

Microsoft® SharePoint® Foundation 2010 Management Pack Guide
for System Center Operations Manager 2007 SP1

Microsoft Corporation

Copyright © Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility. By using or providing feedback on this documentation, you agree to the license agreement below.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, SharePoint, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries/region.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[Quick Start 1](#_Toc246932811)

[Files included in this Management Pack 5](#_Toc246932812)

[Frequently Asked Questions and Known Issues 5](#_Toc246932813)

[Microsoft SharePoint Foundation 2010 Management Pack for Operations Manager 2007 SP1 13](#_Toc246932814)

[Requirements for Microsoft SharePoint Foundation 2010 Management Pack 14](#_Toc246932815)

[Prerequisites for Using the Management Pack 14](#_Toc246932816)

[Security Considerations for the Microsoft SharePoint Foundation 2010 Management Pack 15](#_Toc246932817)

[Configure the SharePoint Discovery/Monitoring Account Run As Profile 15](#_Toc246932818)

[Support for Agentless Monitoring 19](#_Toc246932819)

[Getting Started with the Microsoft SharePoint Foundation 2010 Management Pack 19](#_Toc246932820)

[Import the Management Pack into Operations Manager 2007 SP1 20](#_Toc246932821)

[Deploy and Configure Servers for the Operations Manager 2007 SP1 Agent 21](#_Toc246932822)

[Resize the Agent Event Logs 21](#_Toc246932823)

[Disable Event Log Replication for Monitoring Clustered Servers 22](#_Toc246932824)

[Optional Configuration for the Microsoft SharePoint Foundation 2010 Management Pack 22](#_Toc246932825)

[Customize the Management Pack 23](#_Toc246932826)

[Disable a Monitor or Rule 28](#_Toc246932827)

[Understanding the Microsoft SharePoint Foundation 2010 Management Pack Operations 28](#_Toc246932828)

[Objects the Microsoft SharePoint Foundation 2010 Management Pack Discovers 29](#_Toc246932829)

[Understanding Health Monitoring 29](#_Toc246932830)

[About the Microsoft SharePoint Foundation 2010 Management Pack Monitors 29](#_Toc246932831)

[How Health Rolls Up 33](#_Toc246932832)

[How Health Is Indicated in the Operations Console 33](#_Toc246932833)

[Key Monitoring Scenarios 35](#_Toc246932834)

[Understanding Rules 36](#_Toc246932835)

[Understanding Tasks: 36](#_Toc246932836)

[Viewing Information in the Operations Console 39](#_Toc246932837)

[About the Operations Manager 2007 SP1 Operations Console 39](#_Toc246932838)

[Viewing Status and Performance Data in the Monitoring Pane 39](#_Toc246932839)

[Viewing Management Pack Views in the Authoring Pane 41](#_Toc246932840)

[Viewing Management Pack Rules in the Authoring Pane 42](#_Toc246932841)

[Viewing Management Pack Object Discoveries in the Authoring Pane 43](#_Toc246932842)

[Using the Microsoft SharePoint Foundation 2010 Management Pack Reports 46](#_Toc246932843)

[Selecting a Report 47](#_Toc246932844)

[Report Descriptions 47](#_Toc246932845)

# Quick Start

**Required Updates and Hotfixes**

Please ensure that all applicable updates are applied to your environment.

If any of your System Center Operations Manager servers or agent computers are running on Windows Server 2008 based computers, refer to this article: <http://support.microsoft.com/kb/953141>

Apply all applicable updates in the list below:

<http://support.microsoft.com/kb/954049>

<http://support.microsoft.com/kb/951327>

<http://support.microsoft.com/kb/952664>

<http://support.microsoft.com/kb/951116>

<http://support.microsoft.com/kb/953290>

<http://support.microsoft.com/kb/951526>

Also, please refer to this list of issues that were fixed in Operations Manager 2007 R2. If you are running Operations Manager 2007 SP1, some or all of these updates maybe applicable to your environment:

<http://support.microsoft.com/kb/971410>

It is strongly recommended that Windows Server 2008 Service Pack 2 or later would be the operating system where System Center Operations Manager is installed.

**Get started**

This section provides instructions for setting up the environment, importing management packages and configuring the system for monitoring using Operations Manager 2007 SP1.

1. Setup the System Center Operation Manager 2007 SP1 servers. For more information about installing and configuring Operations Manager 2007, see the Operations Manager 2007 Deployment Guide deployment guide at <http://technet.microsoft.com/en-us/library/bb419281.aspx>.
2. Identify all of the servers in the farm. You can identify all of the servers in the farm by using the Central Administration Web site. If your installation of SharePoint fails to install components on a particular server, it is recommended you troubleshoot the server or remove the server from the farm so the server does not appear in Central Admin; failing to do so may add complications in the management pack discovery.  **Note:** If discovery misses any server in the branch, discovery or monitoring may not function correctly.
3. Install Operations Manager 2007 agent on servers identified in step 2 by running the Operations Manager 2007 Discovery Wizard. It is recommended that you install the agent by adding computers to agent managed through Operations Manager 2007 console. For more information about installing Operations Manager 2007 agents, see the Operations Manager 2007 Deployment Guide at <http://technet.microsoft.com/en-us/library/bb419281.aspx>.

**Note**: If an agent is already installed on the farm computers, you can skip this step.

1. Configure Operations Manager 2007 alert notification – refer to the general guideline from Operations Manager 2007 guide.
2. We recommended that you import and configure the Windows Server Operating System, SQL Server, and Windows Server Internet Information Services (IIS) Management Packs according to the Management Pack guides. These Management Packs are available at http://www.microsoft.com/technet/prodtechnol/scp/catalog.aspx. Ensure that you are using the matching Management Packs for Windows 2008 and Windows 2008 R2.
3. Download and install the Microsoft SharePoint Foundation 2010 Management Package.

**Note:** If the server where the Management Pack installation file is downloaded to runs a 64-bit version of Windows, the Management Pack gets installed to %ProgramFiles(x86)% folder by default.

**Note:** If you are reinstalling a newer version of this Management Pack, rename your existing SharePointMP.Config to SharePointMP-OLD.Config before installing the latest version in order to save your existing changes and overrides to the SharePointMP.Config. Once the newer version of the config file is installed, copy over any custom changes made in SharePointMP-OLD.Config to the newer SharePointMP.Config file.

1. Ensure that the following files are in the “%ProgramFiles%\System Center Management Packs” folder on your Operations Manager 2007 management server:
	* Microsoft.SharePoint.Foundation.2010.mp
	* SharePointMP.Config
2. In the Operations Manager 2007 console, import the Microsoft SharePoint Foundation 2010 Management Package
3. On the Operations Manager 2007 management server, open the Operation Console
4. On the Administration tab, expand Management Packs.
5. Right click the Management Packs node and select Import Management Packs.
6. Go to “%ProgramFiles%\System Center Management Packs” and select Microsoft.SharePoint.Foundation.2010.mp
7. Click Import and then Close.
8. Create a Run As account for Microsoft SharePoint Foundation 2010 discovery and monitoring in Operations Manager 2007 console
9. On the Operations Manager 2007 management server, open the Operation Console
10. On the Administration tab, expand Management Packs.
11. On the Administration tab expand the Security node and right-click **Run As Accounts**, and select **Create Run As Account**.
12. Follow the wizard to create the Run As account and record the account display name which is going to be used in the SharePointMP.config file as described in next step. You can name your Run As account “SharePoint Discovery/Monitoring Account” to avoid updating SharePointMP.config in next step.

**Note**: the Run As account must have sufficient privilege to allow discovery and monitoring to run. We recommend using the account which is a member of the Farm Administrator SharePoint group and is a member of the Administrators group on the database server hosting the SharePoint farm databases and access to all SharePoint databases. Usually the account used to run SharePoint 2010 Product Configuration Wizard has the required privileges.

1. Run the Admin task on Operations Manager 2007 management server to configure Microsoft SharePoint Foundation 2010 discovery and monitoring:
2. Update the SharePointMP.config file with the correct information
3. Open SharePointMP.config file under “%ProgramFiles%\System Center Management Packs”
4. Find the section as below and update the account with the one you created in last step. Also add all computers in the farm for monitoring. For detailed information, please follow the instruction in SharePointMP.config. Ensure all computers that have SharePoint Foundation 2010 installed are included through the regular expression filter that is the value of the Name attribute of the Machine element in the SharePointMP.config file.

|  |
| --- |
| <Association Account="**DisplayName** of RunAS account" Type="Agent"> <Machine Name="agentMachineFilter1" /> <Machine Name="agentMachineFilter2" /> …</Association> |

**Note:** The default value "" of Name attribute matches all agent managed computers. If a computer is included that does not have any SharePoint components, the side effect is that some registry checks will run on it to determine whether it has SharePoint installed on not.

1. Run Admin task to configure the discovery and monitoring
2. On the Operations Manager 2007 management server, open the Operations Console
3. On the Monitoring tab
4. Go to Monitoring **SharePoint 2010 Products** folder (expand it if needed)
5. Click on **Administration** node under SharePoint 2010 Products folder
6. Go to Actions Menu in the toolbar  Microsoft SharePoint 2010 Farm Group Tasks  Configure SharePoint Management Pack
7. Ensure the the SharePointMP.config file is at the right location. Click **Run.**

**Note -** The task will take a few minutes to complete.

1. Close the dialog if there is no error.

If the task succeeds with no errors, then proceed to the next step. Otherwise, fix the problem and rerun the task until it completes with no errors.

**Note:** You can perform this task by usingWindows PowerShell. For more information about using Windows PowerShell to perform this task, see the help for the “Get-Task” and “Start-Task” comdlets by starting the Operations Manager PowerShell console from the Start menu or from %ProgramFiles%\System Center Operations Manager 2007\Microsoft.EnterpriseManagement.OperationsManager.ClientShell.Console and typing “Get-Help Get-Task -full” or “Get-Help Start-Task -full”.

1. After the previous step is completed wait for about half an hour to an hour to allow the discovery process to complete.
2. Verify discovery results.
3. Open the Operations Manager 2007 console,
4. Go to the **Monitoring** tab (bottom left)
5. Go to the SharePoint 2010 Products folder (expand it if needed)
6. Click the **Diagram View** node
7. Expand the diagram view and review with your SharePoint administrator to see if all services that have been provisioned are discovered, if not, check FAQ to see if this a know issue and what is the workaround, if there is none, please retry.

