

Windows SharePoint Services 3.0 Management Pack Guide  
for Operations Manager 2007

Microsoft Corporation

Published: December 2007

Copyright © 2007 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.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

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.

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

[Windows SharePoint Services 3.0 Management Pack for Operations Manager 2007 1](#_Toc184468395)

[SharePoint Monitoring Toolkit 2](#_Toc184468396)

[Document Version 2](#_Toc184468397)

[Getting the Latest Management Pack and Management Pack Documentation 2](#_Toc184468398)

[What's New 2](#_Toc184468399)

[Requirements for the Windows SharePoint Services 3.0 Management Pack 3](#_Toc184468400)

[Prerequisites for Using the Management Pack 3](#_Toc184468401)

[Security Considerations for the Windows SharePoint Services 3.0 Management Pack 4](#_Toc184468402)

[Configure the Default Action Account Run As Profile 4](#_Toc184468403)

[Low-Privilege Environments 5](#_Toc184468404)

[Specify User Privileges with Computer Groups 5](#_Toc184468405)

[Support for Agentless Monitoring 5](#_Toc184468406)

[Getting Started with the Windows SharePoint Services 3.0 Management Pack 6](#_Toc184468407)

[Download the Management Pack Files 6](#_Toc184468408)

[Import the Management Pack into Operations Manager 2007 6](#_Toc184468409)

[Deploy and Configure Servers for the Operations Manager 2007 Agent 7](#_Toc184468410)

[Resize the Agent Event Logs 7](#_Toc184468411)

[Disable Event Log Replication for Monitoring Clustered Servers 8](#_Toc184468412)

[Optional Configuration for the Windows SharePoint Services 3.0 Management Pack 8](#_Toc184468413)

[Customize the Management Pack 9](#_Toc184468414)

[Disable a Monitor or Rule 12](#_Toc184468415)

[Understanding the Windows SharePoint Services 3.0 Management Pack Operations 12](#_Toc184468416)

[Objects the Windows SharePoint Services 3.0 Management Pack Discovers 12](#_Toc184468417)

[Understanding Health Monitoring 13](#_Toc184468418)

[About the Windows SharePoint Services 3.0 Management Pack Monitors 13](#_Toc184468419)

[How Health Rolls Up 15](#_Toc184468420)

[How Health Is Indicated in the Operations Console 15](#_Toc184468421)

[Key Monitoring Scenarios 16](#_Toc184468422)

[Understanding Rules 17](#_Toc184468423)

[Understanding Tasks 17](#_Toc184468424)

[Viewing Information in the Operations Console 18](#_Toc184468425)

[About the Operations Manager 2007 Operations Console 18](#_Toc184468426)

[Viewing Status and Performance Data in the Monitoring Pane 20](#_Toc184468427)

[Viewing Management Pack Views in the Authoring Pane 23](#_Toc184468428)

[Viewing Management Pack Rules in the Authoring Pane 23](#_Toc184468429)

[Viewing Management Pack Attributes in the Authoring Pane 25](#_Toc184468430)

[Viewing Management Pack Object Discoveries in the Authoring Pane 26](#_Toc184468431)

[Using the Windows SharePoint Services 3.0 Management Pack Reports 27](#_Toc184468432)

[Selecting a Report 27](#_Toc184468433)

[Report Descriptions 29](#_Toc184468434)

[Alerts Report 30](#_Toc184468435)

[Most Common Alerts Report 30](#_Toc184468436)

[Event Analysis Report 30](#_Toc184468437)

[Most Common Events Report 30](#_Toc184468438)

[ASP .NET Applications Performance Report 30](#_Toc184468439)

[Logical Disk Performance Report 30](#_Toc184468440)

[Process Performance Report 31](#_Toc184468441)

[Processor Performance Report 31](#_Toc184468442)

[Web Service Performance Report 31](#_Toc184468443)

[Appendix A: Troubleshooting the Windows SharePoint Services 3.0 Management Pack 32](#_Toc184468444)

[Appendix B: Windows SharePoint Services 3.0 Management Pack Rules 35](#_Toc184468445)

[Rule Categories 35](#_Toc184468446)

[Search Rules 38](#_Toc184468447)

[SQL Server Database Rules 43](#_Toc184468448)

[System Performance Rules 46](#_Toc184468449)

[Web Server Rules 49](#_Toc184468450)

[Windows Services Rules 52](#_Toc184468451)

[Windows SharePoint Services 3.0 Application Rules 55](#_Toc184468452)

[Acknowledgments 65](#_Toc184468453)

[Feedback 65](#_Toc184468454)

# Windows SharePoint Services 3.0 Management Pack for Operations Manager 2007

The Windows SharePoint Services 3.0 Management Pack for Operations Manager 2007 helps you manage Microsoft® Windows® SharePoint® Services environments of all sizes.

The highly collaborative environment provided by Windows SharePoint Services 3.0 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 to collaboration challenges. As a result, Windows SharePoint Services deployments have tended to grow unfettered at the departmental level rather than under the control of IT management. This growth, along with the number of components that contribute to the provided services, makes it difficult for IT to monitor and effectively manage these environments.

The Windows SharePoint Services 3.0 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:

* Windows SharePoint Services 3.0 related services (Timer, Tracing, and Search)
* Windows SharePoint Services 3.0 related Events
* Web server applications such as Internet Information Services (IIS)
* IIS related Events
* Microsoft SQL Server™ database related events
* WSS Server performance.

Note



The *SharePoint Asset Inventory Toolkit* will be available as a download by early 2008 on the Microsoft Download Center. It can help you discover unidentified environments that you may wish to monitor.

When there is an issue that may cause a service outage or poor performance, Microsoft System Center Operations Manager 2007 uses the Windows SharePoint Services 3.0 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 Windows SharePoint Services Search service cannot update an index because there is insufficient hard disk space, a monitor changes state to critical and alertsyou. 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 hard disk or move the index files to another drive.

## SharePoint Monitoring Toolkit

The Windows SharePoint Services 3.0 Management Pack and accompanying documentation are part of the SharePoint Monitoring Toolkit Solution Accelerator.

The SharePoint Monitoring Toolkit contains the following Management Packs for System Center Operations Manager 2007:

* The Microsoft Office SharePoint Server 2007 Management Pack and the *Microsoft Office SharePoint Server 2007 Management Pack Guide for Operations Manager 2007* to help you monitor and manage your Microsoft Office SharePoint Server 2007 environment.
* The Windows SharePoint Services 3.0 Management Pack and the *Windows SharePoint Services 3.0 Management Pack Guide for Operations Manager 2007* to help you monitor and manage your Windows SharePoint Services 3.0 environment.

## Document Version

This is Version 1.0 of this documentation, released on December 4, 2007

## Getting the Latest Management Pack and Management Pack Documentation

You can find the latest Windows SharePoint Services 3.0 Management Pack in the Microsoft TechNet *Management Pack Catalog* at [http://www.microsoft.com/technet/prodtechnol/mom/catalog/catalog.aspx.](http://www.microsoft.com/technet/prodtechnol/mom/catalog/catalog.aspx.%20) The latest version of this document is available from the Microsoft TechNet *System Center Operations Manager 2007 Product Documentation* site at <http://technet.microsoft.com/en-us/opsmgr/bb498235.aspx>.

## What's New

The following features are new in this release of the Windows SharePoint Services 3.0 Management Pack:

* New performance collection and event collection rules to increase your ability to resolve issues
* Descriptions for all rules and monitors are updated.
* Knowledge base articles for all rules and monitors are added.
* New reports, which include performance, alerts, most common alerts, most common events, and event analysis reports
* Alert suppression for all event-based rules based on event identification (ID), event source, event description, and logged computer (by agent name).
* Views that are scoped precisely to the target objects of the Management Pack, such as the WSS Computer Group and WSS Application/WSS Server objects. This improves the performance of the Management Pack views and provides more accurate results.
* Both service and event monitors that are fine-tuned to match the alert and health states of the services more precisely.

# Requirements for the Windows SharePoint Services 3.0 Management Pack

This section explains the prerequisites that are necessary for you to use the Windows SharePoint Services 3.0 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:

* Have System Center Operations Manager 2007 deployed in at least one Management Group. A Management Group consists of an Operations Manager 2007 database, at least one Operations Manager 2007 Management Server, the Operations Manager 2007 Operator Console, and managed computers.
* Have the Operations Manager 2007 agent deployed on all computers that you want to monitor.

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

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

## Security Considerations for the Windows SharePoint Services 3.0 Management Pack

This section covers security considerations for the Windows SharePoint Services 3.0 Management Pack. To use this Management Pack correctly, you must know:

* How to configure the **Default Action Account** Run As profile with Run As accounts that have the correct privileges.
* Whether the Management Pack can be run in low-privilege environments.
* How to specify user privileges with computer groups.
* Whether the Management Pack provides support for agentless monitoring.

### Configure the Default Action Account Run As Profile

The rules, monitors, and tasks that are defined in the Windows SharePoint Services 3.0 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 agent installed on it.

