. This data can be compared with System Processor Time to determine to what extent the document manager process is utilizing processor time.

Counter: Process.%Processor Time (msdmserv)

Document Manager Memory

This graph shows summary memory statistics of the SharePoint Portal Server document manager process. The summarized process statistics include the page faults per second, private bytes, and working set used by the process.

Counters:

- Process.Private Bytes (msdmserv)
- Process.Working Set (msdmserv)
- Process.Page Faults/sec (msdmserv)

Index Service CPU

This graph shows summary CPU statistics for the Microsoft index service. The data can be compared with System Processor Time to determine to what extent the indexer is utilizing processor time.

Counter: Process.%Processor Time (mssdmn)

Index Service Memory

This graph shows summary memory statistics of the Microsoft index service. The summarized process statistics include the page faults per second, private bytes, and working set used by the process.

Counters:

- Process.Private Bytes (mssdmn)

- Process.Working Set (mssdmn)
- Process.Page Faults/sec (mssdmn)

Response Time

This graph shows the response time of each SharePoint workspace through the Internet Information Server (IIS) and Web Storage System (WSS).

Search Service CPU

This graph shows summary CPU statistics of the Microsoft search service. The data can be compared with System Processor Time to determine to what extent the search service is utilizing processor time.

Counter: Process.%Processor Time (mssearch)

Service Memory

This graph shows summary memory statistics of the Microsoft search service. The summarized process statistics include the page faults per second, private bytes, and working set used by the process.

Counters:

- Process.Private Bytes (mssearch)
- Process.Working Set (mssearch)
- Process.Page Faults/sec (mssearch)

Related Topics:

- SharePoint Portal Server 2001 reports

SharePoint Portal Server 2003

Microsoft's SharePoint Portal Server is a document repository system accessed through both a web and native client. SharePoint provides formal processes for authoring and approval, to allow simple but reliable document versioning. In addition, SharePoint Portal Server 2003 uses Microsoft Windows SharePoint Services 2003 sites to create portal pages for people, information, and organizations. The portal extends the capabilities of Windows SharePoint Services sites with organization and management tools, and enables teams to publish information in their sites to the entire organization.

The Microsoft Enterprise Servers SPI assists monitoring and managing SharePoint 2003 deployments across enterprises. Following are the SPI product features for the monitoring of SharePoint 2003:

Discovery

The **Microsoft Enterprise Servers SPI Discovery** discovers and maps the service topology and site structure for SharePoint Portal servers and displays the discovered services in various maps.

Configuration Database availability monitoring

Policies access the SharePoint Portal Server 2003 default configuration database, execute a SQL 'Select query', and send an appropriate message to the services map. Using this policy an administrator can check status and connectivity to the SharePoint 2003 Configuration Database.

Content Database availability monitoring

Policies execute SQL 'Select queries' on each of the content databases for all the virtual servers running on a node, and send back appropriate messages to the relevant content database node on the services map. Using these policies an administrator can check SharePoint 2003 Content Database connectivity and status of database. If for some reason a content database goes down, the service map shows all the sites impacted.

Virtual servers availability monitoring

Policies identify virtual servers, make the HTTP 'Get call' to the virtual servers, and send status messages back to the appropriate Virtual Server nodes on the services map. If a virtual server or IIS is down, this can be detected and the impact to the overall SharePoint deployment will be indicated in the service map.

Service monitoring

Policies are automatically deployed depending on which SharePoint services are enabled. They monitor

the status of essential services, like the search service, singlesignon service, admin service, alert service and timer service and send status messages to the console.

Event monitoring

Policies monitor the Windows Event log for warning, error and information level messages sent from SharePoint alert, admin, search, timer, and singlesignon services, and send status messages to the console.

Performance monitoring

Policies monitor MicrosoftGatherer\Reason to BackOff, Active Queue Length, Documents Delayed Retry and Heartbeats counters, and send intelligent status messages to the console.

Reports and graphs

Data logging policies make numerous reports and graphs available, displaying collected data in meaningful ways for managing SharePoint Portal Server successfully.

Reports and Graphs use data from CPU and Memory usage, and Admin, Search, Page/Faults, SingleSignon, Alert, SPTimer, and IIS Worker services and processes.

Browse SharePoint sites

Browse SharePoint Site Tool : Enables user to easily navigate to portal site node from the HPOM console. Right-click the portal site and select **Launch Tool** , which opens the portal site in the browser.