You have completed setting up Operations Manager 2007 to monitor the SharePoint farm.

**Note**: After completing the configuration, monitor your farm for alerts. You must reset some alerts manually after its status has changed to **Critical**. Otherwise, the monitor will remain in a **Critical** state without sending out new alerts.

# Files included in this Management Pack

* Microsoft.SharePoint.Foundation.2010.mp
* Microsoft SharePoint Foundation 2010 Management Pack Guide.docx
* Microsoft SharePoint Foundation 2010 Management Pack Readme.htm
* SharePointMP.config
* EULA.RTF

# Frequently Asked Questions and Known Issues

* **How many farms can I monitor from one set of Operations Manager 2007 servers?**

We recommend having one set of Operations Manager 2007 servers monitor only one SharePoint farm.

We do not recommend having multi-homed agent computer (SharePoint servers that are monitored in multiple Operations Manager 2007 management groups).

* **Is this Management Pack supported for both Operations Manager 2007 SP1 and Operations Manager 2007 R2?**

Yes, this Management Pack is supported in both Operations Manager 2007 SP1 and Operations Manager 2007 R2.

* **Why did the administration task not run successfully after system setup?**

You must restart the Operations Manager 2007 RMS and Management Servers at least once after you configure them for the administration task to run successfully.

* **Why do I not see the SharePointMP.config file on the 64-bit version of Windows Server 2008?**

On the 64-bit version of Windows Server 2008, the SharePointMP.config file is installed in the “%ProgramFiles(x86)%\System Center Management Packs” folder. You must copy the file to the “%Program Files\System Center Management Packs” folder before running the administration task. Otherwise, administrators will see the "Failed to load configuration file" error during management pack configuration

* **Why do components get discovered even after removing them?**

This might be caused by a caching problem. Upgrading or importing a new management pack, with changed monitoring classes properties may result in unexpected discovery results. This may occur when importing a new version of the management pack after importing the Technical Preview or Beta versions. It happens because old classes are still in cache. For more information about clearing the cache by using the clearcache switch with Microsoft.MOM.UI.Console.exe, see the Operations Manager 2007 documentation.

* **Does this management pack include the management packs for other Microsoft technologies?**

No. This management pack does not include monitors or rules for the Windows Operating System, SQL Server or Internet Information Services (IIS)**.** We recommend that you install these management packs to help monitor the services running on the agent computers. These management packs are available at <http://technet.microsoft.com/en-us/opsmgr/cc539535.aspx>

* **Is it possible to override monitor parameters for a specific instance?**

If a monitor is implemented as [cook down](http://www.authormps.com/dnn/Concepts/WorkflowBasics/CookDown/tabid/117/Default.aspx) monitor, overriding a parameter will apply to all instances it targets. User can not override a parameter that targets on only a specific instance.

Affected monitors in this management pack are:

* SPHA Availability Rule Monitor
* SPHA Configuration Rule Monitor
* SPHA Performance Rule Monitor
* SPHA Security Rule Monitor
* SPHA Custom Rule Monitor
* SPHA Availability Rule Monitor on SPServer
* SPHA Configuration Rule Monitor on SPServer
* SPHA Performance Rule Monitor on SPServer
* SPHA Security Rule Monitor on SPServer
* SPHA Custom Rule Monitor on SPServer
* **How do I get additional information on an alert?**

If an alert is triggered and you want to find additional information on top of the notification and alert description you could check out the health explorer. Here are the steps.

1. Start the Operations Console.
2. On the **Monitoring** tab, select the **Active Alerts** node.
3. In the right pane, right-click the individual alert that you want to view, select **Open**, and then **Health Explorer.**
4. In the **Health Explorer** window, select the individual failure that you want to view.
5. On the **State Change Events** tab, view the **Details** section for description and event data.
* **If new agent computers are added to the SharePoint farm, do I have to rerun the SharePointMP.config file?**

Yes.

* **What happens to repeated events monitors if Event Log Flood Protection is on?**

If Event Log Flood Protection is enabled, repeated events monitors may not behave as expected. Repeated event monitors are designed to trigger if certain event gets logged for a specific number of times in a given time period. By default, suppression starts after five of the same event IDs are logged within two minutes. The first five events are written to the event log. Once an event starts flooding the log, a summary event (such as *ULSFloodedEventSuppressedCritical*) is logged every five minutes. The summary event has its own ID that is monitored separately.

* **Why is an Operations Manager 2007 event 2023 appearing on the Operations Manager 2007 agent computer?**

If you see this event with the message “The health service has removed some items from the send queue for management group ‘contoso-SCOM management group‘ since it exceeded the maximum allowed size of 15 megabytes.”, clear the cache on the agent computer by performing the following steps

1. Stop the OpsMgr health service.
2. Navigate to the %ProgramFiles%\System Center Operations Manager 2007\Health Service State\Health Service Store folder and delete all files in that folder.
3. Restart the OpsMgr health service.

**Note**: You must clear the cache. Restarting the agent health service or repairing the agent by using Operations Manager 2007 will not fix this problem.

* **How do I monitor a Web application or a site?**

For more information about monitoring a Web application or a site, see How to Create a Web Application Monitor (<http://technet.microsoft.com/en-us/library/bb381370.aspx>).

**Note**: If the SQL Server management pack is also installed for monitoring the database server there is a possibility of some redundant alerts being generated. To avoid redundant alerts, follow these steps:

1. Open the Operations Console.
2. in the **Authoring** tab, expand **Management Pack Objects** and click **Monitors.**
3. Click **Change Scope…**
4. Select **View all targets**, click **Select All,** and then click **OK.**
5. Type “Auto Update Flag” in the **Look for** textbox, and then click **Find Now**.
6. If both the SQL 2005 and 2008 management pack are installed two same targets will be listed. Disable the rule that corresponds to the version of SQL Server that SharePoint is not using.
7. Right-click on “Auto Update Flag”, select **Overrides**, and then select **Override the monitor** for all objects of type: SQL <2005/2008> DB.
8. Select the **Generates Alert and set Override Setting to False** check box.
9. Under **Select destination management pack** select Microsoft.SharePoint.Foundation.2010.Override, and then click **OK**.
10. Repeat step 6 to 10 and change “Auto Update Flag” to “Auto Create Statistics Flag”.
* **Why do I see two alerts for some Service Monitors?**

There are two Monitors created for the following Services:

* - SPAdminV4
* - SPSearch4
* - SPTimerV4
* - SPUserCodeV4
* - SPTraceV4
* - OSearch14

One of the monitors is an Operations Manager 2007 monitor. The other monitor is a SharePoint Health Analyzer (SPHA) rule monitor. If you want to have only one alert per service application, you must disable the SPHA rule for each service by using the Central Administration Web site. Doing this will stop the SPHA rule monitor from raising alerts (**Note**: you will still receive alerts from the Operations Manager 2007 monitor).

* **Why did the ‘Ping Web Application Failed’ monitor fail upon installing the Management Pack?**
The ‘Ping Web Application Failed’ monitor is not technically a network ping, it is a monitor that attempts to access the Web application default URL through a HTTP GET request; if your System Center Operations Manager Console computer prohibits access to HTTP REQUESTS, this monitor will always be in an unhealthy state.
If this happens, we recommend that you disable this monitor using the System Center Operations Manager Console

To disable this monitor, follow these steps:

1. Open the Operations Console.
2. In the **Authoring** tab , expand the **Management Pack Objects** node and select the **Monitors** node.
3. In the right pane, type ‘Ping Web Application Failed’ in the search field.
4. Doubleclick the **Ping Web Application Failed** Monitor.
5. In the **Overrides** tab, click **Disable**, and select **For all objects of type.**
* **What is SyncTime?**

SyncTime (start time) is a property of discoveries and monitors. SyncTime is a string value in the format of "HH:mm". SyncTime, IntervalSeconds and Management Pack Import time together determine the exact run time of a given workflow.

For example, if IntervalSeconds = 21600 (6 hours) and SyncTime = "01:15", the possible run time of the workflow is 1:15AM, 7:15AM, 1:15PM, 7:15PM; if the Management Pack is imported after 1:15AM but before 7:15AM, it will start at 7:15AM, if the Management Pack is imported after 1:15PM but before 7:15PM, it will start at 7:15PM. However, due to other factors such as network delay the actual start time may still vary. Do not change the default SyncTime value unless absolutely required.