Note



The agent is an Operations Manager 2007 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 Windows SharePoint Services 3.0 Management Pack, Operations Manager 2007 allows you to use Run As profiles and Run As accounts to provide the needed credentials.

When a Management Pack is created, its rules, monitors, and tasks are associated with Run As profiles; the Windows SharePoint Services 3.0 Management Pack’s rules, monitors, and tasks are associated with the **Default Action Account** Run As profile.

Run As accounts allow you to specify the necessary privileges to run the Management Pack’s 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’s rules, monitors, and tasks.

In order for the Windows SharePoint Services 3.0 Management Pack to have the necessary credentials to run its rules, monitors, and tasks, you must make the following configurations:

* Configurethe **Default Action Account** Run As profile with a Run As account that is associated with a user account that has Windows SharePoint Services administrative privileges and access to the related Windows SharePoint Services databases and application programming interface (API).
* Configure the **Default Action Account** Run As profile for each Windows SharePoint Services server with a Run As account that has Windows SharePoint Services administrative privileges and access to the related Windows SharePoint Services-related databases and API. This allows the **Populate Windows SharePoint Services 3.0 Computer Group** object discovery to populate the Windows SharePoint Services 3.0 computer group.

You must do this because, by default, the **Populate Windows SharePoint Services 3.0 Computer Group** object discovery uses the **Agent Action Account**, which usually does not have the privileges that are necessary to discover the relevant relationships

Using the Run As account that is used for the application pool identity on the SharePoint Central Administration Web site is a best practice.

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

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

### Low-Privilege Environments

This Management Pack cannot run in a low-privilege environment.

### Specify User Privileges with Computer Groups

User roles let you specify privileges for users. In the Windows SharePoint Services 3.0 Management Pack, you can scope and authorize roles by using the **Microsoft Windows SharePoint Services 3.0** computer group.

### Support for Agentless Monitoring

The Windows SharePoint Services 3.0 Management Pack does not contain rules for agentless monitoring.

# Getting Started with the Windows SharePoint Services 3.0 Management Pack

To install the Windows SharePoint Services 3.0 Management Pack, you must download the files to your management server and then import the Management Pack into Operations Manager 2007. After you import the Management Pack, you can create optional configurations for the Operations Manager 2007 agents on your Windows SharePoint Services servers.

## Download the Management Pack Files

Two downloads are available as part of the SharePoint Monitoring Toolkit, one for Microsoft Office SharePoint Server 2007 and one for Windows SharePoint Services 3.0. The Windows SharePoint Services 3.0 Management Pack download package, available from the Microsoft TechNet *Management Pack Catalog* at [http://www.microsoft.com/technet/prodtechnol/mom/catalog/catalog.aspx](http://www.microsoft.com/technet/prodtechnol/mom/catalog/catalog.aspx%20), contains the following files:

* Microsoft.Windows.SharePoint.Services.3.0.mp
* Readme.rtf
* License.rtf
* Windows SharePoint Services 3.0 Management Pack Guide.doc

## Import the Management Pack into Operations Manager 2007

To import the Windows SharePoint Services 3.0 Management Pack



1. Log on to a management server with an account that is a member of the Operations Manager 2007 Administrators role for the Operations Manager 2007 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 opens.
4. If necessary, change to the directory where the Windows SharePoint Services 3.0 Management Pack is located.
5. Select **Microsoft.Windows.SharePoint.Services.3.0.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 Windows SharePoint Services 3.0 Management Pack.

No special configuration of the Management Pack is required after you import it, but you can choose to customize or disable its rules. For information about how to customize the Management Pack or disable its rules, see “[Optional Configuration for the Windows SharePoint Services 3.0 Management Pack](#_Optional_Configuration_for)” in this guide.

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

It is important to ensure that the Operations Manager 2007 agent is deployed on each Windows SharePoint Services 3.0 server that you want to monitor. For information about how to deploy the agent, see “How to Deploy the Operations Manager 2007 Agent for Agent-Management of Computers” in the Operations Manager 2007 Online Help at <http://technet.microsoft.com/en-us/library/bb309622.aspx>.

To configure each server to use the Operations Manager 2007 agent with the Windows SharePoint Services 3.0 Management Pack:

* As a best practice, resize the agent event logs to at least 10 MB each for optimal monitoring.
* If you are monitoring clustered servers, you must disable event log replication on each server within the cluster.

The following sections describe these configuration tasks.

### Resize the Agent Event Logs

The Microsoft Windows SharePoint Services 3.0 Management Pack uses the following event logs to monitor the servers:

* Windows System event log
* Windows Application event log

To resize the agent event logs



1. On each server with an Operations Manager 2007 agent installed on it, open the Event Viewer.
2. In the Event Viewer console tree, click **System** and on the **Action** menu, click **Properties**.
3. On the **General** tab, in **Maximum log size**, specify a log size of at least 10240 KB.
4. To put the new setting into effect, 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 Application event log.

### Disable Event Log Replication for Monitoring Clustered Servers

Some Windows SharePoint Services components can be installed on clustered servers. By default, when clustering is installed on servers that are running Windows 2003 Advanced Server or Windows 2003 Datacenter, events that are 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, event log replication must be disabled on each of the servers within the cluster.

For information about how to disable event log replication, see “How to Configure Event Log Replication in Windows 2000 and Windows Server 2003 Cluster Servers” on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/bb419281.aspx>.

# Optional Configuration for the Windows SharePoint Services 3.0 Management Pack

In a large, dispersed network, you may have Windows SharePoint Services 3.0 deployed in a number of different Management Groups. Because each Management Group contains its own Operations Manager 2007 Management Server, you can install the Windows SharePoint Services 3.0 Management Pack in each Management Group and customize it to focus its rules to collect only the information that is needed for that Management Group environment. You customize the Management Pack by using overrides to reconfigure the default settings of its rules or by disabling rules entirely.

Imported Management Packs such as the Windows SharePoint Services 3.0 Management Pack are sealed; therefore, overrides cannot be saved to them. Instead, Operations Manager 2007 saves the overrides to the unsealed default Management Pack, which is imported as part of the Operations Manager 2007 installation. Sealed Management Packs, have the file extension .mp. These are binary files that cannot be edited. Unsealed Management Packs, 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



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 Windows SharePoint Services 3.0 Management Pack:

1. Create a new unsealed Management Pack to contain the overrides.
2. Override the Windows SharePoint Services 3.0 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 Windows SharePoint Services 3.0 Management Pack to another Management Group.

The detailed procedures for this four-step process follow.

Important



For Operations Manager 2007 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 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” 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 opens.
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 pack that contains the name of the Management Pack that holds the default settings. For example, to override the default settings in the Windows SharePoint Services 3.0 Management Pack, you can create a Management Pack named Windows SharePoint Services 3.0 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, for each parameter that you want to override select the appropriate check box in the **Override** column.
6. When you complete your changes, in the **Select destination management pack** drop-down box select the Management Pack that you created for the overrides.
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 Online Help topics:

* “How to Override a Monitor” at <http://technet.microsoft.com/en-us/library/bb309455.aspx>.
* “Overrides in Operations Manager 2007” 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 XML Management Pack file and is ready to be imported to another Management Group.

Note



You can only export unsealed Management Packs.

To import the new Management Pack and the Windows SharePoint Services 3.0 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 opens.
4. If necessary, change to the directory that holds the Management Pack files.
5. Click **Windows** **SharePoint Services 3.0** **Management** **Pack** and then click **Open**. The **Import Management Packs** dialog box opens.
6. In the **Import** **Management** **Packs** dialog box, click **Add**. The **Select Management Packs to Import** dialog box opens 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 also be situations in which you might decide not to collect certain warnings, performance data, or miscellaneous non-critical events. These 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.

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 Online Help at <http://technet.microsoft.com/en-us/library/bb309583.aspx>.

# Understanding the Windows SharePoint Services 3.0 Management Pack Operations

This section describes the objects that the Windows SharePoint Services 3.0 Management Pack discovers, how health rolls up, key monitoring scenarios, and how health is defined and indicated.

## Objects the Windows SharePoint Services 3.0 Management Pack Discovers

The purpose of the Windows SharePoint Services 3.0 Management Pack is to discover and monitor specific objects—Windows SharePoint Services 3.0 components—in your network environment. The Windows SharePoint Services 3.0 Management Pack discovers the following objects:

* Microsoft Windows SharePoint Services 3.0 Computer Group
* Microsoft Windows SharePoint Services 3.0 Application Installation
* Microsoft Windows SharePoint Services 3.0 WSS Server

## Understanding Health Monitoring

One of the most important features of the Windows SharePoint Services 3.0 Management Pack is its ability to monitor the health of your Windows SharePoint Services 3.0 environment. The Management Pack uses monitors to continually assess the health state of monitored components, such as Windows SharePoint Services 3.0 Search 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 monitors, lists the monitors that the Windows SharePoint Services 3.0 Management Pack contains, explains how the roll up of the monitors for a Windows SharePoint Services 3.0 component determines its overall health, and describes how health is indicated in the Operations Console.