Related Topics:

- SharePoint Portal 2003 server policies
- SharePoint Portal 2003 server reports
- SharePoint Portal 2003 server graphs
- SharePoint Portal Server service map

SharePoint Portal Server 2003 policies

The following policies for SharePoint Portal Server 2003 are offered with the Microsoft Enterprise Servers SPI. They are grouped here in the following categories:

- Availability monitoring
- Service monitoring
- Windows Service monitoring
- Event monitoring
- Performance monitoring
- Logging
- Discovery

Availability monitoring

Configuration Database:

NET_SPS_MonitorConfigDB and **NET_SPS_CheckSPSComponents**

Description: These policies access the SharePoint Portal Server 2003 default configuration database, execute a SQL 'Select query', and send an appropriate message to the Configuration Database node on the services map. Using this policy an administrator can check status and connectivity to the SharePoint 2003 Configuration Database.

NOTE:
This policy requires the user-id and password of a service account which has permission to access the SharePoint topology configuration database. Open the NET_SPS_MonitorConfigDB policy and enter the proper user-id/password before deploying the policy to SharePoint nodes.

Content Database:

NET_SPS_MonitorContentDBs and **NET_SPS_CheckSPSComponents**

Description: These policies execute SQL 'select queries' on each of the content databases for all the virtual servers running on a node, and send back appropriate messages to the relevant content database node on the services map. Using these policies an administrator can check SharePoint 2003 Content Database connectivity and status of database. If for some reason a content database goes down, the service map shows all the sites impacted.

NOTE:
The NET_SPS_MonitorContentDBs schedule task policy requires the user-id and password of a service account which has permission to access the SharePoint configuration database. Open the policy and enter the proper user-id/password before deploying the policy to SharePoint nodes.

Virtual servers:

NET_SPS_MonitorVirtualServers and **NET_SPS_CheckSPSComponents**

Description: These policies identify virtual servers, make the HTTP 'Get call' to the virtual servers, and send status messages back to the appropriate Virtual Server nodes on the services map. If a virtual server or IIS is down, this can be detected and the impact to the overall SharePoint deployment will be indicated in the service map.

NOTE:
The NET_SPS_MonitorVirtualServers schedule task policy requires the user-id and password of a service account which has permission to access the SharePoint configuration database. Open the policy and enter the proper user-id/password before deploying the policy to SharePoint nodes.

NET_SPS_CheckSPSComponents

Description: This policy traps all the messages sent from the **NET_SPS_MonitorConfigDB** , **NET_SPS_MonitorContentDBs** and **NET_SPS_MonitorVirtualServers** policies, and sends them on to the appropriate nodes on the services map.

Service monitoring

The following policies are automatically deployed depending on which SharePoint services are enabled. They monitor the status of essential services:

NET_SPS2003SearchServices

Description: This policy checks if the Windows SharePoint Service 'SPSSEARCH' is running properly and sends messages about its status to the console.

NET_SPS2003SingleSignOnService

Description: This policy checks if the Windows SharePoint Service 'ssosrv' is running properly and sends messages about its status to the console.

NET_SPS2003AdminService

Description: checks if the Windows SharePoint Service 'SPAdmin' is running properly and sends messages about its status to the console.

NET_SPS2003AlertService

Description: This policy checks if the Windows SharePoint Service 'SPSAlert' is running properly and sends messages about its status to the console.

NET_SPS2003TimerService

Description: This policy checks if the Windows SharePoint Service 'Sptimer' is running properly and sends messages about its status to the console.

Windows Service monitoring

Policies in the Windows SharePoint Services folder help to monitor the events from Windows SPS, and sources dependent on Windows SPS. These policies are automatically deployed depending on which SharePoint services are enabled.

NET_SPS_FwdWSSError

Description: This policy monitors Database Connection Errors, Database Capacity Reached, Web Part Unsafe Control Detected, OWS Timer, STSWel error, W3WP error, and all other events from Windows SPS with a severity of 'Critical'.

NET_SPS_FwdWSSWarning

Description: This policy monitors the WSS events with a severity of Warning, with a Database Capacity Reached rule, and a rule monitoring all other events from Windows SPS with a severity of 'Warning'.

Event Monitoring

NET_SPSFwdApplicationWarning

Description: This policy monitors the Windows Event log for any warning level messages from SharePoint alert, admin, search, timer, and singlesignon services.

NET_SPSFwdApplicationError

Description: This policy monitors the Windows Event log for any error level messages from SharePoint alert, admin, search, timer, and singlesignon services.