###### Issues

* **Issue:** An *Import* level error occurs if you import the management pack when you have the Technical Preview or Beta management pack installed. **Resolution:** remove or uninstall the Technical Preview or Beta management pack before importing the RTM management pack.
* **Issue:** Performance data is not available in the Performance View and Report, or a Operations Manager 2007 event 10102 or 10103 is raised with the message “In PerfDataSource, could not resolve (or find) counter xxx”, and the module will be unloaded. **Resolution:** Because all SharePoint performance counters are dynamic counters, currently there is a bug in Operations Manager 2007 on collecting data for such counters. Operations Manager 2007 has hot fixes for SP1 and R2. For more information about these fixes, see the Microsoft Support article: http://support.microsoft.com/kb/953141.
* **Issue:** When Operations Manager 2007 is monitoring multiple language Agents, the first event in the system for an event, alert, or rule will set the description language context. The Operations Manager 2007 cache will keep that context. **Resolution:** The work-around for this issue is to restart the Health Service on the agent that the user would like to set the event description language, and make sure that the event is fired from this agent first.
* **Issue:** When the override-controlled parameter “Count” is set to “1” for repeated-event type monitors, the new value will not work and the monitor will fail to change the health state. **Resolution:** This is a known Operations Manager 2007 issue. There is no resolution at the time of writing this document.
* **Issue:** The monitor “SQL Database Connection Failed” is used to ping databases, but does not work for stand-alone SharePoint deployments. (This monitor is disabled by default). **Resolution:** The stand-alone server is using SQL Server Express, in which remote access is disabled by default. This means that Rights Management Services (RMS) cannot ping the database. To enable this monitoring for the stand-alone deployment, change the SQL Server setting to enable remote access. For more information about this, see the Microsoft Support article How to configure SQL Server 2005 to allow remote connections (<http://support.microsoft.com/kb/914277>).
* **Issue**: The computer appears in the “Unidentified Machines” view in the Operations Manager 2007 console. When a computer is under “Unidentified Machines” view, it means that the discovery process could not identify the SharePoint farm to which this computer belongs. A computer can be in the “Unidentified Machines” view for one or more of the following reasons:
* The computer cannot access the SharePoint configuration database
* SharePoint Foundation 2010 is not installed on this computer
* The server configuration failed
* The Agent proxy is not enabled in Operations Manager 2007 for that server
* The Operations Manager 2007 agent has a heart beat failure preventing it from communicating with the Operations Manager 2007 RMS. In this case, the computer icon appears as a gray circle in Operations Manager 2007 Console.
* There is network connectivity issue
* SharePoint Foundation 2010 could not connect to the configuration or the database server
* The Run As account used for discovery or monitoring does not have permission to access the SharePoint Object Model. To find if this is the issue, run the “Set DebugTrace For SharePoint Management Pack” task (for information in the “Understand Tasks” section of this guide), rerun the Admin Task, and then go to Operations Manager Event channel on the server and check events with ID = 0. Look for the timestamp in the event log and then check the SharePoint ULS trace log to ensure that it is the case. For more information about the ULS trace log, see the SharePoint Foundation 2010 documentation on TechNet (<http://technet.microsoft.com/en-us/sharepoint/ee263910.aspx> ).
* The agent is being associated with the SharePoint Run As Profile during the SharePoint Foundation 2010 Discovery cycle interval.
* The main server (the server on which most of the discovery scripts run) is not associated with the SharePoint discovery/monitor Run As profile. In this case all the servers that were supposed to discover using these scripts will end up in the unidentified group.
* If the agent computer is a new server added to the farm after the last discovery, it will be in unidentified group until the next farm discovery. On-demand discovery is not supported in this version of Operations Manager 2007.
* **Issue:** If you add a SPHA Rule by using the Central Administration Web site the management pack interprets this rule as a ‘null-HealthRuleType’ and is unable to monitor the SPHA rule. **Resolution:** Create the custom SPHA rule by adding it through the SharePoint API by manually coding the SPHA Rule.
* **Issue:** The **c**omputer is not showing up in the System Center Diagram View. **Resolution:** Investigate the following possible causes:
* The computer has run out of resources (RAM, CPU)
* The computer has a communication issue with the Operations Manager 2007 Server
* The computer has not been restarted since Windows PowerShell was installed. Restart the computer and rerun the task.
* The computer joined the farm after the SharePoint task has finished running. Either wait for the next farm discovery cycle or rerun the task.

# Microsoft SharePoint Foundation 2010 Management Pack for Operations Manager 2007 SP1

The Microsoft SharePoint Foundation 2010 Management Pack for Operations Manager 2007 SP1 helps you manage Microsoft® Windows® SharePoint® Foundation 2010 environments.

The highly collaborative environment provided by SharePoint Foundation 2010 offers rich support for working across organizational and geographical boundaries. The groups who perform this work have spurred its adoption, quickly recognizing it as a solution for collaboration challenges. This management pack facilitates management of identified environments by monitoring the health of the components of these environments that affect performance and availability. The monitored components include:

* SharePoint Foundation 2010 -related services (Timer, Tracing, and Search)
* SharePoint Foundation 2010 -related events
* Internet Information Services-related events (Only events emitted from SharePoint Application not from IIS)
* Microsoft SQL Server™ database-related events (Only events emitted from SharePoint Application not from SQL Server)
* SharePoint Foundation 2010 server performance.

When there is a problem that may cause a service outage or poor performance, Microsoft System Center Operations Manager 2007 SP1 uses the management pack to detect the issue and alert you so that you can diagnose and fix the issue.

For example, if the management pack detects that the SharePoint Foundation 2010 Search service cannot update an index because there is insufficient drive space, a monitor changes state to Critical and raises an alert in Operations Manager 2007. You can then use the **Alerts** view to determine which server has insufficient disk space. After you determine this, you can delete files from the drive or move the index files to another drive.

# Requirements for Microsoft SharePoint Foundation 2010 Management Pack

This section explains the prerequisites that are necessary for you to use the Microsoft SharePoint Foundation 2010 management pack, and describes some important security considerations of which you should be aware.

## Prerequisites for Using the Management Pack

To use this management pack, you must:

* Download the management pack from the [System Center Pack Catalog](http://technet.microsoft.com/en-us/systemcenter/cc462790.aspx) (http://technet.microsoft.com/en-us/systemcenter/cc462790.aspx).
* Have System Center Operations Manager 2007 SP1 deployed in at least one Management Group. A Management Group consists of an Operations Manager 2007 SP1 database, at least one Operations Manager 2007 SP1 Management Server, the Operations Manager 2007 SP1 Operator Console, and managed computers.
* Have the Operations Manager 2007 SP1 agent deployed on all computers that you want to monitor.
* If an agent computer in a SharePoint deployment is running Windows Server 2008, ensure that all the hotfixes mentioned in the Microsoft Support article (<http://support.microsoft.com/kb/953141/en-us>) are installed on these computers.

For information about deploying Operations Manager 2007 SP1, see the *Operations Manager 2007 SP1 Deployment Guide* at <http://technet.microsoft.com/en-us/library/bb419281.aspx>.

For information about how to deploy the Operations Manager 2007 SP1 agent, see “How to Deploy the Operations Manager 2007 SP1 Agent for Agent-Management of Computers” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb309622.aspx>.

## Security Considerations for the Microsoft SharePoint Foundation 2010 Management Pack

This section covers security considerations for the management pack. To use this management pack correctly, you must know:

* How to configure the **SharePoint Discovery/Monitoring Account** Run As profile with Run As accounts that have the correct privileges.
* Whether the management pack provides support for agentless monitoring.

### Configure the SharePoint Discovery/Monitoring Account Run As Profile

The rules, monitors, tasks and discoveries that are defined in the management pack require credentials to run on a computer. By default, these credentials come from the Default Action Account on each server that has the Operations Manager 2007 SP1 agent installed on it.

Note

The agent is an Operations Manager 2007 SP1 service that runs on each computer that you want to monitor. It captures information from the computer on which it is running, applies rules to the captured data, and performs actions as defined by the rules.

The Default Action Account runs activities such as monitoring and collecting Windows event log data and performance data.

Because the Default Action Account may not have the necessary privileges to accomplish the monitoring activities of the management pack, Operations Manager 2007 SP1 allows you to use Run As profiles and Run As accounts to provide the needed credentials.

When a management pack is created, its discoveries, rules, monitors, and tasks are associated with Run As profiles; the management pack discoveries, rules, monitors and tasks are associated with the **SharePoint Discovery/Monitoring Account** Run As profile.

Run As accounts allow you to specify the necessary privileges to run the management pack discoveries, rules, monitors, and tasks on specific computers. As an administrator, you can associate Run As accounts with Run As profiles to provide the necessary credentials to run the management pack discoveries, rules, monitors, and tasks.

In order for the management pack to have the necessary credentials to run its rules, monitors, and tasks, you must make the following configuration:

**Configuring the management pack**

Create a “SharePoint Discovery/Monitoring Account” Run As Account (pick the DisplayName for the account listed in this config file) that is associated with a user account that has SharePoint 2010 farm administrative privileges and access to the related databases and application programming interface (API). For example, the account used to setup SharePoint Foundation 2010 and run the SharePoint Products and Technologies Configuration Wizard should have the required privileges.

**Automatic:**

This is one significant change from Microsoft SharePoint Services 3.0 management pack. The Microsoft SharePoint Foundation 2010 management pack installs a configuration file (SharePointMP.config) that allows user to configure the management pack by running a task.

**Note:** Ensure that the SharePointMP.config file is located at %ProgramFiles%\System Center Management Packs\ on the Operations Manager 2007 Root Management Server.

SharePointMP.config Contents:

 <?xml version="1.0" encoding="utf-8"?>

<Configuration>

 <Annotation>

 This is the configuration file for the admin task in Microsoft SharePoint Foundation 2010 Management Pack.

 To run the task, save this file on the Root Management Server machine under %ProgramFiles%\System Center Management Packs

 </Annotation>

 <Annotation Element="Association">

 Association element specifies account association. You can have 0, 1, or many Association elements.

 - The Account attribute specifies what RunAs account to be associated. The account must exist before running the admin task.

 RunAs account can be created in the Administration pane of the Operations Console.

 - The Type attribute may have one of two values: "Agent" and "ManagementServer". "Agent" indicates that the account applies to

 agent managed machines. "ManagementServer" indciates that the account applies to management servers.

 - Each Machine node serves as a machine filter. Machine that matches any filter will be associated with the account in the profile.

 - The Name attribute of Machine node holds a regular expression value on full machine name. Go to http://www.bing.com and search for

 "Regex Tutorial" to learn more about regular expression. If you leave the Name attribute empty, all of machines (agent managed or

 management server depending on the type) match.

 - For "Agent" type, discovery proxy is also enabled on the matched machines so that farm level discoveries can work correctly.

 </Annotation>

 <Association Account="SharePoint Discovery/Monitoring Account" Type="Agent">

 <Machine Name="" />

 </Association>

 <Annotation Element="WorkflowCycle">

 WorkflowCycle element specifies the schedule of list workflows. You can have 0, 1, or many WorkflowCycle elements. But if you

 have multiple WorkflowCycle elements, you should avoid listing the same workflow in different WorkflowCycle elements.

 - The BaseStartTime attribute can have value in the form of "HH:mm" or integer. "HH:mm" format works as the start time alignment based on which

 the cycle repeats. Integer format functions as setting the alignment start time to be the current time plus that many seconds. Be aware that

 if you set integer value, every time you rerun the admin task, the cycle start time is recalculated.

 - The Length attribute specifies the length (in seconds) of each cycle.

 - The Spacing attribute specifies the spacing time (in seconds) between one workflow's timeout time and the next workflow's start time.

 For example, SPFarm.Discovery has timeout 300 and base start time at "14:00". If the Spacing is 60, the base start time of SPService.Discovery

 is set to 14:00 + Ceiling[(300 + 60) / 60] = 14:06. If you set negative Spacing, workflows may overlap and cause performance and out of memory problems.

 - The WorkflowTimeout attribute (optional) if defined applies to each workflow in the cycle unless being overridden in the Script node.

 If not set, current timeout values are respected.