### About the Windows SharePoint Services 3.0 Management Pack Monitors

There are various types of monitors that are available in Operations Manager 2007. The Windows SharePoint Services 3.0 Management Pack contains the following two types of monitors:

* Unit monitors
* Aggregate rollup monitors

Tables 1 and 2 list the monitors that the Windows SharePoint Services 3.0 Management Pack contains and describe the components that they assess.

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

Table 1. Windows SharePoint Services 3.0 Management Pack Unit Monitors

| **Monitor Name** | **Description** |
| --- | --- |
| The Windows SharePoint Services Tracing Service State | Monitors the state of the Tracing service and generates an alert if the monitor is in a critical health state |
| The Windows SharePoint Services Timer Service State | Monitors the state of the Timer service and generates an alert if the monitor is in a critical health state |
| The Windows SharePoint Services Search Service State | Monitors the state of the Search service and generates an alert if the monitor is in a critical health state |
| The Microsoft Internet Information Services State | Monitors the service health of the IIS service |
| SQL Server Connection State | Monitors the state of the SQL Server connection |
| SQL Server Database Error | Monitors SQL Server Database error events |
| Plug in Connection to SQL Server | Monitors failure of Plug in Connect ion to SQL Server error events |
| Insufficient SQL Server Database Permissions | Monitors Insufficient SQL Server Database Permissions error events |
| SQL Server Database Space | Monitors the full SQL Server Database error event |

Aggregate rollup monitors are used to group one or more monitors into one monitor that is then used to set the health state and generate an alert.

Important



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

* SQL Server Connection State
* SQL Server Database Error
* Plug in Connection to SQL Server
* Insufficient SQL Server Database Permissions
* SQL Server Database Space

Table 2. Windows SharePoint Services 3.0 Management Pack Aggregate Rollup Monitors

| **Monitor Name** | **Description** |
| --- | --- |
| WSS 3.0 Server Entity State | Monitors the WSS 3.0 Server Entity state |
| Tracing | Monitors the WSS Tracing service |
| Timer | Monitors the WSS Timing service |
| Search | Monitors the WSS Search service |
| IIS | Monitors the IIS Search service |
| SQL Server Connection | Monitors the SQL Server connection |
| SQL Server Database Error | Monitors SQL Server Database errors |
| Plug in Connection to SQL Server | Monitors the Plug in connection to SQL Server |
| SQL Server Database Permissions | Monitors SQL Server Database permissions |
| SQL Server Database Space | Monitors the full SQL Server Database error event |

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

To view the Windows SharePoint Services 3.0 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 Windows SharePoint Services 3.0 Management Pack regards the services of Windows SharePoint Services 3.0 as a hierarchy. The health of each level depends on the health of the level below it.

* The top level aggregate monitor is the Windows SharePoint Services 3.0 Server Entity State, which represents the health of the WSS server.
* At the second level are aggregate rollup monitors, which each have individual unit monitors assigned to them. Their function is to interpret the health state of the unit monitor and roll it up to the top level.
* At the bottom level are unit monitors, which monitor services and events.

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 your Windows SharePoint Server 3.0 environment’s health. Operations Manager 2007 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

|  |  |
| --- | --- |
|  | Indicates that all services are running correctly and that the server is available. |
|  | Indicates that there may be an issue with one or more services or that the server itself may be unavailable. |
|  | 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 Windows SharePoint Services 3.0 Management Pack collects.

Table 4 lists the key Windows SharePoint Services 3.0 Management Pack monitoring scenarios.

Table 4. Windows SharePoint Services 3.0 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. |
| Information Rights Management | Monitors connectivity with Information Rights Management servers. |
| 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:   * Windows SharePoint Services Timer * Windows SharePoint Services Tracing * Windows SharePoint Services 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 Windows SharePoint Services 3.0 Management Pack rules collect data that its monitored components generate. The rules are grouped into categories that are based on these components. The Windows SharePoint Services 3.0 Management Pack rule categories are:

* Search Service
* SQL Server Database
* System Performance
* Web Server Performance
* Windows Services
* Windows SharePoint Services 3.0 Application

For descriptions of the rule categories and a complete list of the Windows SharePoint Services 3.0 Management Pack rules, see [Appendix B](#_Appendix_B:_Windows) in this guide.

**To view the Windows SharePoint Services 3.0 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” in the Operations Manager 2007 Online Help at <http://technet.microsoft.com/en-us/library/bb381367.aspx>.

## Understanding Tasks

Tasks are actions that diagnose or repair a problem. The Windows SharePoint Services 3.0 Management Pack includes the tasks that are shown in Table 5.

Table 5. Windows SharePoint Services 3.0 Management Pack Tasks

|  |  |
| --- | --- |
| **Task** | **Description** |
| Start WSS Tracing Service | Starts the Windows SharePoint Services Tracing service |
| Start WSS Timer Service | Starts the Windows SharePoint Services Timer service |
| Start WSS Search Service | Starts the Windows SharePoint Services Search service |
| Windows SharePoint Services 3.0 IIS Reset | Starts the IIS Reset utility |

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

To view the Windows SharePoint Services 3.0 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 Windows SharePoint Services 3.0 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 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 Operations Console

The Operations Console is the main user interface for Operations Manager 2007, with navigation buttons that enable you to access to the **Monitoring**, **Authoring**, **Reporting**, **Administration**, and **My** **Workspace** panes. Figure 1 shows the Operations Console and the navigation buttons.

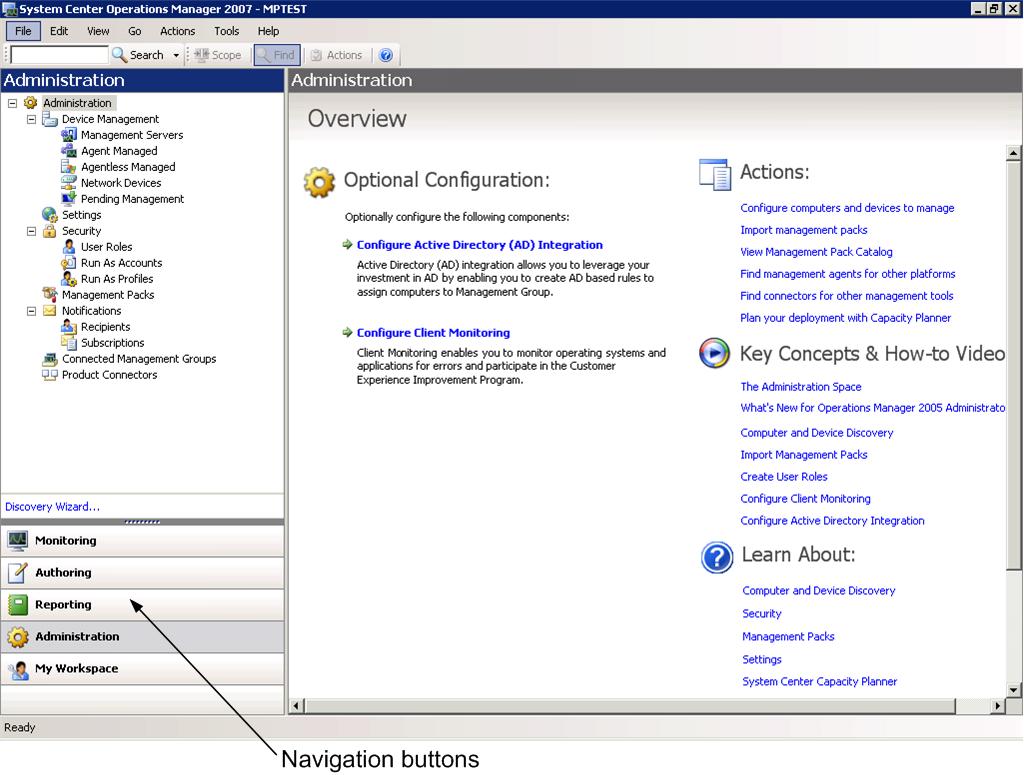


Figure 1. Navigation buttons on the Operations Console

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 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 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” in the Operations Manager 2007 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 your Windows SharePoint Services 3.0 environment. This section describes the Windows SharePoint Services 3.0 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.

#### Windows SharePoint Services 3.0 Management Pack Views

This Management Pack has the following views:

* The **Alerts** view lists the alerts that are generated by the Management Pack rules.
* The **Diagram** view displays a graphical view of the Windows SharePoint Services 3.0 components monitored by the Management Pack and how they relate to each other. In this view, you can right-click a Windows SharePoint Services 3.0 component to perform tasks that are related to that component.
* The **Events** view lists the events that are recorded in the event logs of the servers in your Windows SharePoint Services 3.0 environment.
* The **Performance** view displays data that is collected from the Management Pack performance rules.
* The **Server Inventory** view displays all of the Windows SharePoint Services 3.0 servers discovered by the Management Pack.
* The **State** view displays relationships between Windows SharePoint Services 3.0 components, computers, and computer groups.
* The **Task** **Status** view displays the status of the Management Pack tasks.