NET_SPSFwdInformation

Description: This policy monitors the Windows Event log for any information level messages from SharePoint services, according to rules concerning virus checking and Active Directory account creation and deletion.

NET_SPS_HTML_Transformation

Description: HTML transformation server is an optional component for a server farm running Windows Share Point Services. This policy has the rules to monitor HTML launcher started, HTML load balancer stopped, HTML launcher, and HTML load balancer started stopped events.

Performance monitoring

NET_SPS_ReasonToBackOff

Description: This policy monitors MicrosoftGatherer\Reason to BackOff counter to see if its value is higher than zero. A non zero number means that document crawling has been paused because of insufficient system resources. Usually a non zero value indicates that the system is low on memory, or that the current disk IO is too high to process requests.

NET_SPSActive Queue Length

Description: This policy monitors Microsoft Gatherer\Active Queue Length. The counter indicates the number of documents that are waiting for a robot thread to process them. Normally, this number should be zero. If this number is not zero, it means that the server is falling behind, which could be a temporary condition caused by an especially busy period. If this number is anything other than zero, then all available threads should be filtering. If the number is above zero, but all possible threads aren't filtering, it usually means that the SharePoint services need to be stopped and restarted.

NET_SPSDocuments Delayed Retry

Description: This policy monitors Microsoft Gatherer\Documents Delayed Retry. Normally the value should be zero and a non zero value means that SharePoint is having problems accessing the Web storage system. Access attempts will keep retrying until successful. If the Documents Delayed Retry value momentarily goes above zero and then goes back down, it means that the system was simply busy at the time of the original request, but later was able to catch up with the demand being placed on it. If, however, the number continues to steadily rise, this indicates a Web storage system failure.

NET_SPSHeartBeats

Description: This policy monitors the Microsoft Gatherer\Heartbeats counter. By default, a heartbeat occurs every ten seconds. If you see that the number of heartbeats isn't increasing, it means that the SharePoint services have either stopped or are unresponsive.

NET_SPSIndexerCatalogsNumofDocument

Description: This policy auto deploys to SharePoint Portal indexing server nodes and runs every 12 hours. This policy sends a message back to the console with the total number of documents in all indexes, and increases in the number of documents. This will help in identifying whether there is a need to add additional indexing servers.

Logging

NET_SPS_Indexingcounters_Logging and **NET_SPS_CreateCodaDataSources**

Description: These policies are auto deployed to SharePoint Portal Server 2003 indexing server nodes. NET_SPS_CreateCodaDataSources creates the data source required to log data, and NET_SPS_Indexingcounters_Logging logs index name, number of documents in each index, index size, increase in number of documents indexed, increase in size of the index, total free space remaining, and used space on indexing servers. This policy runs every 30minutes. Deploying these policies is essential for generating indexing server reports

NET_SPS_Common_Logging and **WINOSSPI-WINOS-Win2k-Logging**

Description: These policies are auto deployed to all the SharePoint installed nodes in the topology. The WINOSSPI-WINOS-Win2k-Logging policy logs the cpu and memory related statistics for all the sharepoint services, and NET_SPS_Common_Logging creates the data source which helps in creating the CPU and Memory related reports. Deploying these policies is essential for generating CPU and Memory report.

NOTE:
Deploy the Windows OS SPI logging policy (WINOSSPI-WINOS_Win2k_Logging) to log SharePoint Portal Server process-related data for CPU and memory counters. In addition, the WINOSSPI-IISCollector is also required to log SharePoint web usage statistics.

Discovery

NET_SPS_Discovery

Description: This policy discovers and maps workspaces and service topology for SharePoint Portal Server.

NET_SPSSitesDiscovery

Description: This policy discovers and maps the site structure for SharePoint Portal Server.

Related Topics:

- Deploying policies for Microsoft Enterprise Servers

- SharePoint Portal Server 2003 Overview

SharePoint Portal Server 2003 reports

Memory and CPU reports

These reports can be used to plan and predict capacity of SharePoint Portal Server deployment. They can assist determining whether an additional search server or Web front end server needs to be added to improve performance.

> **NOTE:**
> Deploy the WINOSSPI-WINOS_Win2k_Logging policy for these reports to function correctly.