 - The Id attribute of Workflow node is a list of the discovery/monitor Id(s) separated by ';' (for the workflow).

 - The MP attribute (optional) of Workflow node is for workflow not defined in the SharePoint Foundation MP.

 - The Type attribute of Workflow node indicates the workflow type. Only "Discovery" and "Monitor" are supported.

 - The Times attribute of Workflow node specifies how many times the workflow needs to run within a cycle.

 If you set it to 0 or negative, the workflow is disabled.

 - The Timeout attribute (optional) of Workflow node if defined overrides the timeout of the workflow.

 </Annotation>

 <WorkflowCycle BaseStartTime="+300" Length="28800" Spacing="60">

 <Workflow Id="WSSInstallation.Discovery" Type="Discovery" Times="1" />

 <Workflow Id="SPFarm.Discovery" Type="Discovery" Times="1" />

 <Workflow Id="SPService.Discovery" Type="Discovery" Times="4" />

 <Workflow Id="SPSharedService.Discovery" Type="Discovery" Times="4" />

 <Workflow Id="SPHARule.Discovery" Type="Discovery" Times="1" />

 <Workflow Id="SPHARuleMonitor.Availability;SPHARuleMonitor.Security;SPHARuleMonitor.Performance;SPHARuleMonitor.Configuration;SPHARuleMonitor.Custom" Type="Monitor" Times="8" />

 <Workflow Id="SPHARuleMonitor.SPServer.Availability;SPHARuleMonitor.SPServer.Security;SPHARuleMonitor.SPServer.Performance;SPHARuleMonitor.SPServer.Configuration;SPHARuleMonitor.SPServer.Custom" Type="Monitor" Times="8" />

 </WorkflowCycle>

</Configuration>

**Note:** Ensure that you run the Admin Task after updating file,

For more information about Run As profiles and Run As Accounts, see:

* “Run As Profiles and Run As Accounts in Operations Manager 2007 SP1” at <http://technet.microsoft.com/en-us/library/bb309667.aspx>.
* “Running a Task, Rule, or Monitor with Run As in Operations Manager 2007 SP1” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb309594.aspx>.

### Support for Agentless Monitoring

The Microsoft SharePoint Foundation 2010 management pack does not contain rules for agentless monitoring.

# Getting Started with the Microsoft SharePoint Foundation 2010 Management Pack

To install the Microsoft SharePoint Foundation 2010 Management Pack, you must download the files to your management server and then import the management pack into Operations Manager 2007 SP1. After you import the management pack, you can create optional configurations for the Operations Manager 2007 SP1 agents on your SharePoint Foundation 2010 servers.

## Import the Management Pack into Operations Manager 2007 SP1

To import the Microsoft SharePoint Foundation 2010 management pack:

1. Log on to a management server with an account that is a member of the Operations Manager 2007 SP1 Administrators role for the Operations Manager 2007 SP1 Management Group.
2. In the Operations Console, click the **Administration** workspace button in the lower-left side of the console.
3. In the Administration tree view, right-click the **Management Packs** node, and then click **Import Management Packs**. The **Select Management Packs to import** dialog box appears.
4. If necessary, navigate to the directory where the Microsoft SharePoint Foundation 2010 management pack is located.
5. Select **Microsoft.SharePoint.Foundation.2010.mp**, and then click **Open**. The **Import Management Packs** dialog box opens.
6. Click **Import**. When the import process is complete, the dialog box displays an icon next to the management pack that indicates whether the import succeeded or failed.
7. Click **Close**. The **Management Packs** pane of the Operations Console now lists the Microsoft SharePoint Foundation 2010 management pack.

After importing the management pack, you must run the admin task to enable SharePoint farm discovery as described in the “Configure the SharePoint Discovery/Monitoring Account Run As Profile” section in this guide. You can also choose to customize or disable its rules. For information about how to customize the management pack or disable its rules, see the “Optional Configuration for the Microsoft SharePoint Foundation 2010 Management Pack” section in this guide.

## Deploy and Configure Servers for the Operations Manager 2007 SP1 Agent

It is important to ensure that the Operations Manager 2007 SP1 agent is deployed on each SharePoint Foundation 2010 server that you want to monitor. For information about how to deploy the agent, see “How to Deploy the Operations Manager 2007 SP1 Agent for Agent-Management of Computers” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb309622.aspx>.

To configure each server to use the Operations Manager 2007 SP1 agent with the Microsoft SharePoint Foundation 2010 Management Pack:

### Resize the Agent Event Logs

As a best practice, resize the agent event logs to at least 10 MB each for optimal monitoring. The Microsoft SharePoint Foundation 2010 management pack uses the following event logs to monitor the servers:

* Windows Application event log
* Microsoft SharePoint Foundation 2010\Operational event log

To resize the agent event logs:

1. On each server with an Operations Manager 2007 SP1 agent installed on it, open the Event Viewer.
2. In the Event Viewer console tree, click **Application** and on the **Action** menu, and then click **Properties**.
3. On the **General** tab, in **Maximum log size (KB)**, specify a log size of at least 10240 KB.
4. To apply the new setting, click **Clear Log**. If you want to retain the information that is currently in the log, click **Yes** when a message appears asking if you want to save the original log before clearing it.
5. Click **OK**.
6. Repeat the above process for the Microsoft SharePoint Foundation 2010 \Operational event log.

### Disable Event Log Replication for Monitoring Clustered Servers

Some SharePoint Foundation 2010 components can be installed on clustered servers. By default, when clustering is installed on servers that are running Windows 2008 Enterprise Server or Windows 2008 Datacenter, events logged in the event log of one node in the cluster are also shown in the event logs of the other nodes. To monitor these clustered servers using Operations Manager 2007 SP1, event log replication must be disabled on each of the servers within the cluster.

# Optional Configuration for the Microsoft SharePoint Foundation 2010 Management Pack

The management pack can be customized on each Operations Manager 2007 SP1 Server to focus its monitoring on specific aspects of the environment that are important to the administrator. You customize the management pack by using overrides to reconfigure the default settings of its rules or by disabling rules entirely.

In a large, dispersed network, you may have SharePoint Foundation 2010 deployed in a number of different Management Groups. Because each Management Group contains its own Operations Manager 2007 SP1 Management Server, you can install the management pack in each Management Group and customize it to focus on collecting only the information that is needed for that Management Group environment.

Imported management packs, including the SharePoint Foundation 2010 Management Pack, are *sealed*; therefore, overrides cannot be saved to them. Instead, Operations Manager 2007 SP1 saves the overrides to the unsealed default management pack, which is imported as part of the Operations Manager 2007 SP1 installation. Sealed management pack, have the file extension .mp. These are binary files that cannot be edited. Unsealed management pack, have the file extension .xml. These are XML files that can be edited.

It is a best practice to put overrides to a sealed management pack into a new unsealed management pack instead of the default management pack for the following reasons:

* It simplifies the process of exporting overrides that were created in your test and pre-production environments to your production environment.
* It allows you to delete the original management pack without deleting the default management pack.
* It makes it possible to export the overrides to another Management Group.

Important

Running the “Configure SharePoint Management Pack” task automatically creates an override management pack “Microsoft.SharePoint.Foundation.2010.Override”.

We recommend putting all the override values for the Microsoft SharePoint Foundation 2010 management pack in an override management pack.

If you do not store your override in an override management pack, the overrides automatically go into the default management pack.

## Customize the Management Pack

Use the following four-step process to customize the management pack:

1. Create a new unsealed management pack to contain the overrides.
2. Override the Microsoft SharePoint Foundation 2010 management pack and save the customizations to the new unsealed management pack.
3. Export the new management pack that contains the overrides.
4. Import the new management pack and the Microsoft SharePoint Foundation 2010 management pack to another Management Group.

The detailed procedures for this four-step process are provided later in this document:

Important

For Operations Manager 2007 SP1 to use the overrides in an unsealed management pack, both the unsealed management pack and the original, sealed management pack on which the overrides were based must be imported to another Management Group.

For more information about sealed and unsealed management packs, see “Management Pack Formats” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb381260.aspx>.

For more information about management pack customizations and the default management pack, see “About Management Packs in Operations Manager 2007 SP1” at <http://technet.microsoft.com/en-us/library/bb309721.aspx>.

To create a new management pack for overrides:

1. In the Operations Console, click the Administration button.
2. In the **Administration** pane, right-click Management Packs, and then click Create Management Pack. The Create a Management Pack wizard appears.
3. In the **General Properties** page, type a name for the management pack in **Name**, the correct version number in **Version**, and a short description in **Description**.
4. Click Next. The **Knowledge** page opens.
5. Click **Edit** to create the overview knowledge article for this Management Pack. Include information about the purpose of the management pack in the article.
6. When you finish the article, click **File**, and then click **Save to MOM**.
7. To finish creating the Management Pack, click **Create**.

Note

When you create a management pack to store overrides, you should use a name for the management pack that contains the name of the management pack that holds the default settings. For example, to override the default settings in the Microsoft SharePoint Foundation 2010 Management Pack, you can create a management pack named “Microsoft SharePoint Foundation 2010 Overrides”.

Caution

The overrides that you save to this new management pack will supersede the default settings in the original management pack.

To override rules and save the customizations to the new management pack:

1. In the Operations Console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects**, and then click **Rules**.
3. In the **Rules** pane, click a rule that you want to override.
4. On the **Operations** **Manager** toolbar, click **Overrides**, and then point to **Override the Rule**. You can choose to override this rule for objects of a specific type, or for all objects within a category. After you choose which category or object type to override, the **Override Properties** dialog box opens, which enables you to view the parameters that can be overridden for the rule. You can then choose whether to override each individual parameter that is contained in the rule.
5. In the **Override Properties** dialog box, select the appropriate check box in the **Override** column for each parameter that you want to override.
6. When you complete your changes, select the management pack that you created for the overrides in the **Select destination management pack** drop-down box.
7. Click **OK**.
8. Repeat this process for each rule that you want to customize.

Important

You must have Advanced Operator user rights to create an override.

For more information, see the following Operations Manager 2007 SP1 Online Help topics:

* “How to Override a Monitor” at <http://technet.microsoft.com/en-us/library/bb309455.aspx>.
* “Overrides in Operations Manager 2007 SP1” at <http://technet.microsoft.com/en-us/library/bb381198.aspx>.
* “How to Monitor Using Overrides” at <http://technet.microsoft.com/en-us/library/bb309719.aspx>.