To select a view



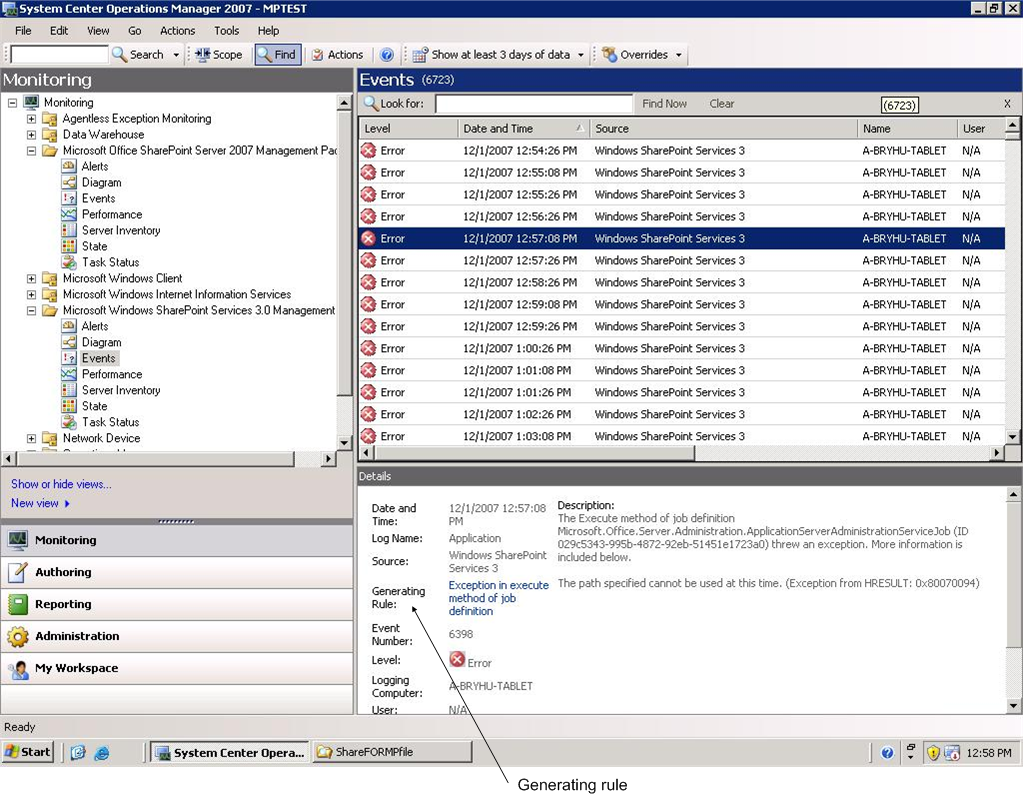
1. In the Monitoring pane of the Operations Console, expand Monitoring.
2. Expand Microsoft Windows SharePoint Services 3.0 Management Pack.
3. Click a view.

To view detailed information about a particular alert or event



1. In the Monitoring pane of the Operations Console, expand Monitoring.
2. Expand Microsoft Windows SharePoint Services 3.0 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.



**Figure 2. Generating rule for an event or alert**

1. In the **Properties** dialog box, click the **Product** **Knowledge** tab.

Figure 3 shows an example of the **Product Knowledge** tab in the **Properties** dialog box.

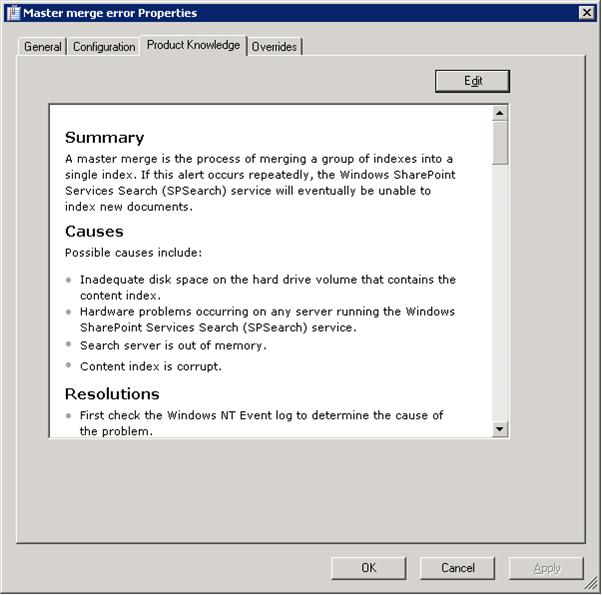


Figure 3. Product Knowledge tab of the Properties dialog box

For more information, see “Views in Operations Manager 2007” in the Operations Manager 2007 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 Online Help topics:

* “How to Create a State View in Operations Manager 2007” 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 Windows SharePoint Services 3.0 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 Microsoft Office SharePoint Server 3.0 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"](#_Viewing_Status_and) in this guide.

### Viewing Management Pack Rules in the Authoring Pane

You can view the Windows SharePoint Services 3.0 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 Windows SharePoint Services 3.0 Management Pack"](#_Optional_Configuration_for) in this guide.

To view the Management Pack rules



1. In the Operations Console, click the **Authoring** button.
2. In the Authoring pane, expand Management Pack Objects.
3. Expand **Rules**. The rules are displayed in the **Rules** pane.
4. On the **Operations** **Manager** toolbar, click the **Scope** button. The **Scope Management Packs by targets(s)** dialog box opens.
5. In the **Target** column, select the **Microsoft Office SharePoint Services 3.0 WSS Server** and the **Microsoft** **Windows SharePoint Services 3.0 Computer Role**, and then click **OK**. This allows only the rules for the Windows SharePoint Services 3.0 Management Pack to be displayed in the **Rules** pane.

Important



This works correctly only if all other check boxes in the **Targets** column are clear.

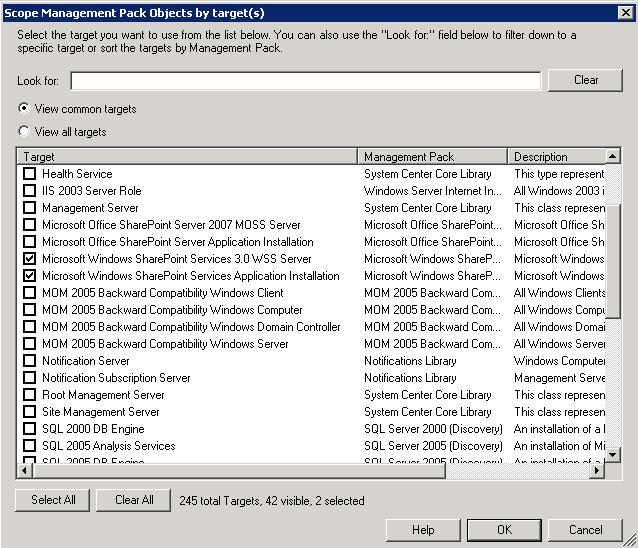


Figure 4. Selecting the list of rules in the Target column

1. In the **Rules** pane, click a rule. More information about the rule appears in the **Rule Details** pane.
2. In the **Rule Details** pane, click the **View Knowledge** link to open the **Properties** dialog box for the rule.

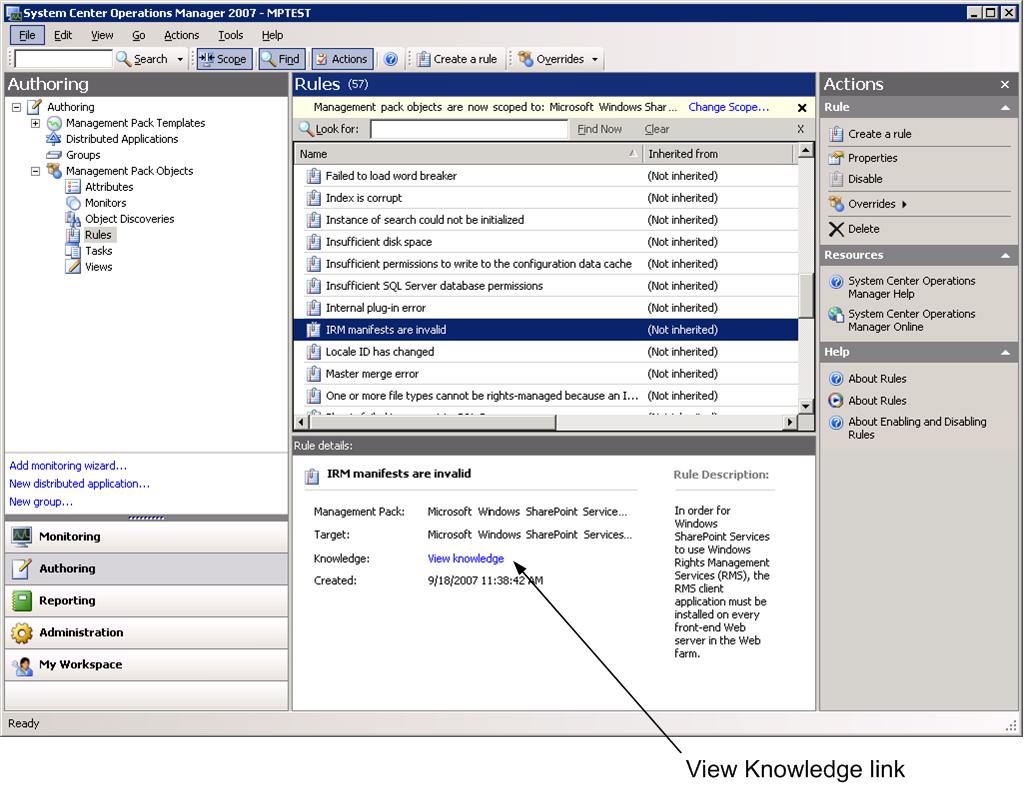


Figure 5. View Knowledge link in the Rule Details pane

### Viewing Management Pack Attributes in the Authoring Pane

Attributes are properties that define a commonality within a group of components that are monitored by a Management Pack. This Management Pack collects the following attributes:

* Microsoft Windows SharePoint Services 3.0 Server Role
* Display Name
* Server\_Name

For more information, see “Attributes in Operations Manager 2007” in the Operations Manager 2007 Online Help at <http://technet.microsoft.com/en-us/library/bb309538.aspx>.