Weekly CPU Usage Summary (g_SPSCPUWeeklySummary.rpt)

This report shows summary CPU statistics of Admin, Alert and Timer services for each of the SharePoint Portal Server 20003 installed nodes in an enterprise deployment. The displays for every six hours over the last 7 days, compared with overall CPU statistics of the system, in both graphical and tabular format. This report can help administrators see which server is heavily loaded and which process is causing so much load.

Weekly CPU Usage Summary of Search\Indexing Service
(g_SPS_IdxSearchService_CPUWeeklySummary.rpt)

This report shows summary Indexing\Search services for each of the SharePoint 2003 installed nodes in an enterprise deployment. The data displays for every six hours over the past 7 days, and compared with overall CPU statistics of the system, in both graphical and tabular format. This report can be used for capacity\expansion planning for the search and indexing servers in the topology.

Weekly Memory Usage Summary (g_SPSMemoryWeeklySummary.rpt)

This report shows summary of memory statistics of Admin, Alert, Timer, Search and Indexing services for each of the SharePoint Portal Server 20003 installed nodes in an enterprise deployment. The data displays for every six hours over the last 7 days, compared with overall CPU statistics of the system, in both graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by Admin, Alert, Timer, Search and Indexing services.

Indexing Server reports

Weekly summary of Indexing space used, Free Space, Total Used Space
(g_SPSIndexingWeeklySummary.rpt)

This report shows the size of each index, total free space, and total used space left on each of the SharePoint Portal Server 2003 Indexing servers. The report shows data points, and charts for every 12 hours in each day over the past seven days.

Monthly summary of Indexing space used, Free Space, Total Used Space
(g_SPSIndexingMonthlySummary.rpt)

This report shows the size of each index, total free space, and total used space left on each of the SharePoint Portal Server 2003 Indexing servers. The report shows data points, and charts for every day over the past 30 days.

Weekly summary of Increase in Indexing space used, Free Space, Total Used Space
(g_SPSIntervalIndexingWeeklySummary.rpt)

This report shows the increase in the size of each index, total free space, and total used space left on each of the SharePoint Portal Server 2003 Indexing servers. The report shows data points, and charts for every 12 hours in each day over the past seven days.

Weekly summary of Indexing space used, Free Space, Total Used Space
(g_SPSIntervalIndexingMonthlySummary.rpt)

This report shows the increase in the size of each index, total free space, and total used space left on each of the SharePoint Portal Server 2003 Indexing servers. The report shows data points, and charts for every day over the past 30 days.

Weekly summary of Number of Docs in Indexes, Increased Number of Docs, Index Size
(g_SPSDocsInIndexingWeeklySummary.rpt)

This report shows the increased number of documents, total number of documents, and total size of each index for every SharePoint Portal Server 2003 Indexing server. The report shows data points, and charts for every 12 hours in each day over the past seven days.

Weekly summary of Indexing space used, Free Space, Total Used Space
(g_SPSDocsInIndexingMonthlySummary.rpt)

This report shows the increased number of documents, total number of documents, and total size of each index for every SharePoint Portal Server 2003 Indexing server. The report shows data points, and charts for every day over the past 30 days.

NOTE:
Deploy the WINOSSPI-IISCollector and NET_SPS_Logging policies for these reports to function correctly.

IIS Worker Process reports

Weekly Summary of IIS Worker Process CPU Usage

(g_SPS_IIS_CPUWeeklySummary.rpt)

This report shows the summary of CPU usage of IIS worker process (w3wp process) for the past week. The report can be used to find out whether the IIS is getting used heavily, and can give an indication of whether is may be necessary to add additional web front end servers.

> **NOTE:**
> Deploy the WINOSSPI-IISCollector and NET_SPS_Logging policies for this report to function correctly.

Related Topics:

- SharePoint Portal Server 2003 graphs

SharePoint Portal Server 2003 graphs

The following predefined graphs for SharePoint Portal Servers are available with the Microsoft Enterprise Servers SPI:

SharePoint Portal Server Admin service CPU usage (2003 and later)

This graph shows summary CPU statistics of the SharePoint admin service process (spsadmin.exe). This data can be compared with System Processor Time to determine to what extent the SharePoint admin service is utilizing processor time.

SharePoint Portal Server Admin service Memory usage (2003 and later)

This graph shows summary memory statistics of the SharePoint admin service process (spsadmin.exe). The summarized process statistics show private bytes, and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set

SharePoint Portal Server Search Service CPU usage

This graph shows summary CPU statistics of the SharePoint search service process (mssearch.exe). This data can be compared with System Processor Time to determine to what extent the SharePoint admin service is utilizing processor time.