To export the new management pack that contains the overrides:

1. In the Operations Console, click the Administration button.
2. In the **Administration** pane, click **Management Packs**. This displays a list of the imported management packs.
3. In the **Management Packs** pane, right-click the management pack that contains the overrides, and then click **Export Management Pack**.
4. In the **Save As** dialog box, enter the path and file name for the management pack, or click **Browse** to save to a different directory, and then click **Save**.

The management pack is saved as an Operations Manager 2007 SP1 XML management pack file and is ready to be imported to another Management Group.

Note

You can only export an unsealed management pack.

To import the new management pack and the Microsoft SharePoint Foundation 2010 Management Pack to another Management Group:

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Management Group.
2. In the Operations Console, click the **Administration** button.
3. Right-click the **Management** **Packs** node, and then click **Import** **Management** **Packs**. The **Select Management Packs to Import** dialog box appears.
4. If necessary, change to the directory that contains the Microsoft SharePoint Foundation 2010 management pack files.
5. Click **Microsoft SharePoint Foundation 2010 Management** **Pack** and then click **Open**. The **Import Management Packs** dialog box appears.
6. In the **Import** **Management** **Packs** dialog box, click **Add**. The **Select Management Packs to Import** dialog box appears again.
7. Click the management pack that contains the overrides, and then click **Open**.
8. In the **Import Management Packs** dialog box, click the **Import** button.
9. After the import process is complete, click the **Close** button.

## Disable a Monitor or Rule

There may be situations in which you decide not to collect certain warnings, performance data, or miscellaneous non-critical events. These situations may include:

* Deployments across satellite links.
* Large branch office deployments.
* Deployments with very slow wide area network (WAN) links.
* Deployments where alerts are forwarded to a global network operations center.
* Situations where warnings and informational messages are not needed.

**Note**: Disabling rules might result in insufficient data for reports. For example if you disable alert for a particular monitor, that alert will not be counted in number of alerts hence will not be reflected in top alerts report

In situations such as these, you can disable the rules that generate the data that you do not want to be notified about. For more information, see “How to Disable a Monitor or Rule Using Overrides” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb309583.aspx>.

# Understanding the Microsoft SharePoint Foundation 2010Management Pack Operations

This section describes the objects that the management pack discovers, how health information rolls up, key monitoring scenarios, and how health is defined and indicated.

## Objects the Microsoft SharePoint Foundation 2010 Management Pack Discovers

The purpose of the management pack is to discover and monitor SharePoint Foundation 2010 components in your farm. The management pack discovers these objects.

## Understanding Health Monitoring

One of the most important features of the management pack is its ability to monitor the health of your SharePoint Foundation 2010 environment. The management pack uses monitors to continually assess the health state of monitored components, such as the SharePoint Foundation Search V4 (SPSearch4) service.

Note

A monitor is a management pack feature that uses events, performance data, and other information to assess the health state of a monitored component.

This section describes the types of Operations Manager 2007 SP1 monitors, lists the monitors that the management pack contains, explains how the roll up of the monitors for a SharePoint Foundation 2010 component determines its overall health, and describes how health is indicated in the Operations Console.

### About the Microsoft SharePoint Foundation 2010 Management Pack Monitors

There are various types of monitors that are available in Operations Manager 2007 SP1. The management pack contains the following three types of monitors:

* Unit monitors
* Aggregate rollup monitors
* Dependency monitors

**Unit monitors** are used to monitor specific counters, events, scripts, and services. Unit monitors are rolled up to aggregate rollup monitors.

**Unit monitor type definitions:**

* **Event Manual Reset Monitor: This monitor monitors an Event Log to watch for specific events. If an event is triggered, this monitor will change its health to a defined health state. The monitor will remain in that health state until an administrator manually switches it back to a different health state through the Operations Console.**
* **Event Timer Reset Monitor: This monitor monitors an event Log to watch for specific events. If an event is triggered, this monitor will change its health to a defined health state. After a defined period of time, the monitor will reset its health to a new health state.**
* **Repeated Event Manual Reset Monitor: This monitor monitors an event Log to watch for specific events. If the event is triggered multiple times, this monitor will change its health to a defined health state when the threshold is met. The monitor will remain in that health state until an administrator manually switches it back to a different health state through the Operations Console.**
* **Repeated Event Timer Reset Monitor: This monitor monitors an event Log to watch for specific events. If the event is triggered multiple times, this monitor will change its health to a defined health state when the threshold is met. After a defined period of time, the monitor will reset its health to a new health state.**
* **Service Monitor: This monitor watches over a Windows Service. If the component is a Windows Service, then this monitor can watch over the service status.**
* **Performance Simple Threshold Monitor: This monitor watches over a single Performance Counter threshold. If the Performance Counter goes over the threshold, this monitor will change health state.**
* **Performance Double Threshold Monitor: This monitor watches over a single Performance Counter threshold. If the Performance Counter goes over or under the defined thresholds, this monitor will change health state.**
* **Performance Consecutive Threshold Monitor: This monitor watches whether a Performance Counter hits a defined threshold multiple times in a certain period of time. If that threshold is met, the monitor will change health state.**

An **aggregate rollup monitor** reflects the state of unit, dependency rollup, or other aggregate rollup monitors targeted to an object. You typically use an aggregate rollup monitor to group multiple monitors into one monitor and then use that monitor to set the health state and generate an alert.

A **dependency rollup monito**r rolls up health states from objects linked by either a hosting or a containment relationship. Hosting and containment relationships for a given target are defined in most Management Packs. A dependency rollup monitor can be used to make the health state of a particular object dependent on the health state of components that are either hosted or contained.

Important

The health state of the following aggregate monitors must be manually reset when they display an error or warning state:

* Security Token Service Signing Certificate Is Missing
* Security Token Service Cannot Create Signing Credential
* Claims Auth Cannot Establish EndPoint
* Claims Auth Provider Exception Error
* Business Data Catalog Service Application Not Accessible
* Business Data Catalog Metadata Database Exception
* Business Data Catalog Database Backend Connectivity Exception
* Business Data Catalog Web Service Backend Connectivity Exception
* Insufficient Permission
* Database Full
* Product Help Library Site Collection Permission Could Not Refresh
* Windows SMTP Service Is Not Running
* SharePoint Lists Cannot Receive Email
* Mail Service Cannot Deliver Email
* Usage Service Unable To Access Log Directory
* Usage Service Timer Job Failed
* Topology Service Is Not Available
* Shared Service Application Endpoints Are Not Available
* Not Enough Free Space For Usage Log
* Not Enough Trace Log Free Space
* SharePoint Web Application Invalid Application Pool Account
* Credential Deployment Timer Job Failed
* Application Server Administration Service Timer Job Failed

For more information, see “About Monitors in Operations Manager 2007 SP1” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb381404.aspx>.

To view the management pack monitors:

1. In the Operations Console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects**, and then click **Monitors**. The monitors appear in the **Monitors** pane. To see more information in the **Monitor** **Details** pane, click any monitor.

### How Health Rolls Up

The management pack regards the components of SharePoint Foundation 2010 as a hierarchy. The health of each level depends on the health of the level below it.

When a unit monitor changes state, the state of the monitor at the level above changes to match; in other words, the health of the lower level rolls up to the level above it.

### How Health Is Indicated in the Operations Console

This management pack monitors the state of the health of the SharePoint Foundation 2010 environment. Operations Manager 2007 SP1 continuously updates the status of its managed computers and presents the status as part of the **State** view in the Monitoring pane of the Operations Console. Table 3 lists the icons that are used in the **State** view to indicate the server status.

 Table 3. Icons Used in the State View

|  |  |
| --- | --- |
| GreenCheck32x32 | Indicates that all services are running correctly and that the server is available. |
| AlertSeverity_Warning32x32 | Indicates that there may be an issue with one or more services or that the server itself may be unavailable. |
| RedX32x32 | Indicates that one or more services are unavailable or that the server itself is unavailable. |

## Key Monitoring Scenarios

This section describes the key monitoring scenarios that represent the types of information that the management pack collects.

Table 4. Microsoft SharePoint Foundation 2010 Management Pack Monitoring Scenarios

| **Scenario** | **Description** |
| --- | --- |
| Active Directory® | Monitors the application pool account for insufficient permission to add or read users from Active Directory. |
| Authentication | Monitors for issues that result from improper configuration of the authentication provider. |
| Backup and restore | Monitors backup failures and recycle bin quotas. |
| Databases | Monitors for connectivity issues with SQL database servers. |
| Diagnostic system | Monitors events related to the health of the tracing infrastructure. |
| E-mail | Monitors connectivity with the SMTP server. |
| IIS | Monitors the application pool account for issues writing to disk or registry key. |
| Performance | Monitors performance counters. |
| Search | Monitors events that are critical to the sound operation of the search service. |
| State monitoring and service discovery | Monitors Windows NT® service availability, including the following:* Microsoft SharePoint Foundation 2010 Timer
* Microsoft SharePoint Foundation 2010 Tracing
* Microsoft SharePoint Foundation 2010 Search
* Microsoft Internet Information Service
 |
| Timer | Monitors events associated with the Timer service. |
| Web parts and event handlers | Monitors events associated with failures to load event handlers and safe control assembly paths. |

## Understanding Rules

The management pack rules collect data that its monitored components generate. The rules are grouped into categories that are based on these components. The management pack Rules could be conceptually grouped as follows:

• Rules for Search Service

• Rules for SQL Server Database

• Rules for System Performance

• Rules for Web Server Performance

• Rules for Windows Services

• Rules for Microsoft SharePoint Foundation 2010

**To view the management pack rules:**

1. In the Operations Console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects**, and then click **Rules**. The rules appear in the **Rules** pane.
3. To view more information in the **Rule Details** pane, click any rule.

For more information, see “Rules in Operations Manager 2007 SP1” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb381367.aspx>.

## Understanding Tasks:

Tasks are a predefined command, script or code that can be run on a monitored computer. Tasks are primarily used for diagnostic or corrective action purposes. Task may also be used to configure monitoring environments. The management pack includes the tasks that are shown in Table 5.