To view the Management Pack attributes



1. In the Operations Console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Attributes**. The attributes appear in the **Attributes** pane. The **Management Pack** column lists the attributes that belong to the Microsoft Office SharePoint Server Management Pack.
3. To view more information in the **Attribute Details** pane, click any attribute.

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

In Operations Manager 2007, 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” in the Operations Manager 2007 Online Help at <http://technet.microsoft.com/en-us/library/bb381270.aspx>.

Table 6 lists the object discoveries that are included in the Windows SharePoint Services 3.0 Management Pack.

Table 6. Windows SharePoint Services 3.0 Management Pack Object Discoveries

| Object Discovery Name | Description |
| --- | --- |
| Windows SharePoint Services 3.0 Computer Group | Populates the Windows SharePoint Services 3.0 computer group |
| Microsoft Windows SharePoint Services 3.0 Application Installation Discovery | Discovers the objects of the Microsoft Windows SharePoint Services Application Installation |
| WSS 3.0 Server Script Discovery | Discovers the objects of the Windows SharePoint Services 3.0 Server |

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 Windows SharePoint Services 3.0 Management Pack.
3. To view more information in the **Object Discovery Details** pane, click any object discovery.

# Using the Windows SharePoint Services 3.0 Management Pack Reports

To look at trends in your environment across days, weeks, or months, you can use the Windows SharePoint Services 3.0 Management Pack reports. This section:

* Describes how to select a Windows SharePoint Services 3.0 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 Windows SharePoint Services 3.0 Management Pack**.
4. In the **Reports** pane, click a report and then click the **Open** button.

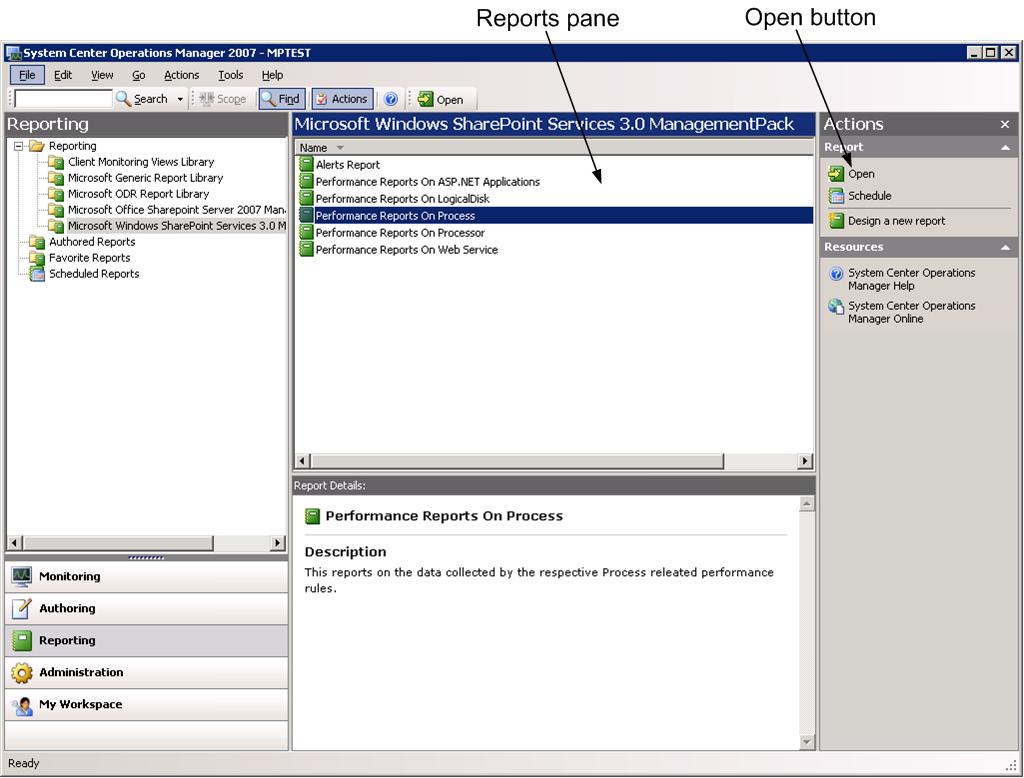


Figure 6. Reports pane

1. A dialog box that displays the parameters for the selected report opens.

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” in the Operations Manager 2007 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. Figure 7 shows an example of an alert report.

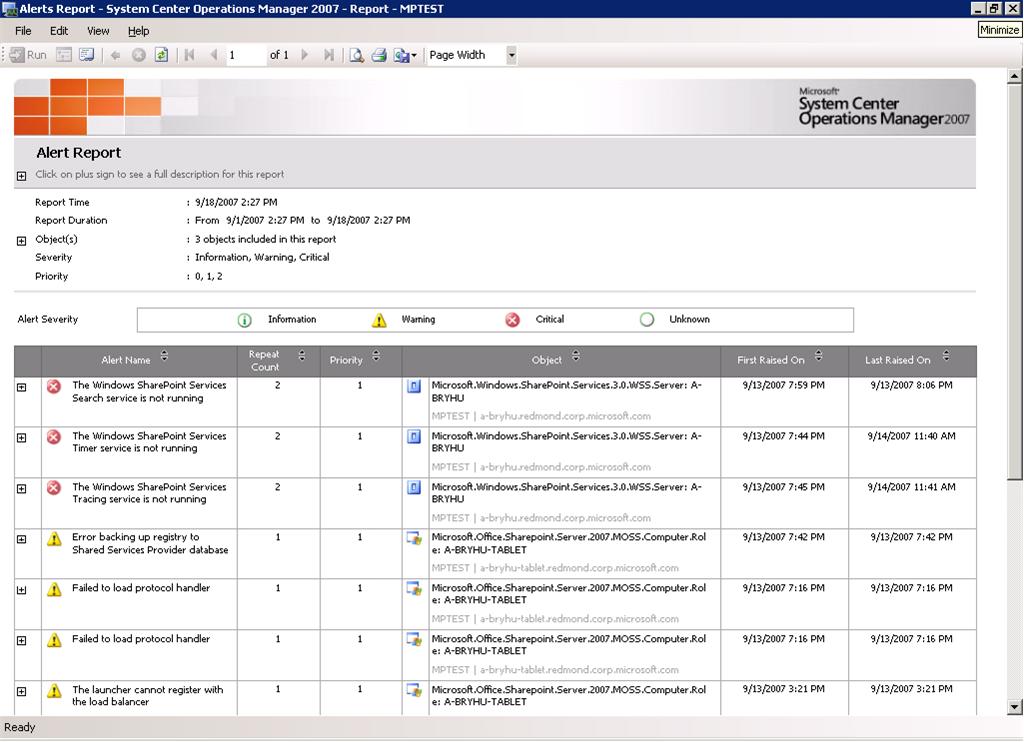


Figure 7. Example of an Alerts report

## Report Descriptions

The Windows SharePoint Services 3.0 Management Pack provides the following reports:

* Alert report
* Most Common Alerts report
* Event Analysis report
* Most Common Events report
* ASP .NET Applications Performance report
* Logical Disk Performance report
* Process Performance report
* Processor Performance report
* Web Service Performance report

These reports and the rules that collect the data for them are described in the following sections. For detailed information about the rules, see [Appendix B](#_Appendix_B:_Windows) in this guide.

### Alerts Report

This report displays the alerts that have occurred for selected Windows SharePoint Services 3.0 components during the report period.

### Most Common Alerts Report

This report displays the most common alerts that are collected by the Windows SharePoint Services 3.0 Management Pack during the specified time period.

### Event Analysis Report

This report displays detailed information about the events that are collected by the Windows SharePoint Services 3.0 Management Pack during the specified time period.

### Most Common Events Report

This report displays the most common events that are collected by the Windows SharePoint Services 3.0 Management Pack during the report period. You can use this report to analyze trends and discover potential problem areas.