SharePoint Portal Server Search Service Memory usage

This graph shows summary memory statistics of the SharePoint search service process (mssearch.exe). The summarized process statistics include the private bytes, and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set

SharePoint Search Service Page Faults/sec

This graph shows summary memory statistics of the SharePoint Search service process (mssearch.exe). The summarized process statistics include the Page Faults\sec by the process.

Counters:

- Process:Page Faults\sec

SharePoint Portal Server SingleSignon Service CPU usage (2003 and later)

This graph shows summary CPU statistics of the SharePoint Single sign on service process (SSOSRV.exe). This data can be compared with System Processor Time to determine to what extent the SharePoint Single sign on service is utilizing processor time.

SharePoint Portal Server SingleSignon Service Memory usage (2003 and later)

This graph shows summary memory statistics of the SharePoint single sign on service process (SSOSRV.exe). The summarized process statistics include the private bytes, and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set

SharePoint Portal Server SPTimer Service CPU Usage (2003 and later)

This graph shows summary CPU statistics of the SharePoint SPTimer service process (OWSTIMER.exe). This data can be compared with System Processor Time to determine to what extent the SharePoint SPTImer service is utilizing processor time.

SharePoint Portal Server SPTimer Service Memory usage (2003 and later)

This graph shows summary memory statistics of the SharePoint SPTimer service process (OWSTIMER.exe). The summarized process statistics include the private bytes and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set, Process

SharePoint Portal Server Alert Service CPU usage (2003 and later)

This graph shows summary CPU statistics of the SharePoint Alert service process (SPSNotificationService.exe). This data can be compared with System Processor Time to determine to what extent the SharePoint SPTImer service is utilizing processor time.

SharePoint Portal Server 2003 Alert Service Memory usage (2003 and later)

This graph shows summary memory statistics of the SharePoint Alert service process (SPSNotificationService.exe). The summarized process statistics include the private bytes and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set, Process

IIS Worker process CPU usage (2003 and later)

This graph shows summary CPU statistics of the IIS worker process service (w3wp.exe). This data can be compared with System Processor Time to determine to what extent the IIS worker process service is utilizing processor time, which can be used in making decisions about whether to add additional web front end servers.

IIS Worker process Memory usage (2003 and later)

This graph shows summary memory statistics of the IIS worker process service (w3wp.exe). The summarized process statistics include the private bytes and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set

IIS Worker processes Page Faults (2003 and later)

This graph shows summary memory statistics of the IIS worker process service (w3wp.exe). The summarized process statistics include the Page Faults\sec by the process.

Counters:

- Process:Page Faults\sec

Related Topics:

- SharePoint Portal Server 2003 reports

SharePoint Portal Server 2007

Microsoft's SharePoint Portal Server is a document repository system accessed through both a web and native client. SharePoint provides formal processes for authoring and approval, to allow simple but reliable document versioning.

The following policies are available to monitor SharePoint Portal Server services:

Availability Monitoring

- **MSES_MOSS_AdminService** : monitors the 2007 server. If the service is stopped it is restarted automatically
- **MSES_MOSS_Document Conversions Load Balancer Service** : monitors the Document Conversions Load Balancer Service process
- **MSES_MOSS_OfficeServerSearchService** : monitors the Office Sharepoint server search.
- **MSES_MOSS_ TimerService** : monitors the 2007 server. If the service is stopped it is restarted automatically
- **MSES_MOSS_Document Conversions Launcher Service** : monitors the Document Conversions Launcher Service process
- **MSES_MOSS_SearchService** : monitors the 2007 server. If the service is stopped it is restarted automatically
- **MSES_MOSS_SingleSignOnService** : monitors the 2007 server. If the service is stopped it is restarted automatically

Logging

- **MSES_MOSS-2k7_Logging_Process_MOSS.Conversions.LoadBalancer** : collects data for Microsoft Office Server Conversions LoadBalancer
- **MSES_MOSS-2k7_Logging_Process_WSSTRACING** : collets data for the WSSTRACING process
- **MSES_MOSS-2k7_Logging_Process_SPWRITER** : collets data for the SPWRITER process