Table 5. Microsoft SharePoint Foundation 2010 Management Pack Tasks

|  |  |
| --- | --- |
| **Task Name** | **Description** |
| Configure SharePoint Management Pack | This task configures the management pack by ensuring the existence of an override management pack, associating 'RunAs' account(s) to servers, enabling proxy settings, and initiating discoveries. |
| Set DebugTrace For SharePoint Management Pack | Enable or Disable DebugTrace for the SharePoint management pack Discovery and Monitoring scripts. |
| Restart Admin Service | Task to restart the Windows SharePoint Services Administration V4 (SPAdminV4) service. |
| Restart Timer Service | Task to restart the Windows SharePoint Services Timer V4 (SPTimerV4) service. |
| Restart Search Service | Task to restart the SharePoint Server Search 14 (OSearch14) service. |
| Restart HelpSearch Service | Task to restart the SharePoint Foundation Search V4 (SPSearch4) service. |
| Restart UserCode Service | Task to restart the Windows SharePoint Services User Code Host V4 (SPUserCodeV4) service. |
| Restart SPTrace Service | Task to restart the Windows SharePoint Services Tracing V4 (SPTraceV4) service. |

The “Set DebugTrace For SharePoint Management Pack” task will enable debug trace on those agent computers that run Windows PowerShell script based discoveries and SPHA monitors. By default it is turned off. When it is enabled, the script based discoveries and monitors will write debug trace information to Event Log in Operations Manager channel on all agent computers, and all the debug trace events have an event ID of 0. Typically the event description will include script name, startup/stop information and how long each script runs. A sample debug trace event is shown as below:

[Debug] C:\Program Files\System Center Operations Manager 2007\Health Service State\Monitoring Host Temporary Files 7\2\WSSBPAMonitor.ps1

Current User: [username]

Current PID: 1584

start time: 10/26/2009 1:03:09 PM

stop time: 10/26/2009 1:04:21 PM

time taken: 71046.3459

Windows PowerShell script WSSBPAMonitor.ps1 execution ended.

**To run the SetDebugTrace task, from the Operations Manager 2007 console:**

1. Select Monitoring, then select SharePoint 2010 Products, and then select Administration view.
2. On the **Actions** panel, click the task named “Set DebugTrace For SharePoint Management Pack”. A Run Task window will popup,
3. To enable debug trace (the default option), click **Run**. To disable debug trace, click **Override**.
4. Set the Enabled parameter value to “False” in the popup dialog.
5. Click **Override** to close the dialog.
6. Click **Run**.
7. Wait for the task to finish in Task Status window, and then check the Task Output to ensure that the task completes successfully.
8. Click **Close**.

 If you have the management packs for both Microsoft SharePoint Foundation 2010 and Microsoft SharePoint 2010 Products imported, the task will turn on trace for all discoveries and script monitors in both management packs, otherwise, it will only turn on trace for Microsoft SharePoint Foundation 2010 management pack.

For more information, see “Tasks in Operations Manager 2007 SP1” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb309743.aspx>.

To view the management pack tasks:

1. In the Operations Console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects**, and then click **Tasks**. The tasks appear in the **Tasks** pane. The **Management Pack** column lists the tasks that belong to the Microsoft SharePoint Foundation 2010 Management Pack.
3. To view more information in the **Task** **Details** pane, click any task.

## Viewing Information in the Operations Console

This section describes the Operations Manager 2007 SP1 Operations Console and explains how to view status and performance data and the management pack views, rules, attributes, and object discoveries.

### About the Operations Manager 2007 SP1 Operations Console

The Operations Console is the main user interface for Operations Manager 2007 SP1, with navigation buttons that enable you to access to the **Monitoring**, **Authoring**, **Reporting**, **Administration**, and **My** **Workspace** panes.

Each Operations Console pane has a specific purpose:

* The **Monitoring** pane is used to display monitoring data, and track and resolve issues easily. You can use this pane to view the health status of your monitoring environment and handle alerts. This pane displays different views of the monitoring data that Operations Manager 2007 SP1 collects.
* The **Authoring** pane is used to configure management pack objects—such as monitors, rules, and tasks—distributed applications, groups, and management pack templates.
* The **Reporting** pane is used to display default and management pack-specific reports, and to save and schedule reports.
* The **Administration** pane is used to edit Operations Manager 2007 SP1 settings and perform a number of functions including importing and creating management packs, and creating overrides for management packs.
* The **My Workspace** pane is used to customize how you view the Operations Console.

For more information about the Operations Console, see “Operations Console in Operations Manager 2007 SP1” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb381361.aspx>.

### Viewing Status and Performance Data in the Monitoring Pane

The Monitoring pane of the Operations Console provides numerous views that you can use to check the status and performance of the SharePoint Foundation 2010 environment. This section describes the management pack views, explains how to select a view in the **Monitoring** pane and get detailed information about an alert or event, and discusses creating custom views.

#### The Microsoft SharePoint Foundation 2010 Management Pack Views

This management pack has the following views:

|  |  |
| --- | --- |
| View Name | Description |
| Diagram View | SharePoint Foundation 2010 farm group diagram view. |
| Active Alerts | Displays all active SharePoint Services alerts. |
| Events | Displays all events collected for SharePoint Services objects. |
| Administration | This is the entry point for administration tasks to configure SharePoint farm discovery and monitoring. |
| Farms | Displays the state of SharePoint farms. |
| Servers | Displays the state of SharePoint servers. |
| Services | Displays state of the SharePoint services. |
| Web Applications | Displays state of the SharePoint Web applications. |
| Shared Services | Displays state of the SharePoint service applications. |
| Task Status | Displays status of SharePoint tasks. |
| Performance | Displays performance view of SharePoint Services objects in Operations Manager 2007 console. |
| Configuration Databases | Displays state of SharePoint Services configuration databases. |
| Content Databases | Displays state of SharePoint Services content databases. |
| SPHA Rules | Displays state of SharePoint Health Analyzer (SPHA) rules. |
| Service Front Ends | Displays state of the SharePoint Web servers. |
| Unidentified Machines | Displays state of unidentified SharePoint computers. |

To select a view:

1. In the Monitoring pane of the Operations Console, expand Monitoring.
2. Expand **Microsoft SharePoint Foundation 2010** Management Pack.
3. Click a view.

To view detailed information about a particular alert or event:

1. In the Monitoring pane of the Operations Console, expand Monitoring.
2. Expand Microsoft SharePoint Foundation 2010 Management Pack.
3. Click the **Alerts** or **Events** view.
4. In the **Alerts** or **Events** pane, click an alert or event. More information about the alert or event appears in the **Alert Details** or **Event Details** pane.
5. In the **Alert Details** or **Event Details** pane, click the name of the rule that generated the alert or collected the event.

The **Properties** dialog box for the generating rule opens. This dialog box displays information about the rule, including knowledge about the causes and resolution of the alert or event.

1. In the **Properties** dialog box, click the **Product** **Knowledge** tab. Click the link to get product knowledge.

For more information, see “Views in Operations Manager 2007 SP1” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb381272.aspx>.

#### Custom Views

You can create custom views to suit your environment. For information about creating custom views, see the following Operations Manager 2007 SP1 Online Help topics:

* “How to Create a State View in Operations Manager 2007 SP1” at <http://technet.microsoft.com/en-us/library/bb381457.aspx>
* “How to Create a Diagram View” at <http://technet.microsoft.com/en-us/library/bb309701.aspx>
* “How to Personalize a View” at <http://technet.microsoft.com/en-us/library/bb309591.aspx>

### Viewing Management Pack Views in the Authoring Pane

You can view the management pack views in the **Authoring** pane of the Operations Console. This allows you to see the properties, such as the criteria and display settings, of a particular view including the criteria and display settings for the view. You can use this information to customize the view or create a different view with similar characteristics.

**To view the Management Pack views:**

1. In the Operations Console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Views**. The views appear in the **Views** pane.
3. The **Management Pack** column lists the views that belong to the management pack.
4. To see more information in the **View Details** pane, click any view.
5. To see the properties of the view, click **Properties** in the **Actions** pane.

For detailed descriptions of the views, see "Viewing Status and Performance Data in the Monitoring Pane" in this guide.

### Viewing Management Pack Rules in the Authoring Pane

You can view the management pack rules in the **Authoring** pane of the Operations Console. This allows you to find rules that you may want to disable or modify. For more information about modifying and disabling rules, see "Optional Configuration for the Microsoft SharePoint Foundation 2010 Management Pack" in this guide.

To view the Management Pack rules

1. In the Operations Console, click **Authoring**.
2. In the Authoring pane, expand **Management Pack Objects**.
3. Click the **Rules** node. The rules are displayed in the Rules pane.
4. On the Operations Manager toolbar, click **Scope**. The **Scope Management Packs by targets(s)** dialog box opens.
5. Click **Clear All** to clear the existing selection.
6. Enter “Microsoft SharePoint Foundation 2010” in the **Look for** text box.
7. Click **Select All**.
8. Click **OK**.
9. In the **Rules** pane, click a rule. More information about the rule appears in the **Rule Details** pane.
10. In the **Rule Details** pane, click **View Knowledge** to open the **Properties** dialog box for the rule.

### Viewing Management Pack Object Discoveries in the Authoring Pane

In Operations Manager 2007 SP1, object discoveries are used to find the specific objects on a network that need to be monitored based on the object types that the management pack defines. Because management pack developers do not know the specific objects that are in your network environment, they only define the types of objects that their management pack monitors. However, the developers also include object discoveries to find the specific objects on your network that the management pack monitors.

For more information, see “Object Discoveries in Operations Manager 2007 SP1” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb381270.aspx>.

Table 6 lists the object discoveries that are included in the management pack.

Table 6. Microsoft SharePoint Foundation 2010 Management Pack Object Discoveries

|  |  |
| --- | --- |
| Object Discovery Name | Description |
| Admin Service in SPService | Admin Service in SPService for a particular farm. |
| Admin Service in SPServiceInstance | Admin Service in SPServiceInstance for a particular server. |
| Base Class of Shared Service | Base class of a Shared Service. |
| Business Data Connectivity Service Application Database | Business Data Connectivity Service Application Database. |
| Business Data Connectivity Service Instance | Business Data Connectivity Service Instance. |
| CentralAdmin Service in SPServiceInstance | CentralAdmin Service in SPServiceInstance for a particular server. |
| Database Base Class For Shared Service | An abstract class For various Shared Service Database related classes. |
| Help Search Service in SPServiceInstance | Help Search Service in SPServiceInstance for a particular server. |
| Search Service | Search Service in SPService for a particular farm. |
| Search Service Instance | Search Service in SPServiceInstance for a particular server. |
| Business Data Connectivity Shared Service | Shared Service - Business Data Connectivity. |
| Business Data Connectivity Application | Shared service application - Business Data Connectivity Application. |
| SharePoint component | This is one instance of a particular SharePoint component. |
| SharePoint Configuration Database | SharePoint Configuration Database stores all configuration information for a farm. |
| SharePoint Content Database | This is one of the SharePoint Content Databases, and it stores actual content for one or many sites. |
| SharePoint Content Database Collection | This collection contains all Content Databases in a SharePoint farm. |
| SharePoint Database | SharePoint Database base class. |
| SharePoint Farm | One of the farm in SharePoint Farm Group. |
| SharePoint Farm Group | Farm group for Microsoft SharePoint Foundation 2010. |
| SharePoint Server | SharePoint Server. |
| SharePoint Server Group | Server group in a SharePoint farm. |
| SharePoint Service | This is one instance of a particular SharePoint Service. |
| SharePoint Service Instance | This is one instance of a particular SharePoint Service Instance. |
| SharePoint Services Group | This group contains all SharePoint Foundation 2010 services. |
| SharePoint Shared Service Application | Shared service application instance. |
| SharePoint Shared Service Group | This group contains all shared services for a farm. |
| SharePoint Timer Job | This is a Timer Job for specific service or service application. |
| SharePoint Timer Job Instance | This is one of the SharePoint Timer Job instance on specific computer. |
| SharePoint Application and Topology Application | Application and Topology application instance. |
| SharePoint Usage and health service Application | Usage and health application instance. |
| SharePoint Web Application Group | This group contains all Web Application running in a farm. |
| SharePoint Web Application Instance | This is an instance of SharePoint web application. |
| SPHA Availability Rule | SharePoint Health Analyzer (SPHA) Availability Rule defined in a SharePoint Farm. |
| SPHA Configuration Rule | SharePoint Health Analyzer (SPHA) Configuration Rule defined in a SharePoint Farm. |
| SPHA Custom Rule | SharePoint Health Analyzer (SPHA) Custom Rule defined in a SharePoint Farm. |
| SPHA Performance Rule | SharePoint Health Analyzer (SPHA) Performance Rule defined in a SharePoint Farm. |
| SPHA Rule | This is a SharePoint Health Analyzer (SPHA) Rule defined in a SharePoint Farm. |
| SPHA Rule Group | This is SharePoint Health Analyzer (SPHA) Rule Group for a SharePoint Farm. |
| SPHA Rule Sub Group | This is SharePoint Health Analyzer (SPHA) Rule Sub Group for a SharePoint Farm (Any or All). |
| SPHA Security Rule | SharePoint Health Analyzer (SPHA) Security Rule defined in a SharePoint Farm. |
| System Timer Job Hosting Object | This object is the target of various System Timer Job monitors. |
| Timer Service in SPService | Timer Service in SPService for a particular farm. |
| Timer Service in SPServiceInstance | Timer Service in SPServiceInstance for a particular server. |
| Application and Topology in SPServiceInstance | Application and Topology Service in SPServiceInstance for a particular server. |
| Application and Topology Shared Service | Applicatin and Topology Shared Service. |
| Unidentified SharePoint Machine | All computers which could not be identified as SharePoint computers. |
| Unidentified SharePoint Servers | This group contains servers that have Microsoft SharePoint Foundation 2010 installed but not configured or correctly functioning. |
| Usage Service in SPServiceInstance | Usage Service in SPServiceInstance for a particular server. |
| Usage Shared Service | Usage Shared Service. |
| Sandboxed code in SPService | Sandboxed Code Service in SPService for a particular farm. |
| Sandboxed code in SPServiceInstance | Sandboxed Code Service in SPServiceInstance for a particular server. |
| Web Service in SPService | Web Service in SPService. |
| SharePoint Objects Group | This group contains all Microsoft SharePoint Foundation 2010 objects. |
| SharePoint site in Spweb application | SharePoint site in a Web application.  |
| SharePoint site collection in SPWebApplication | Site collection in a Web application. |
| SharePoint web Application | SharePoint Web Application. |
| Web application host instance collection in SPWebApplication | SharePoint host instance collection for a Web application. |
| Web application host instance in SPWebApplication | SharePoint host instance for a Web application. |
| Incoming email service in spservice |  Incoming email service in spservice.  |
| Trace service instance |  Trace service instance in spserviceinstance. |
| Incoming email service instance | incoming email service instance in spserviceinstance. |
| SharePoint foundation 2010 installed server | A computer with SharePoint foundation 2010 installed. |
| Security Token service instance |  Security Token service instance in spserviceinstance. |
| Security Token service Application | Security token service application in spsharedserviceapplication. |
| Security Token service in spsharedservice |  Security Token service in spsharedservice . |

To view the Management Pack object discoveries:

1. In the Operations Console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects**, and then click **Object Discoveries**. The object discoveries appear in the **Object Discoveries** pane. The **Management Pack** column lists the object discoveries that belong to the management pack.
3. To view more information in the **Object Discovery Details** pane, click any object discovery.

# Using the Microsoft SharePoint Foundation 2010Management Pack Reports

To look at trends in your environment across days, weeks, or months, you can use the management pack reports. This section:

* Describes how to select a management pack report and shows an example of a report.
* Lists all the reports that the management pack provides.
* Explains the purpose of and the lists the rules that collect the data for each report.

## Selecting a Report

To select a Management Pack report:

1. In the Operations Console, click the **Reporting** button.
2. Expand **Reporting**.
3. Click **Microsoft SharePoint Foundation 2010 Management Pack**.
4. In the **Reports** pane, click a report and then click **Open**.
5. A dialog box that displays the parameters for the selected report appears.

Note

The instructions for selecting report parameters are beyond the scope of this guide. For information about how to select the parameters for a report, see “How to Run a Report from the Reporting Pane in Operations Manager 2007 SP1” in the Operations Manager 2007 SP1 Online Help at <http://technet.microsoft.com/en-us/library/bb381183.aspx>.

1. After you enter the parameters for the report, click **Run** in the toolbar to run the report.

The report graphs the data that you have selected and shows the rules that collected the data.

## Report Descriptions

The Microsoft SharePoint Foundation 2010 management pack provides the following reports:

|  |  |
| --- | --- |
| Server Alert | This report renders all alerts raised by specified server(s). |
| Service Alert | This report renders all alerts raised by specified service(s). |
| Server Event | This report renders all events raised on specified server(s). |
| Service Event | This report renders all events raised on specified service(s). |
| Top Server Events | This report renders top 20 events raised on specified server(s). |
| Top Service Events | This report renders top 20 events raised on specified service(s). |
| Top Alerts | This Most Common Alert Report helps to identify high volume alerts, the volume a distinct alert contributes to the total number of alerts and the resolution times. This report helps in tuning the alerts. |
| Server Performance | This report renders performance data for specified server(s). |
| Entity State | This report renders entity state for specified SharePoint object(s) over time. |

**Monitors**

|  |  |
| --- | --- |
| **Name** | **Description** |
| Security Token Service Signing Certificate Is Missing | A critical state of this Monitor indicates that the Security Token Service Signing Certificate is missing. |
| Security Token Service Cannot Create Signing Credential | A critical state of this Monitor indicates that SharePoint is unable to create the signing credentials to sign the security token. It is possible that the certificate is corrupt. |
| Claims Auth Cannot Establish EndPoint | A critical state of this Monitor indicates that an exception occurred when trying to establish an endpoint for context. |
| Claims Auth Provider Exception Error | A critical state of this Monitor indicates that Claims provider exception occurred. |
| Business Data Connectivity Service Application Not Accessible | A critical state of this Monitor indicates that Business Data Connectivity service application is not accessible. |
| Business Data Connectivity Metadata Database Exception | A critical state of this Monitor indicates that Business Data Connectivity service application failed because of a database exception. |
| Business Data Connectivity Database Backend Connectivity Exception | A critical state of this Monitor indicates that Business Data Connectivity failed to open connection. |
| Business Data Connectivity Web Service Backend Connectivity Exception | A critical state of this Monitor indicates that Business Data Connectivity Service Application could not obtain a proxy to web service for External Data Source. |
| SPHA Availability Rule Monitor | A critical state of this Monitor indicates that SharePoint Health Analyzer (SPHA) Availability Rule failed. |
| SPHA Configuration Rule Monitor | A critical state of this Monitor indicates that SharePoint Health Analyzer (SPHA) Configuration Rule failed. |
| SPHA Performance Rule Monitor | A critical state of this Monitor indicates that SharePoint Health Analyzer (SPHA) Performance Rule failed. |
| SPHA Security Rule Monitor | A critical state of this Monitor indicates that SharePoint Health Analyzer (SPHA) Security Rule failed. |
| SPHA Custom Rule Monitor | A critical state of this Monitor indicates that SharePoint Health Analyzer (SPHA) Custom Rule failed. |
| SQL Database Connection Failed | A critical state of this Monitor indicates that a SQL Database connection attempt failed for a specified connection string. Note:This Monitor is disabled by default, enable this Monitor if you want this Management Pack to monitor the SQL Database Connection for SharePoint 2010. |
| SPHA Availability Rule Monitor On SPServer | A critical state of this Monitor indicates that SharePoint Health Analyzer (SPHA) Availability Rule failed on SPServer. |
| SPHA Configuration Rule Monitor On SPServer | A critical state of this Monitor indicates that SharePoint Health Analyzer (SPHA) Configuration Rule failed on SPServer. |
| SPHA Performance Rule Monitor On SPServer | A critical state of this Monitor indicates that SharePoint Health Analyzer (SPHA) Performance Rule failed on SPServer. |
| SPHA Security Rule Monitor On SPServer | A critical state of this Monitor indicates that SharePoint Health Analyzer (SPHA) Security Rule failed on SPServer. |
| SPHA Custom Rule Monitor On SPServer | A critical state of this Monitor indicates that SharePoint Health Analyzer (SPHA) Custom Rule failed on SPServer. |
| Failed To Write Registry Entry | A critical state of this Monitor indicates that there are failures of web application when writing to server registry. |
| Failed To Write File | A critical state of this Monitor indicates that the application pool account has insufficient permissions to write files. |
| Throttling Status | A warning state of this Monitor indicates that the server is entering into throttling state. |
| SQL Server Not Found | A critical state of this Monitor indicates that a SQL Server was not found. |
| Database Not Found | A critical state of this Monitor indicates that the database was not available on a particular instance on SQL Server. |
| Insufficient Permission | A critical state of this Monitor indicates that a server has insufficient SQL Server database permissions. |
| Login Failed | A critical state of this Monitor indicates that an Application Login failed on this server. |
| Database Full | A critical state of this Monitor indicates that a SQL database is full. |
| Unacceptable Response Time | A critical state of this Monitor indicates that the Response Time to render content is more than 7500ms for 3 consecutive performance values. |
| Read Only Database | A critical state of this Monitor indicates that the database is read only. Write permission is required to set this Monitor into a healthy state. |
| Product Help Library Site Collection Permission Could Not Refresh | A critical state of this Monitor indicates that there is an issue when refreshing permissions for product help library. |
| Admin Service Is Not Running | A critical state of this Monitor indicates that the Admin Service is not running on a particular server. |
| Windows SMTP Service Is Not Running | A critical state of this Monitor indicates that Windows SMTP Service is not running; without the Windows SMTP Service, SharePoint Incoming Email Service cannot send/receive email. |
| SharePoint Lists Cannot Receive Email | A critical state of this Monitor indicates that SharePoint Lists cannot receive email. |
| Mail Service Cannot Deliver Email | A warning state of this Monitor indicates that a large number of Incoming Email Service lookup fails. |
| Timer Service Is Not Running | A critical state of this Monitor indicates that the Timer Service is not running on a particular server. |
| Timer Service Restart Failed | A critical state of this Monitor indicates that the timer service restart has failed. |
| SharePoint Timer Service Backup Timer Creation Failure | A warning state of this Monitor indicates that the same item is already in the process of being backed up or restore. To check the status of that process, go to the backup/restore job status page in the administration site. |
| Search Service Is Not Running | A critical state of this Monitor indicates that Search Service is not running on a particular server. |
| Help Search Service Is Not Running | A critical state of this Monitor indicates that Help Search Service is not running on a particular server. |
| Usage Service Unable To Access Log Directory | A critical state of this Monitor indicates that the usage service was unable to access log directory. |
| Usage Service Timer Job Failed | A warning state of this Monitor indicates that the Usage timer job failed. You can rerun this job using the Timer Job status page in the SharePoint Central Administration site. |
| Sandboxed Code Service Is Not Running | A critical state of this Monitor indicates that the Sandboxed Code Service is not running on a particular server. |
| Application Discovery And Load Balancer Service Application Are Not Available | A critical state of this Monitor indicates that the Application Discovery and Load Balancer Service Application are unable to retrieve the list of published service applications from the remote farm. |
| Service Application Endpoints Are Not Available | A critical state of this Monitor indicates that the Application Discovery and Load Balancer Service Application are unable to retrieve the list of endpoints for a service application from the remote farm. |
| Not Enough Free Space For Usage Log | A critical state of this Monitor indicates that the usage log does not have enough free disk space. |
| Not Enough Trace Log Free Space | A critical state of this Monitor indicates that the trace log does not have enough free disk space. |
| Trace Log Reaching Max Storage | A warning state of this Monitor indicates that the trace log is reaching max storage. |
| Usage Log Reaching Max Storage | A warning state of this Monitor indicates that the usage log is reaching max storage. |
| Trace Service Is Not Running | A critical state of this Monitor indicates that the Trace Service is not running on a particular server. |
| Ping Web Application Failed | A critical state of this Monitor indicates that a ping attempt failed for the Web Application URL. |
| SharePoint Web Application Invalid Application Pool Account | A critical state of this Monitor indicates that the IIS Application Pool account is not registered in Active Directory as a Service Principal Name in the Web Application Domain. |
| Site Creation Failed | A critical state of this Monitor indicates that site creation failed on the SPHostInstance. |
| Ping A Site Failed | A critical state of this Monitor indicates that a ping attempt failed for the site URL. |
| Generate Password Timer Job Failed | A critical state of this Monitor indicates that SPGeneratePasswordJobDefinition timer job has thrown an exception. |
| Content Application Pool Credential Deployment Timer Job Failed | A critical state of this Monitor indicates that SPContentAppPoolCredentialDeploymentJobDefinition timer job has thrown an exception. |
| Admin Application Pool Credential Deployment Timer Job Failed | A critical state of this Monitor indicates that SPAdminAppPoolCredentialDeploymentJobDefinition timer job has thrown an exception. |
| Master Passphrase Deployment Timer Job Failed | A critical state of this Monitor indicates that SPMasterPassphraseDeploymentJobDefinition timer job has thrown an exception. |
| Password Management Timer Job Failed | A critical state of this Monitor indicates that SPPasswordManagementJobDefinition timer job has thrown an exception. |
| Credential Deployment Timer Job Failed | A critical state of this Monitor indicates that SPWindowsServiceCredentialDeploymentJobDefinition timer job has thrown an exception. |

**Rules**

|  |  |
| --- | --- |
| **Name** | **Description** |
| Event Log Flooding Protection Activated | This Rule collects data when Event Log Flood Protection was activated because an event was fired more than 5 times in 2 minutes. |
| Cannot Connect To SQL Server | This Rule collects data when SharePoint Foundation 2010 could not connect to the SQL Server database. |
| Insufficient SQL Server Database Permissions | This Rule collects data when insufficient privileges have been granted in the SQL Server database to the service account specified in SharePoint Foundation 2010. |
| SQL Server Database Is Full | This Rule collects data when a SQL Server error occurred because the database size limit has been reached. |
| SQL Server Database Login Failed | This Rule collects data when the user name or password for the SharePoint Foundation 2010 account was invalid before the session or became invalid during the session. |
| Access Denied For Writing To Registry | This Rule collects data when the application pool used by SharePoint Foundation 2010 attempts to update a registry key or file folder and is denied access because the service account used by the application pool has inadequate permissions. |
| Access Denied For Writing To Disk | This Rule collects data when the application pool used by SharePoint Foundation 2010 attempts to update a file folder and is denied access because the service account used by the application pool has inadequate permissions. |
| An Error Occurred While Communicating With The SMTP Server | This Rule collects data when an error occurs while trying to communicate with the SMTP server. |
| Cannot Connect To SMTP Host | This Rule collects data when SharePoint Foundation 2010 cannot connect to the Simple Mail Transfer Protocol (SMTP) host. |
| Cannot Resolve Name Of The Outbound SMTP Server | This Rule collects data when SharePoint Foundation 2010 cannot resolve the name of the Simple Mail Transfer Protocol (SMTP) server. This can happen because the name of the SMTP mail server is incorrect or the Domain Name Server (DNS) server is unavailable. |
| The Application Pool Account Must Be Registered As A Kerberos Service Provider | This Rule collects data when the application pool account has insufficient permissions to add user accounts to Active Directory. When using Kerberos authentication, the service account used by the Internet Information Services (IIS) application pool for your Web application must be registered in Active Directory as a Service Principal Name (SPN) on the domain on which the Web front-end is a member. |
| Alternate Access Mapping Update Failed | This Rule collects data when the timer job used to update alternate access mappings failed on the specified server. |
| Unable To Load Authentication Provider | This Rule collects data when the Role Manager or Membership Provider that is specified for a particular web application is incorrectly configured. |
| Backup Failed Due To Insufficient Permissions | This Rule collects data when the backup of a website fails due to the administrator having inadequate permissions to perform a backup to a file share or folder on the local server, or to the SQL Server database. |
| Event Handler Failed To Load | This Rule collects data when the specified event handler failed to load. This can happen because the event receiver assembly is missing or the assembly does not have the event receiver class. |
| Failed To Create Site | This Rule collects data when an attempt to create a new SharePoint site has failed. |
| Insufficient Permissions To Write To The Configuration Data Cache | This Rule collects data when the permissions on the %systemdrive%\inetpub\wwwroot\wss\config folder where the SharePoint Foundation 2010 configuration data cache is stored has been changed. |
| Service Instance Provisioning Failed | This Rule collects data when an attempt to start or stop a service instance on a server in the server farm has failed. Additional details about why the service could not be started or stopped are included in the exception message of the Windows NT Event log. |
| The Active Directory Organization Unit Registered In SharePoint Foundation 2010 Does Not Exist | This Rule collects data when the Active Directory organizational unit that was created for account creation mode does not exist. This condition can occur due to a provisioning-time error or a runtime error. |
| The Application Pool Account Has Insufficient Permissions To Add User Accounts To Active Directory | This Rule collects data when the application pool account used by a SharePoint site lacks permissions to add user information to the Active Directory. |
| Page Response Time | This Rule collects data on Executing Time/Page Request counter which counts the amount of time application is taking to render a webpage. |
| Server Is About To Enter Into Throttling State | This Rule collects data when the Server is about to enter into throttling state. |
| Timer Job To Update Central Admin Failed | This Rule collects data when the SharePoint Foundation 2010 timer job to update central administration on a particular URL failed. |
| Event Receiver Failed | This Rule collects data when the event receiver failed. |
| SharePoint Administration Service Is Disabled | This Rule collects data when the SharePoint Foundation 2010 timer job is executed and discovers that the SharePoint Foundation 2010 Administration service is disabled. |
| Windows SMTP Service Is Not Running Rule | This Rule collects data when Windows SMTP Service is not running. |
| SharePoint Lists Cannot Receive Email Rule | This Rule collects data when SharePoint Lists cannot receive email. |
| Mail Service Cannot Deliver Email Rule | This Rule collects data when a large number of Incoming Email Service lookup fails. |
| Backup Failed Due To Timer Job Failure | This Rule collects data when the SharePoint Foundation 2010 timer job used to perform the backup of a site failed. |
| Exception In Execute Method Of Job Definition | This Rule collects data when an exception occurred in the execute method of the job definition for a particular timer job. |
| Unable To Write To Trace Log | This Rule collects data when the SharePoint Foundation 2010 cannot write to the Windows Trace log. This can happen because the hard drive on which the Trace log is located is full or the permissions on the trace logging directory are not set correctly. |