### ASP .NET Applications Performance Report

This report displays data that is collected by the following Windows SharePoint Services 3.0 Management Pack ASP .NET applications performance rule.

Table 7. ASP.NET Applications Performance Data Rules

|  |  |
| --- | --- |
| **Rule** | **Description** |
| ASP .NET worker process restarts on the Web server | Collects and reports performance data from the Windows Server® 2003 performance counter that indicates the number of times a worker process has restarted on the server |

### Logical Disk Performance Report

This report displays the data that is collected by the following Windows SharePoint Services 3.0 Management Pack logical disk performance rules.

Table 8. Logical Disk Performance Report Rules

|  |  |
| --- | --- |
| **Rule** | **Description** |
| WFE Disk Space | Calculates the percentage of total usable space on the selected logical disk drive |

### Process Performance Report

This report displays data that is collected by the following Windows SharePoint Services 3.0 Management Pack process performance rules.

Table 9. Process Performance Report Rules

| **Rule** | **Description** |
| --- | --- |
| Excessive CPU Utilization | Calculates the percentage of elapsed time of all the process threads used by the processor to execute instructions |

### Processor Performance Report

This report displays data that is collected by the following Windows SharePoint Services 3.0 Management Pack processor performance rules.

Table 10. Processor Performance Report Rules

| **Rule** | **Description** |
| --- | --- |
| Excessive Usage | Calculates the percentage of the elapsed time that the processor spends to execute a non-idle thread |

### Web Service Performance Report

This report displays data that is collected by the following Windows SharePoint Services 3.0 Management Pack Web service performance rules.

Table 11. Web Service Performance Report Rules

| **Rule** | **Description** |
| --- | --- |
| Current ISAPI request per sec to the SharePoint server | Collects and reports performance data from the Windows Server 2003 performance counter that indicates the rate of ISAPI Extension requests received by Windows SharePoint Services 3.0 |
| Current total ISAPI connections to the SharePoint Server | Collects and reports performance data from the Windows Server 2003performance counter that indicates the current number of ISAPI requests that Windows SharePoint Services 3.0 is processing simultaneously |

# Appendix A: Troubleshooting the Windows SharePoint Services 3.0 Management Pack

This section describes issues that can occur with the Windows SharePoint Services 3.0 Management Pack, and presents possible resolutions. The issues covered are:

* A series of warnings and errors from performance rules appear in the Events view.
* The alert description on the **General** tab of the **Alert Properties** dialog box is truncated.
* The performance collection rules do not display when you first use the Management Pack after you install it.
* After upgrading to Windows SharePoint Services 3.0 SP1, alerts appear in the **Alerts** pane and the SharePoint server is set to an unhealthy state.

#### A series of Warnings and Errors appear in the Windows Event Viewer and in the default SCOM Event View, telling the user that a counter could not be resolved, and the module will be unloaded.

**Cause:** These errors occur when a performance rule fails to resolve towards its target Object, Counter, or Instance when the target is not available or applicable on the agent machine. They can occur in the following circumstances:

* During the initial process of loading the performance rules after the Management Pack is installed.
* When the Root Management Server and the agent machines are in an out-of-sync state.
* When a client, agent, or target machine is temporarily disconnected from the Operations Manager 2007 Management Server (RMS) and then reconnected.
* A number of other scenarios, including when there are network issues, or when a client machine is turned off and then back on again.

**Resolution:** No action is required. When a performance rule fails to load in any of these scenarios, it is automatically unloaded with a Warning or Error. The error description contains the workflow name that is affected by the error.  The rules stay unloaded as long as they remain inapplicable to the agent machine’s environment. The rules will load automatically once they are able to resolve towards their target Object, Counter, or Instance.

#### The alert description on the General tab of the Alert Properties dialog box is truncated.

**Cause:** This is a function of Operations Manager 2007 and cannot be changed.

**Resolution:** Close the **Alert Properties** dialog box andclick the alert in the **Alerts** pane.Use the scroll bar to view the entire alert description.

#### The performance collection rules do not display when you first use the Management Pack after you install it.

**Cause:** This may occur when the Management Pack creates the **Performance** view before it finished loading the performance rules.

**Resolution:** Wait at least one to two hours for the performance rules to poll the data, then check to see if the performance rules are displayed. If not, check the **Time Range** parameter to see if it is set to a date prior to the installation of the Management Pack. This can happen if the values in the **Time Range** dialog box have been cached from a previous Management Pack. To resolve this, you must edit the **Time Range** parameter to a date that is after the Management Pack was installed.

To edit the Select Time Range parameter



1. In the Operations Console, click the **Monitoring** button.
2. In the Monitoring pane, expand **Monitoring.**
3. Expand Windows SharePoint Services 3.0 Management Pack.
4. Click the **Performance** view.
5. In the **Performance** pane, right-click and then click **Select time range**. The **Time Range** dialog box opens.
6. In the **Time Range** dialog box, select a time range that begins after the Management Pack was installed, and then click **OK**.

Alternatively, after discovery is complete you can delete the Performance view and then create a new one.

**To delete the Performance view**



1. In the Operations Console, click the **Monitoring** button.
2. In the Monitoring pane, expand **Monitoring.**
3. Expand Windows SharePoint Services 3.0 Management Pack.
4. Right-click **Performance** and then click **Delete**.
5. Click **Yes** in the dialog box that appears.

To create a new Performance view



1. In the Operations Console, click the **Monitoring** button.
2. In the Monitoring pane, right-click **Monitoring**, point to **New**, and then click **Performance**.
3. In the **Properties** dialog box, type **Performance** in the **Name** box and type a description of the view in the **Description** box.
4. On the **Criteria** tab, click the ellipses (**…**) next to the **Show data related to** box. The **Select a Target Type** dialog box displays a list of the object types available in your Management Group.
5. Click **Windows SharePoint Services 3.0 WSS Server** and then click **OK**.
6. Click **OK**.

#### After you upgrade to Windows SharePoint Services 3.0 SP1, alerts display in the Alerts pane and the SharePoint server is set to an unhealthy state.

**Cause:** This is a known issue with the Windows SharePoint Services 3.0 SP1 patch. The alerts that appear are:

* Timer Job exception in event log during SP1 patch setup
* SQL Exception 15023 in event log after applying patch

These alerts are false; the server is actually in healthy, not unhealthy, state.

**Resolution:** Currently there is no resolution to this issue; just be aware that these false alerts will occur when you upgrade to SP1.

# 

# Appendix B: Windows SharePoint Services 3.0 Management Pack Rules

The rules in this Management Pack collect data, such as events, that the servers in your Windows SharePoint Services 3.0 environment generate. Many of the rules also generate alerts when the data they collect indicates a problem with the health state of your environment. This appendix lists all of the rules contained in the Windows SharePoint Services 3.0 Management Pack, and provides the following information for each rule:

* Name
* Rule ID
* Description
* Category
* Rule target
* Alert type
* Event ID for event collection rules
* Event source for event collection rules

## Rule Categories

In order to make it easier for you to find the information you need, the rules are categorized by function. For example, all rules that pertain to searching, crawling, and indexing have been placed in the Search rule category. Table 12 lists the names of the rule category and the types of rules that are included in each category.

Table 12. Rule Categories

| **Rule Categories** | **Includes** |
| --- | --- |
| Search Service | Search Indexing Crawling |
| SQL Server Database | SQL Server Database |
| System Performance | Processor Memory Logical Disk Physical Disk  Process |
| Web Server Performance | ASP .NET CLR IIS W3WP SMTP Web Service |
| Windows Services | Timer Service Tracing Service  Service Not Running |
| Windows SharePoint Services 3.0 Application | Active Directory SharePoint Sites SharePoint Administration Service Information Rights Management (IRM) Rights Management Services (RMS) |

## Search Rules

| **Rule Name** | **Rule Properties** |
| --- | --- |
| Crawler cannot read from registry | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Crawler\_cannot\_read\_from\_registry  **Description:** This alert indicates that the crawler was unable to read from the registry in order to load configuration information needed by the SharePoint Services Search service.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 2438  **Event Source:** Windows SharePoint Services 3 Search |
| Crawler exception | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Crawler\_exception  **Description:** The crawler component of search uses the Windows SharePoint Services Search service to read its settings from the Windows registry of the search server. This alert indicates that an unexpected error has occurred in the crawler.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 2414  **Event Source:** Windows SharePoint Services 3 Search |
| Failed to load index | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Failed\_to\_load\_index  **Description:** This alert indicates that the Windows SharePoint Services Search service could not load the index. This can happen because the search service is paused or stopped, or the index is corrupt or missing.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 7043  **Event Source:** Windows SharePoint Services 3 Search |
| Failed to load word breaker | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Failed\_to\_load\_word\_breaker  **Description:** This alert indicates that a particular word breaker could not be loaded and, therefore, documents that require this word breaker will be crawled using a language-neutral word breaker.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 2462  **Event Source:** Windows SharePoint Services 3 Search |
| Index is corrupt | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Index\_is\_corrupt  **Description:** The Windows SharePoint Services Search service has detected that the content index is corrupted. This can occur on either an index server or a query server. When this error occurs on an index server, the search service automatically attempts to reset and start a full update of the content index.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 4138  **Event Source:** Windows SharePoint Services 3 Search |
| Instance of search could not be initialized | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Instance\_of\_search\_could\_not\_be\_initialized  **Description:** This alert indicates that the configuration information for search could not be loaded from the SQL Server database, which prevented an instance of the SharePoint Services Search service from initializing.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 2458  **Event Source:** Windows SharePoint Services 3 Search |
| Internal plug-in error | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Internal\_plug\_in\_error  **Description:** This error indicates that the search server is out of memory or that there is an unexpected problem with the search server plug-in.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 9502  **Event Source:** Windows SharePoint Services 3 Search |
| Master merge error | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Master\_merge\_error  **Description:** This alert indicates that an error has occurred during a master merge, which is the process of merging a group of indexes into a single index. If this alert occurs repeatedly, the Windows SharePoint Services Search service will eventually be unable to index new documents.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 4105, 4106  **Event Source:** Windows SharePoint Services 3 Search |
| Plug-in failed to connect to SQL Server | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Plug\_in\_failed\_to\_connect\_to\_SQL\_Server  **Description:** This alert indicates that an error occurred in the Windows SharePoint Search service. The plug-in did not connect to the SQL Server instance listed in the Windows NT Event log and the update of the content source cannot continue.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 9503, 9510  **Event Source:** Windows SharePoint Services 3 Search |

## 

## SQL Server Database Rules

| **Rule Name** | **Rule Properties** |
| --- | --- |
| Cannot connect to SQL Server | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Cannot\_connect\_to\_SQL\_Server  **Description:** This alert indicates that Windows SharePoint Services could not connect to the SQL Server database.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 3355  **Event Source:** Windows SharePoint Services 3 |
| Insufficient SQL Server database permissions | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Insufficient\_SQL\_Server\_database\_permissions  **Description:** This error typically occurs during when insufficient privileges have been granted in the SQL Server database to the service account specified in Windows SharePoint Services.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 5214  **Event Source:** Windows SharePoint Services 3 |
| SQL Server Database Error | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.SQL\_Server\_Database\_Error  **Description:** This alert indicates that an unexpected SQL Server database error occurred while the Windows SharePoint Services Search attempted to communicate with the database.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 9511  **Event Source:** Windows SharePoint Services 3 Search |
| SQL Server database is full | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.SQL\_Server\_database\_is\_full  **Description:** This alert indicates that a SQL Server error occurred because the database size limit has been reached.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 3758  **Event Source:** Windows SharePoint Services 3 |
| SQL Server database login failed | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.SQL\_Server\_database\_login\_failed  **Description:** This alert indicates that the user name or password for the Windows SharePoint Services service account was invalid before the session or became invalid during the session.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 3351  **Event Source:** Windows SharePoint Services 3 |
| Unknown SQL Exceptions | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Unknown\_SQL\_Exceptions  **Description:** This rule triggers an alert whenever any unknown SQL exceptions occur. The details of the exception are displayed in the alert.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 5586  **Event Source:** Windows SharePoint Services 3 |

## System Performance Rules

| **Rule Name** | **Rule Properties** |
| --- | --- |
| Current ISAPI request per sec to the SharePoint server | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Current\_ISAPI\_request\_per\_sec\_to\_the\_SharePoint\_server  **Description:** This rule uses the ISAPI Extension Requests/sec counter to measure the rate at which ISAPI Extension requests are received by the Web service.  **Rule Category:**  Performance Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Not applicable |
| Current total ISAPI connections to the SharePoint server | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Current\_total\_ISAPI\_connections\_to\_the\_SharePoint\_server  **Description:** This rule uses the Current ISAPI Extension Requests counter to count the current number of ISAPI requests that are simultaneously processed by the Web service.  **Rule Category:** Performance Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Not applicable |
| Excessive CPU Utilization | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Excessive\_CPU\_Utilization  **Description:** This rule uses the % Processor Time counter to calculate the percentage of the elapsed time of all of the process threads used by the processor to execute instructions. An instruction is the basic unit of execution in a computer, a thread is the object that executes instructions, and a process is the object created when a program is run. Code executed to handle some hardware interrupts and trap conditions are included in this count.  **Rule Category:** Performance Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Not applicable |
| Excessive Usage | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Excessive\_Usage  **Description:** This rule uses the % Processor Time counter to calculate the percentage of the elapsed time that the processor spends to execute a non-Idle thread. The calculation measures the duration that the idle thread is active in the sample interval, and subtracts that time from the interval duration. (Each processor has an idle thread that consumes cycles when no other threads are ready to run.) This counter is the primary indicator of processor activity, and displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time that the service is inactive and subtracting that value from 100%.  **Rule Category:** Performance Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Not applicable |
| Insufficient disk space | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Insufficient\_disk\_space  **Description:** This alert indicates that the hard disk on which the content index files reside is full. The crawl will automatically resume after sufficient hard disk space becomes available.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 7013  **Event Source:** Windows SharePoint Services 3 Search |
| WFE Disk Space | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.WFE\_Disk\_Space  **Description:** This rule uses the % Free Space counter to calculate the percentage of total usable space on the selected logical disk drive.  **Rule Category:** Performance Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Not applicable |

## Web Server Rules

| **Rule Name** | **Rule Properties** |
| --- | --- |
| Access denied for writing to registry | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Access\_denied\_for\_writing\_to\_registry  **Description:** This error occurs when the application pool used by Windows SharePoint Services 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.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6589  **Event Source:** Windows SharePoint Services 3 |
| Access denied for writing to disk | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Access\_denied\_for\_writing\_to\_disk  **Description:** This error occurs when the application pool used by Windows SharePoint Services 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.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6589  **Event Source:** Windows SharePoint Services 3 |
| An error occurred while communicating with the SMTP server | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.An\_error\_occurred\_while\_communicating\_with\_the\_SMTP\_server  **Description:** This error typically occurs due to a misconfigured SMTP server.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 6858  **Event Source:** Windows SharePoint Services 3 |
| ASP.NET worker process restarts on the Web server | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.ASP.NET\_worker\_process\_restarts\_on\_the\_Web\_server  **Description:** This rule uses the **Worker Process Restarts** counter to count the number of times a worker process has restarted on the server.  **Rule Category:** Performance Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Not applicable |
| Cannot connect to SMTP host | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Cannot\_connect\_to\_SMTP\_host  **Description:** This alert indicates that Windows SharePoint Services cannot connect to the Simple Mail Transfer Protocol (SMTP) host.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6857  **Event Source:** Windows SharePoint Services 3 |
| Cannot resolve name of the outbound SMTP server | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Cannot\_resolve\_name\_of\_the\_outbound\_SMTP\_server  **Description:** This alert indicates that Windows SharePoint Services 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.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6856  **Event Source:** Windows SharePoint Services 3 |
| The application pool account must be registered as a Kerberos service provider | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.The\_application\_pool\_account\_must\_be\_registered\_as\_a\_Kerberos \_service\_provider  **Description:** 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.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 6590  **Event Source:** Windows SharePoint Services 3 |

## 

## Windows Services Rules

| **Rule Name** | **Rule Properties** |
| --- | --- |
| Alternate access mapping update failed | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Alternate\_access\_mapping\_update\_failed  **Description:** This error occurs when the timer job used to update alternate access mappings failed on the specified server.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6397  **Event Source:** Windows SharePoint Services 3 |
| The Windows SharePoint Services Search service is not running | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.The\_Windows\_SharePoint\_Services\_Search\_service\_state  **Description:** This alert indicates that the Windows SharePoint Search service is not running. This can happen because the administrator stopped the service or the Startup Type of the service was set to manual and the computer was restarted.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Information  **Event ID:** 21207  **Event Source:** Microsoft Operations Manager (SPSearch) |
| The Windows SharePoint Services Timer service is not running | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.The\_Windows\_SharePoint\_Services\_Timer\_service\_state  **Description:** This alert indicates that the Windows SharePoint Services Timer service is not running. This can happen because the administrator stopped the Windows SharePoint Services Timer service or the Startup Type of the service was set to manual and the computer was restarted.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Information  **Event ID:**  21207  **Event Source:** Microsoft Operations Manager (SPTimer) |
| The Windows SharePoint Services Tracing service is not running | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.The\_Windows\_SharePoint\_Services\_Tracing\_service\_state  **Description:** This alert indicates that the Windows SharePoint Services Tracing service is not running.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 21207  **Event Source:** Microsoft Operations Manager(SPTracer) |
| Unable to create a log file | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Unable\_to\_create\_a\_log\_file  **Description:** This alert indicates that the Windows SharePoint Services Tracing service could not create a log file.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 3250  **Event Source:** Windows SharePoint Services 3 |
| Unable to load authentication provider | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Unable\_to\_load\_authentication\_provider  **Description:** This error indicates that the Role Manager or membership Provider that is specified for a particular Web application is incorrectly configured.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6143  **Event Source:** Windows SharePoint Services 3 |
| Unable to write to trace log | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Unable\_to\_write\_to\_trace\_log  **Description:** This alert indicates that Windows SharePoint Services 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.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 5401  **Event Source:** Windows SharePoint Services 3 |

## Windows SharePoint Services 3.0 Application Rules

| **Rule Name** | **Rule Properties** |
| --- | --- |
| An RMS server refused access to a computer running Windows SharePoint Services | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.An\_RMS\_server\_refused\_access\_to\_a\_computer\_running\_Windows \_SharePoint Services  **Description:** This alert indicates that a front-end Web server contacted the Rights Management Services (RMS) server but the RMS server denied access to the Web server. Generally, this error occurs when an administrator is first enabling Information Rights Management (IRM) for the Web farm in Central Administration. If this is the case, IRM cannot be enabled in Central Administration and list administrators will not be able to enable IRM on a document library or list until the error is resolved. If this error occurs after IRM is enables, downloads from a rights-managed list or library will fail until the error is resolved.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 5056, 5127, 5133, 5106, 5112, 5091, 5097  **Event Source:** Windows SharePoint Services 3 |
| Backup failed due to insufficient permissions | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Backup\_failed\_due\_to\_insufficient\_permissions  **Description:** Backup of a Web site failed because the administrator had inadequate permissions to perform a backup to a file share or folder on the local server, or to the SQL Server database.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 3353  **Event Source:** Windows SharePoint Services 3 |
| Backup failed due to timer job failure | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Backup\_failed\_due\_to\_timer\_job\_failure  **Description:** This alert indicates that the Windows SharePoint Services timer job used to perform the backup of a site failed.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 7035  **Event Source:** Windows SharePoint Services 3 |
| Cannot establish a connection with a Windows Rights Management Services (RMS) server | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Cannot\_establish\_a\_connection\_with\_a\_Windows\_Rights\_Management \_Services\_\_RMS\_\_server  **Description:** This alert indicates that Windows SharePoint Services could not connect to the specified Rights Management Services (RMS) server.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 5047, 5048, 5049, 5059, 5060, 5058, 5105, 5131, 5111, 5089, 5068, 5070, 5095  **Event Source:** Windows SharePoint Services 3 |
| Event handler failed to load | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Event\_handler\_failed\_to\_load  **Description:** This alert indicates that 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.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6644  **Event Source:** Windows SharePoint Services 3 |
| Exception in execute method of job definition | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Exception\_in\_execute\_method\_of\_job\_definition  **Description:** This alert indicates that an exception occurred in the execute method of the job definition for a particular timer job.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6398  **Event Source:** Windows SharePoint Services 3 |
| Exception loading timer job definition | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Exception\_loading\_timer\_job\_definition  **Description:** This alert indicates that an exception occurred when Windows SharePoint Services attempted to load a timer job definition.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6396  **Event Source:** Windows SharePoint Services 3 |
| Failed to create a SharePoint site | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Failed\_to\_create\_a\_SharePoint\_site  **Description:** This alert indicates that an attempt to create a new SharePoint site has failed.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6141  **Event Source:** Windows SharePoint Services 3 |
| Failed to load protocol handler | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Failed\_to\_load\_protocol\_handler  **Description:** This alert indicates that the Windows SharePoint Services protocol handler, which is used to access content that you want to crawl, cannot be loaded. This means that documents that require the protocol handler cannot be crawled.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 2483, 2484  **Event Source:** Windows SharePoint Services 3 Search |
| Failed to load safe control assembly path | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Failed\_to\_load\_safe\_control\_assembly\_path  **Description:** This error indicates that that the identified safe control Web part is not installed on the server.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6611  **Event Source:** Windows SharePoint Services 3 |
| Insufficient permissions to write to the configuration data cache | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Insufficient\_permissions\_to\_write\_to\_the\_configuration\_data\_cache  **Description:** This alert indicates that the permissions on the %systemdrive%\inetpub\wwwroot\wss\config folder where the Windows SharePoint Services configuration data cache is stored have been changed.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 6395  **Event Source:** Windows SharePoint Services 3 |
| IRM manifests are invalid | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.IRM\_manifests\_are\_invalid  **Description:** This alert indicates that the Windows SharePoint Services server manifests could not be found or that they were invalid on at least one front-end Web server. Until this problem is resolved, users cannot download rights-managed documents from or upload rights-managed documents to a document library.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 5046, 5126, 5141, 5140, 5137, 5142  **Event Source:** Windows SharePoint Services 3 |
| Locale ID has changed | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Locale\_ID\_has\_changed  **Description:** This error occurs when an administrator changes the regional setting Locale ID for a site after it was indexed using the previous Locale ID.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 2486  **Event Source:** Windows SharePoint Services 3 Search |
| One or more file types cannot be rights-managed because an IRM protector registered an error | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.One\_or\_more\_file\_types\_cannot\_be\_rights\_managed\_because\_an \_IRM\_protector\_registered\_an\_error  **Description:** This error indicates that one or more Information Rights Management (IRM) protectors are not functioning. Until the problem is resolved, any file type registered with a malfunctioning protector will not be rights-managed when downloaded.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 5032, 5033, 5036  **Event Source:** Windows SharePoint Services 3 |
| Service instance provisioning failed | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.Service\_instance\_provisioning\_failed  **Description:** This error indicates that 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.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 7034  **Event Source:** Windows SharePoint Services 3 |
| SharePoint Administration service is disabled | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.SharePoint\_Administration\_service\_is\_disabled  **Description:** This alert indicates that the Microsoft Windows SharePoint Services timer job that was run requires the Windows SharePoint Services Administration service which is disabled.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 7399  **Event Source:** Windows SharePoint Services 3 |
| The Active Directory organization unit registered in Windows SharePoint Services does not exist | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.The\_Active\_Directory\_organization\_unit\_registered\_in\_Windows \_SharePoint\_Services\_does\_not\_exist  **Description:** 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.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 3360  **Event Source:** Windows SharePoint Services 3 |
| The application pool account has insufficient permissions to add user accounts to Active Directory | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.The\_application\_pool\_account\_has\_insufficient\_permissions\_to\_add \_user\_accounts\_to\_Active\_Directory  **Description:** This alert indicates that the application pool account used by the SharePoint site lacks permissions to add user information to the Active Directory.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 3359  **Event Source:** Windows SharePoint Services 3 |
| The application pool account has insufficient permissions to read user data from Active Directory | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.The\_application\_pool\_account\_has\_insufficient\_permissions\_to\_read \_user\_data\_from\_Active\_Directory  **Description:** This alert indicates that the application pool used by the affected SharePoint site lacks permissions to read user information in Active Directory.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Error  **Event ID:** 6142  **Event Source:** Windows SharePoint Services 3 |
| The Rights Management Services (RMS) client on a computer running Windows SharePoint Services registered an error with its environment | **Rule ID:** Microsoft.Windows.SharePoint.Services.3.0.The\_Rights\_Management\_Services\_\_RMS\_\_client\_on\_a\_computer \_running\_Windows\_SharePoint\_Services\_registered\_an\_error\_with\_its\_environment  **Description:** This alert indicates that an Application Programming Interface (API) call returned a serious error that is preventing Information Rights Management (IRM) from functioning. Uploads to and downloads from IRM-enabled document libraries on all SharePoint sites will typically fail until the problem is resolved.  **Rule Category:** Event Collection  **Rule Target:** Microsoft.Windows.SharePoint.Services.3.0.WSS.Application  **Alert Type:** Warning  **Event ID:** 5050, 5051, 5052, 5053, 5054, 5055, 5057, 5061, 5062, 5125, 5132, 5135, 5132, 5135, 5136, 5138, 5139, 5143, 5134, 5145, 5130, 5129  **Event Source:** Windows SharePoint Services 3 |

# 

# Acknowledgments

The Microsoft Solution Accelerator Team (SAT) would like to acknowledge the team that produced the *SharePoint Manageability Toolkit*. The following people were either directly responsible for, or made a substantial contribution to, the writing, development, and testing of the solution described in this guide.

Program Manager

Luis Camara Manoel (Microsoft Corporation)

**Engineering Lead**

Oleg Glubochansky (Microsoft Corporation)

**Developer**

Vijayarangan Raghavan (Volt Technical Services)

**Test Lead**

Bryan Hughes (Excell Data Corporation)

**Product Manager**

Peter Larsen (Microsoft Corporation)

**UE Lead and Release Manager**

Gaile Simmons (Microsoft Corporation)

**Lead Writer**

Elizabeth Houser (Volt Technical Services)

**Editor**

Susan Fairo (Sakson & Taylor)

**Technical Reviewers**

Edhi Sarwono (Microsoft Corporation)

Joel Oleson (Microsoft Corporation)

Tarang Shah (Microsoft Corporation)

# Feedback

Send suggestions and comments about this document to [omphelp@microsoft.com](mailto:omphelp@microsoft.com). Please include the Management Pack guide name with your feedback.