- **MSES_MOSS-2k7_Logging_Process_WSADMIN** :collects data for WSADMIN process
- **MSES_MOSS-2k7_Logging_Process_OWSTIMER** : collects data for the OWSTIMER process
- **MSES_MOSS-2k7_Logging_Process_MSSEARCH** : collects data for MSSEARCH process
- **MSES_MOSS-2k7_Logging_Process_w3wp** : collects data for w3wp process
- **MSES_MOSS-2k7_ Logging_Process_SSOSRV :** collects data for the SSOSRV process
- **MSES_MOSS-2k7_Logging_Process_ MOSS.Conversions.Launcher:** collects data for conversions.Launcher process
- **MSES_MOSS-2k7_ CreateCodeDataSources:** creates a code data source for MOSS services

Service Monitoring

- **MSES_MOSS-2k7_Database_Monitoring :** checks the status of the MOSS database instances
- **MSES_MOSS-2k7_ Logical_Services_Monitoring** : checks the status of the MOSS logical services
- **MSES_MOSS_Documents Delayed Retry** : monitors the Documents Delayed Retry counter

Application Monitoring

- **MSES_MOSS_FwdApplicationInformation :** handles informational information from all sharepoint services
- **MSES_MOSS_FwdApplicationWarning** : handles the warning messages from all sharepoint services

The following SharePoint Portal Server reports are available:

Memory and CPU Reports

- **Daily/Weekly CPU Usage Summary** (g_MOSS2k7CPUSummary.rpt/g_MOSS2k7CPUWeeklySummary.rpt) : this report shows summary CPU statistics of MOSS 2007 server's services installed nodes in an enterprise deployment. The displays for every six hours over the last 7 days, compared with overall CPU statistics of the system, in both

graphical and tabular format. This report can help administrators see which server is heavily loaded and which process is causing so much load.

- **Daily/Weekly Memory Usage Summary** (g_MOSS2k7MemorySummary.rpt/ g_MOSS2k7MemoryWeeklySummary.rpt) : this report shows summary CPU statistics of MOSS 2007 server's services installed nodes in an enterprise deployment. The data displays for every six hours over the last 7 days, compared with overall CPU statistics of the system, in both graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the services.

IIS Worker Process reports

- **Weekly Summary of IIS Worker Process CPU Usage** (g_MOSS2k7_IIS_CPUWeeklySummary.rpt): this report shows the size of each index, total free space, and total used space left on each of the SharePoint Portal Server 2003 Indexing servers. The report shows data points, and charts for every 12 hours in each day over the past seven days.
-

The following SharePoint Portal Server graphs are available:

- **SharePoint Server Admin service CPU usage** (2007)
- **SharePoint Portal Server Admin service Memory usage** (2007)
- **SharePoint Portal Server Search Service CPU usage**
- **SharePoint Portal Server Search Service Memory usage** .
- **SharePoint Search Service Page Faults/sec**
- **SharePoint Portal Server SingleSignon Service CPU usage** (2007)
- **SharePoint Portal Server SingleSignon Service Memory usage** (2007)
- **SharePoint Portal Server SPTimer Service CPU Usage** (2007)
- **SharePoint Portal Server SPTimer Service Memory usage** (2007)
- **IIS Worker process CPU usage** (2007)
- **IIS Worker process Memory usage** (2007)
- **IIS Worker processes Page Faults** (2007)

Related Topics:

- SharePoint Portal Server Policies
- SharePoint Portal Server Reports
- SharePoint Portal Server Graphs
- SharePoint Portal Server Service Map

Auto Deployment Policies

HPOM automatically deploys policies to a node if the agent is correctly installed. You can disable the auto-deployment for all nodes if you manually wish to deploy the policies. The following describe the Sharepoint Portal Server 2007 policies.

Availability Monitoring

Policy Name: **MSES_MOSS_AdminService**

Policy Group: SPI for MSES> en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Description: Monitors the 2007 server. If the service is stopped it is restarted automatically

Default Schedule: Every 5 minutes daily.

Policy Type: Windows Management Interface

Policy Name: **MSES_MOSS_Document Conversions Load Balancer Service**

Description: Monitors the Document Conversions Load Balancer Service process

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Windows Management Interface

Policy Name:**MSES_MOSS_OfficeServerSearchService**

Description: Monitors the Office Sharepoint server search.

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Windows Management Interface

Policy Name: **MSES_MOSS_ TimerService**

Description: Monitors the 2007 server. If the service is stopped it is restarted automatically

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Windows Management Interface

Policy Name: **MSES_MOSS_Document Conversions Launcher Service**

Description: Monitors the Document Conversions Launcher Service process

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Windows Management Interface

Policy Name: **MSES_MOSS_SearchService**

Description: Monitors the 2007 server. If the service is stopped it is restarted automatically

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Windows Management Interface

Policy Name: **MSES_MOSS_SingleSignOnService**

Description: Monitors the 2007 server. If the service is stopped it is restarted automatically

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Windows Management Interface

Logging

The following metrics are collected for all the processes mentioned under Logging.

Metric Name	Data Type
Instance Name	Text
Working Set	Real64
Page Faults per sec	Real64
Private Bytes	Real64
Thread Count	Real64
Processor Time (%)	Real64

Policy Name: **MSES_MOSS-2k7_Logging_Process_MOSS.Conversions.LoadBalancer**

Description: Collects data for Microsoft Office Server Conversions LoadBalancer

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Measurement Threshold

Service Name: Office Document Conversions Load Balancer Service

Monitored Process: Micorsoft.Office.Server.conversions.LoadBalancer.exe

Policy Name: **MSES_MOSS-2k7_Logging_Process_WSSTRACING**

Description: Collets data for the WSSTRACING process

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Measurement Threshold

Service Name: Windows SharePoint Services Tracing

Monitored Process: wsstracing.exe

Policy Name: **MSES_MOSS-2k7_Logging_Process_SPWRITER**

Description: Collets data for the SPWRITER process

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Measurement Threshold

Service Name: Windows SharePoint Services VSS Writer

Monitored Process: spwriter.exe

Policy Name: **MSES_MOSS-2k7_Logging_Process_WSADMIN**

Description: Collects data for WSADMIN process

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Measurement Threshold

Service Name: Measurement Threshold

Monitored Process: wssadmin.exe

Policy Name: **MSES_MOSS-2k7_Logging_Process_OWSTIMER**

Description: Collects data for the OWSTIMER process

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Measurement Threshold

Service Name: Windows SharePoint Services Timer

Monitored Process: owstimer.exe

Policy Name: **MSES_MOSS-2k7_Logging_Process_MSSEARCH**

Description: Collects data for MSSEARCH process

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Measurement Threshold

Service Name: Windows SharePoint Servicer Search

Monitored Process: mssearch.exe

Policy Name: **MSES_MOSS-2k7_Logging_Process_w3wp**

Description: Collects data for w3wp process

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Measurement Threshold

Service Name: Windows IIS worker process

Monitored Process: w3wp.exe

Policy Name: **MSES_MOSS-2k7_ Logging_Process_SSOSRV**

Description: Collects data for the SSOSRV process

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Measurement Threshold

Service Name: Microsoft Single Sign-on Service

Monitored Process: ssosrv.exe

Policy Name: **MSES_MOSS-2k7_Logging_Process_ MOSS.Conversions.Launcher**

Description: Collects data for conversions.Launcher process

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 5 minutes daily.

Policy Type: Measurement Threshold

Service Name: Office Document Conversions Launcher Service

Monitored Process: Microsoft.Office.Server.Conversions.Launcher.exe

Policy Name: **MSES_MOSS-2k7_ CreateCodeDataSources**

Description: Creates a code data source for MOSS services

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 30 minutes daily.

Policy Type: Scheduled task

Service Name: Office Document Conversions Launcher Service

Monitored Process: Microsoft.Office.Server.Conversions.Launcher.exe

Service Monitoring

Policy Name: **MSES_MOSS-2k7_Database_Monitoring**

Description: Checks the status of the MOSS database instances

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 30 minutes daily.

Policy Type: Scheduled task

Policy Name: **MSES_MOSS-2k7_ Logical Services_Monitoring**

Description: Checks the status of the MOSS logical services

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 30 minutes daily.

Policy Type: Scheduled task

Policy Name: **MSES_MOSS_Documents Delayed Retry**

Description: Monitors the Documents Delayed Retry counter

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: Every 20 minutes daily.

Policy Type: Measurement Threshold

Application

Policy Name: **MSES_MOSS_FwdApplicationInformation**

Description: Handles informational information from all sharepoint services

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: N/A

Policy Type: Windows Event Log

Policy Name: **MSES_MOSS_FwdApplicationWarning**

Description: Handles the warning messages from all sharepoint services

Policy Group: SPI for MSES > en > Sharepoint Portal Server > Microsoft Office Sharepoint Server 2007

Default Schedule: N/A

Policy Type: Windows Event Log

MOS 2007 reports

Memory and CPU reports

These reports can be used to plan and predict capacity of SharePoint Portal Server deployment. They can assist determining whether an additional search server or Web front end server needs to be added to improve performance.

> **NOTE:**
> Deploy the WINOSSPI-WINOS_Win2k_Logging policy for these reports to function correctly.

Daily/Weekly CPU Usage Summary
(g_MOSS2k7CPUSummary.rpt/g_MOSS2k7CPUWeeklySummary.rpt)

This report shows summary CPU statistics of MOSS 2007 server's services installed nodes in an enterprise deployment. The displays for every six hours over the last 7 days, compared with overall CPU statistics of the system, in both graphical and tabular format. This report can help administrators see which server is heavily loaded and which process is causing so much load.

Daily/Weekly Memory Usage Summary (g_MOSS2k7MemorySummary.rpt/ g_MOSS2k7MemoryWeeklySummary.rpt)

This report shows summary CPU statistics of MOSS 2007 server's services installed nodes in an enterprise deployment. The data displays for every six hours over the last 7 days, compared with overall CPU statistics of the system, in both graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the services.

IIS Worker Process reports

Weekly Summary of IIS Worker Process CPU Usage (g_MOSS2k7_IIS_CPUWeeklySummary.rpt)

This report shows the size of each index, total free space, and total used space left on each of the SharePoint Portal Server 2003 Indexing servers. The report shows data points, and charts for every 12 hours in each day over the past seven days.

> **NOTE:**
> Deploy the WINOSSPI-IISCollector and NET_SPS_Logging policies for this report to function correctly.

Related Topics:

- MOSS 2007 graphs

MOSS 2007 graphs

The following predefined graphs for SharePoint Portal Servers are available with the Microsoft Enterprise Servers SPI:

SharePoint Server Admin service CPU usage (2007)

This graph shows summary CPU statistics of the SharePoint admin service process (spsadmin.exe). This data can be compared with System Processor Time to determine to what extent the SharePoint admin service is utilizing processor time.

SharePoint Portal Server Admin service Memory usage (2003 and later)

This graph shows summary memory statistics of the SharePoint admin service process (spsadmin.exe). The summarized process statistics show private bytes, and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set

SharePoint Portal Server Search Service CPU usage

This graph shows summary CPU statistics of the SharePoint search service process (mssearch.exe). This data can be compared with System Processor Time to determine to what extent the SharePoint admin service is utilizing processor time.

SharePoint Portal Server Search Service Memory usage

This graph shows summary memory statistics of the SharePoint search service process (mssearch.exe). The summarized process statistics include the private bytes, and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set

SharePoint Search Service Page Faults/sec

This graph shows summary memory statistics of the SharePoint Search service process (mssearch.exe). The summarized process statistics include the Page Faults\sec by the process.

Counters:

- Process:Page Faults\sec

SharePoint Portal Server SingleSignon Service CPU usage (2007)

This graph shows summary CPU statistics of the SharePoint Single sign on service process (SSOSRV.exe). This data can be compared with System Processor Time to determine to what extent the SharePoint Single sign on service is utilizing processor time.

SharePoint Portal Server SingleSignon Service Memory usage (2007)

This graph shows summary memory statistics of the SharePoint single sign on service process (SSOSRV.exe). The summarized process statistics include the private bytes, and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set

SharePoint Portal Server SPTimer Service CPU Usage (2007)

This graph shows summary CPU statistics of the SharePoint SPTimer service process (OWSTIMER.exe). This data can be compared with System Processor Time to determine to what extent the SharePoint SPTImer service is utilizing processor time.

SharePoint Portal Server SPTimer Service Memory usage (2007)

This graph shows summary memory statistics of the SharePoint SPTimer service process (OWSTIMER.exe). The summarized process statistics include the private bytes and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set, Process

IIS Worker process CPU usage (2007)

This graph shows summary CPU statistics of the IIS worker process service (w3wp.exe). This data can be compared with System Processor Time to determine to what extent the IIS worker process service is utilizing processor time, which can be used in making decisions about whether to add additional web front end servers.

IIS Worker process Memory usage (2007)

This graph shows summary memory statistics of the IIS worker process service (w3wp.exe). The summarized process statistics include the private bytes and working set used by the process.

Counters:

- Process.Private Bytes
- Process.Working Set.

IIS Worker processes Page Faults (2007)

This graph shows summary memory statistics of the IIS worker process service (w3wp.exe). The summarized process statistics include the Page Faults\sec by the process.

Counters:

- Process:Page Faults\sec

Related Topics:

- MOSS 2007 reports

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback: