SolarWinds Orion®

Application Performance Monitor Administrator Guide

APPLICATION PERFORMANCE MONITOR

Application Performance Monitor Administrator Guide 8.9.2009

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	1.866.530.8100 http://www.solarwinds.com
Technical Support	http://www.solarwinds.com/support, you need a customer account to access the Customer Support area of the website.
User Forums	http://www.thwack.com contains the community oriented user forums

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including buttons and fields.
Italics	Book and CD titles, variable names, new terms
`Fixed font`	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [*value*]	Optional command parameters
Curly braces, as in {*value*}	Required command parameters
Logical OR, as in *value1*|*value2*	Exclusive command parameters where only one of the options can be specified

SolarWinds Application Performance Monitor Documentation Library

The following documents are included in the Application Performance Monitor documentation library:

Document	Purpose
Application Performance Monitor Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Page Help	Provides help for every window in the Application Performance Monitor user interface
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com/.

The following documents supplement the Application Performance Monitor documentation library with information about Orion Network Performance Monitor product:

Document	Purpose
Orion Network Performance Monitor Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Page Help	Provides help for every window in the Orion Network Performance Monitor user interface
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com.

Contents

Appendix A

Appendix B

Chapter 1

Introduction

The Orion Application Performance Monitor (Orion APM) module provides much more than up/down status checks and process monitoring. By allowing you to create and monitor your own custom collection of monitored components, Orion APM provides an open field of opportunity to the network engineer. Built on the proven capabilities and solid architecture of Orion NPM, you know your current needs will be met and, as your needs grow, the Orion platform and Orion APM module will scale with you.

What is an Application?

SolarWinds knows that an application is much more than a single process or daemon running on a server. With Orion Application Performance Monitor, you create flexible application monitor templates to combine process monitors, port availability, and performance counters, allowing you to assess the status of every aspect of your application and the health of the application as a whole.

Templates provide blueprints you can quickly roll out to numerous application servers, customizing only the one or two component monitors that need to change for a specific environment. Application Performance Monitor recognizes and answers the complexity of today's business applications with scalability, flexibility, and reliability.

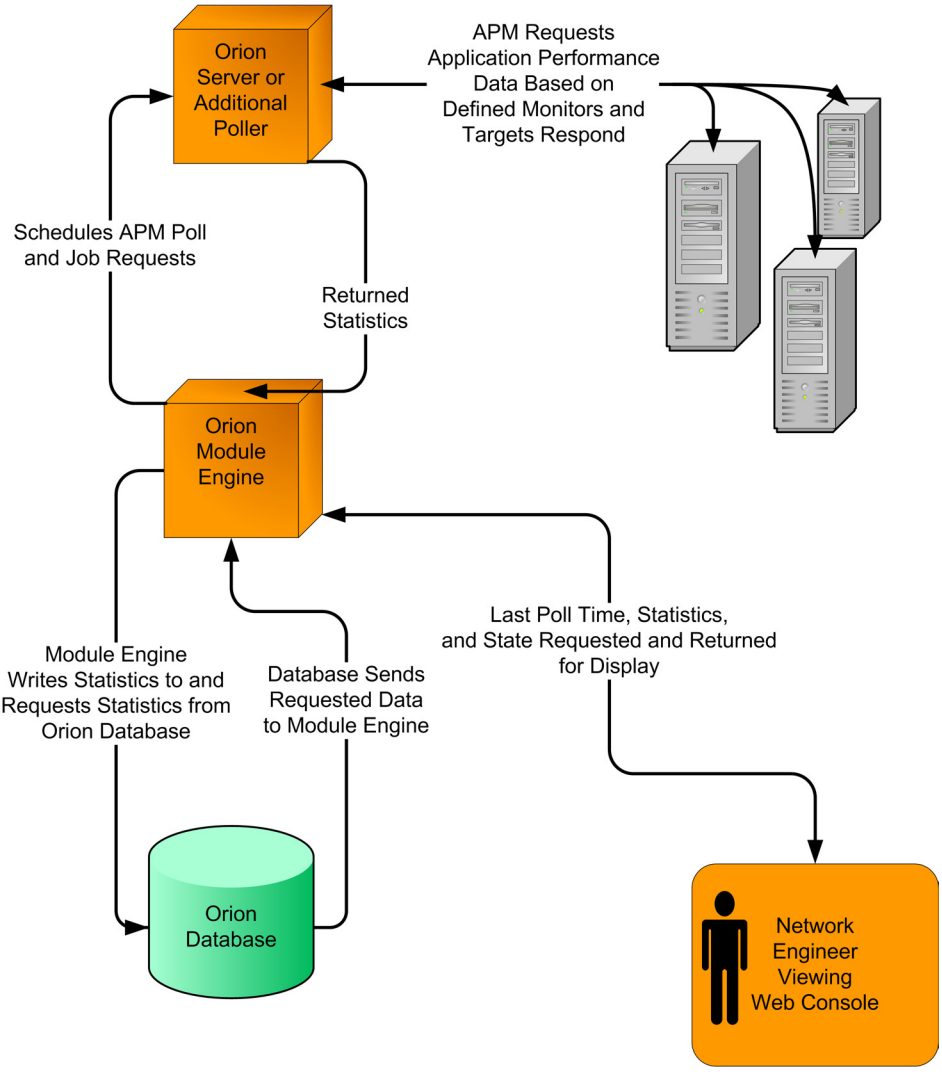
What Application Performance Monitor Offers

Orion APM provides focused application monitoring for network engineers. With Orion APM, you can focus monitoring on your core services while easily ensuring application outages do not originate in the network. Orion APM provides many features to help, including:

- Network service monitoring
- General TCP port monitoring
- WMI and SNMP process monitoring
- Service monitoring
- User experience monitoring using HTTP or HTTPS content checking

How Does Application Performance Monitor Work?

Application Performance Monitor joins the proven performance and solidity of Orion NPM and extends Orion NPM functionality into the realm of application performance monitoring. Using UDP, TCP, SNMP, and WMI calls to your network framework and application servers, Application Performance Monitor provides realtime feedback on your applications and trending through statistics stored in the Orion NPM database. Keeping with the Orion core infrastructure, there are no agents installed on your servers and no remote software to maintain. All calls are made in realtime and displayed on a Web Console accessible from any supported browser.



Chapter 2

Installing Orion Application Performance Monitor

Installing the Orion Application Performance Monitor (Orion APM) module for Orion NPM is a simple, wizard-driven process. Resource and space requirements are nominal, and most deployments do not require hardware updates to your Orion NPM server.

Requirements

You must have Orion NPM version 9.5 Service Pack 3 or later installed before installing Application Performance Monitor.

Enterprise-level Orion APM deployments with the potential for more than 1000 monitors may need additional computing resources above the standards required for Orion NPM.

Component Monitors	Additional Requirements
Up to 1000	No additional requirements
More than 1000	Up to 5GB of additional RAM (total 8 GB)

For more information about system requirements for Orion NPM, see "Requirements" in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

Installing or Upgrading Application Performance Monitor

Application Performance Monitor offers an intuitive wizard to guide you through installing and configuring the product. You must have Orion NPM version 9.5 Service Pack 3 or later installed before installing Application Performance Monitor.

Note: If you have any additional Orion APM web consoles or pollers, you must upgrade them too.

To install or upgrade Application Performance Monitor:

1. Log on to your Orion NPM server with a local administrator account.
2. ***If you downloaded the product from the SolarWinds website,*** navigate to your download location and launch the executable.

3. ***If you received physical media,*** navigate the autorun and launch the setup program. If the autorun does not automatically start, run the `autorun.exe` in the root of the DVD.
4. Read the welcome message, and then click **Next**.
5. Select **I accept the terms of the license agreement**, and then click **Next**.
6. Click **Install**.
7. Click **Finish** when the setup completes.

Activating Your License

After installing the software through the setup wizard, you are prompted to enter the license activation key for your product. If you do not have an activation key, the product runs in a time-limited evaluation mode.

To evaluate the software without a license:

Click **Continue Evaluation**.

To license the software on a server with Internet access:

1. Click **Enter Licensing Information**.
2. Select **I have internet access and an activation key**.
3. Click the http://www.solarwinds.com/customerportal link to access the customer portal on the SolarWinds web site.
4. Log on to the portal using your SolarWinds customer ID and password.
5. Click **License Management** on the left navigation bar.
6. Navigate to your product, choose an activation key from the **Unregistered Licenses** section, and then copy the activation key.
7. ***If you cannot find an activation key in the Unregistered Licenses section,*** contact SolarWinds customer support.
8. Return to the Activate APM window, and then enter the activation key in the **Activation Key** field.
9. ***If you access Internet web sites through a proxy server,*** click **I access the internet through a proxy server**, and enter the proxy address and port.
10. Click **Next**.
11. Enter your email address and other registration information, and then click **Next**.

To license the software on a server without Internet access:

1. Click **Enter Licensing Information**
2. Select **This server does not have internet access**, and then click **Next**.
3. Click **Copy Unique Machine ID**.
4. Paste the copied data into a text editor document.
5. Transfer the document to a computer with Internet access.
6. On the computer with Internet access, complete the following steps:
7. Browse to http://www.solarwinds.com/customerportal/licensemanagement.aspx and then log on to the portal with your SolarWinds customer ID and password.
8. Navigate to your product, and then click **Manually Register License**.
9. If the **Manually Register License** option is not available for your product, contact SolarWinds customer support.
10. Provide the Machine ID from Step 5, and then download your license key file.
11. Transfer the license key file to the server.
12. Return to the Activate APM window, browse to the license key file, and then click **Next**.

Finishing Installing Orion APM

After activating your license, you are prompted to configure Orion APM. Doing so configures the Orion APM database, website, and services to work in your specific Orion NPM environment.

1. Click **Next** on the Orion Configuration Wizard Welcome window.
2. Check the appropriate Application Performance Monitor services or plugins, and then click **Next**. If you have installed other modules, the `APM Job Engine Plugin` may be your only selectable option.
3. Review the configuration summary provided by the Configuration wizard, and then click **Next**.
4. Click **Finish** when the Configuration wizard completes.

Upgrading from Orion APM v1.0

If you are upgrading from Orion APM v1.0, your existing component-specific alerts lose their component type. For example, a status alert for an HTTP monitor becomes a generic status alert that could be triggered by any component. This is a side-effect of the improvements we made to the alerts to make them less cumbersome to configure.

To make a converted component monitor alert work the same way it did in APM v1.0, edit the alert in Advanced Alert Manager, and add a **Component Type is equal to x** condition to the alert, where **x** is the component monitor type value. For a list of component monitor type values, see "Component Monitor Alerting Properties" on page 38.

Upgrading from Orion Application Monitor

Contract SolarWinds support for assistance upgrading Orion Application Monitor (Orion AM) to Orion APM v3.0.

Licensing

The Orion APM license you purchase is based on the number of allowed assigned component monitors. You can have as many application templates and assigned application monitors as you need, as long as the number of assigned component monitors does not exceed the license count.

Orion APM licenses do not have to mirror your Orion NPM license. For example, you can install Orion APM with a 50 component license on an Orion NPM server with an unlimited node license.

Chapter 3

Configuring Orion APM

You can configure Orion APM and its templates and component monitors through the Application Performance Monitor portion of the Orion NPM Web Console.

To configure Application Performance Monitor:

1. Log on to your Orion NPM Web Console with an Administrator account.

   Note: Initially, `Admin` is the default administrator user ID with a blank password.
2. Click **Admin** in the Views bar.
3. Click **APM Settings**.
4. Review the available options on the APM Settings page. You can configure the following options from this landing page:

   Add New Application Monitors with Application Discovery

   Allows you to scan nodes and automatically add application monitors.

   Add New Application Monitors

   Allows you to assign application monitors to server nodes.

   Manage Assigned Application Monitors

   Allows you to view, edit, and delete assigned application monitors and their component monitors.

   Manage Application Monitor Templates

   Allows you to create, import, export, assign, copy and delete application templates and their component monitors.

   Import Application Monitor Templates from thwack

   Allows you to browse and use application templates contributed by fellow administrators.

   Find Processes, Services, and Performance Counters

   Allows you to scan a node and pick the processes, services, and performance counters you want from a list.

Credentials Library

Allows you to create, edit, and delete the credential sets component monitors use to access protected system resources.

Data & Database Settings

Allows you to set the polling engine mode and the data compression and grooming interval.

License Summary

Allows you to see a comparison between the number of active component monitors and the limit allowed by your Orion APM license.

For more information about an option, click **Help**.

Compressing and Grooming the Database

The amount of data collected from your network and the size of that data in the database is dependent on the number of applications and the number of component monitors per application you define.

Due to the volume of data collected, detailed statistics are stored in hourly averages after a specified time period (7 days, by default) and hourly statistics are again compressed into daily statistics after a number of days (30 days, by default). Detailed statistics are based on the individual polling intervals for each component monitor.

Grooming the database sets a length of time after which Orion APM purges data from the database.

Note: Before modifying your database compression and grooming setting, consider noting your database size, collecting application data for a week, and then rechecking your database size. Projecting the amount of data collected over the amount of time you want to save data. This will help you forecast and plan for an appropriate data compression and retention period.

To set statistics compression and database grooming intervals:

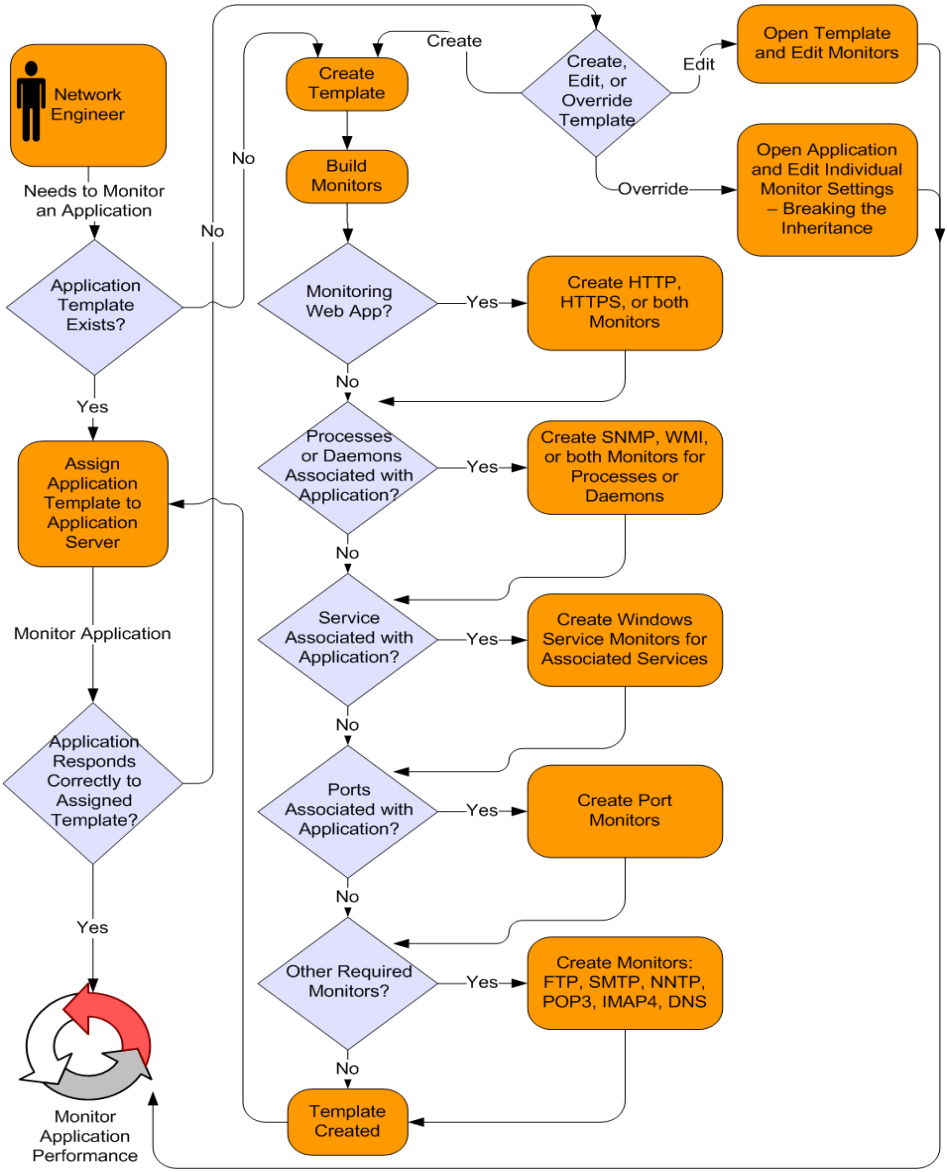
1. Log on to your Orion NPM Web Console with an Administrator account.

   Note: Initially, `Admin` is the default administrator user ID with a blank password.
2. Click **Admin** in the Views bar.
3. Click **APM Settings**.
4. Click **Data & Database Settings**.
5. Specify the appropriate values for the Orion APM data retention settings.

Chapter 4

Building Component Monitors and Templates

The following diagram illustrates the work flow involved in creating an application to be monitored by Application Performance Monitor.



Understanding Component Monitors and Application Monitor Templates

The following terms are used throughout this guide to describe the Orion APM concepts that allow you to monitor your applications.

Component Monitors

Component monitors are the building blocks of Orion APM. They monitor the status and performance of different aspects of an application. There are several different types of component monitors, each containing settings that define how and what is monitored.

Some types of component monitors allow you to set threshold conditions on the monitored parameters. You can set separate thresholds to indicate warning and critical conditions. For example, if you are monitoring the percentage of free space remaining on a volume, you can set a warning threshold at 15%, and a critical condition at 5%.

Application Monitor Templates

A template is a group of component monitors modeling the total availability and performance level of an application. A complicated application such as Microsoft Exchange Server may require dozens of component monitors to accurately assess its current status and performance.

A template is only a blueprint and does not perform any monitoring on its own. Only after assigning the template to a server node are active assigned component monitors created.

Assigned Component Monitors

Assigned component monitors are created by assigning application monitor templates to server nodes. Each actively monitors its assigned node according to its settings. Component monitors inherit these initial settings from the template. If you make a change to a template, that same change is rolled out to all assigned application monitors based on the template.

You can override the template settings at any time, breaking the inheritance relationship between the component monitor and its template. For example, the user name and password usually differ for each node, and you would select a different credential for each assigned application monitor, thus overriding the template setting for the Credentials field.

To restore the inheritance relationship between a component monitor and its template, click **Inherit From Template** next to the setting.

Assigned Application Monitors

An assigned application monitor runs its assigned component monitors at regular intervals, and then uses the status results from the component monitors to determine an overall status for the application.

If some of the component monitors are up and others are down, the application monitor follows the Status Rollup Mode setting in the Orion Web Console Settings to show either the worst status of the group or a warning status.

Monitoring External Nodes

Only nodes that are in the Orion database can have Orion APM templates assigned to them. If you want to monitor services and applications on a node that you do not directly manage, you should add that node to the Orion database as an external node. For more information, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Orion Network Performance Monitor Administrator Guide.

Note: Orion NPM does not collect or monitor any network performance data from external nodes.

Understanding the Credential Library

You typically need to associate credentials with component monitors to enable them to retrieve application data. For example, to use a WMI monitor, you must provide valid domain or computer credentials. Or, if your web server requires credentials, you must provide the appropriate credentials to access the protected sections of your site.

You can add credentials to the Credential Library page for use later, or you can create credentials on the spot (Quick Credentials) when editing templates and component monitors.

Notes:

- Application Performance Monitor uses the same SNMP credentials as Orion NPM. There is no need to specify additional credentials for SNMP operations.
- Orion APM stores credentials in the database encrypted.

To add credentials from the Credential Library page:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.

4. Click **Credentials Library**.
5. Click **Add New Credential**.
6. Provide a friendly name for the credential set. Application Performance Monitor displays this name in the **Credential for Monitoring** field of monitors that accept credentials.
7. Provide the user name and password, and then confirm the password and click **Submit**. If you are providing windows credentials for accessing and harvesting information through WMI, ensure you provide the account name in the following syntax: *`domainOrComputerName\userName`* for domain level authentication or *`userName`* for workgroup level authentication.

You can assign credentials to all the associated components of a template or application monitor.

To create and assign credentials using Quick Credentials when editing a template or application monitor:

1. ***If the credential you want to assign does not exist,*** create it by following these instructions:
   a. Select **<New Credential>** in the **Choose Credential** field.
   b. Type a name for the new credential in the **Credential Name** field.
   c. Type the user name for the credential in the **User Name** field.
   d. Type the password in the **Password** field, and type it again in the **Confirm Password** field.
2. ***If you want to assign an existing credential,*** select the credential from the **Choose Credential** field.
3. Click **Set Component Credentials** to set this credential as the credential for all the components in the application monitor or template

Using Application Monitor Templates

This section discusses the many operations you can perform in Orion APM regarding the use and management of application monitor templates. The topics include:

- Discovering Applications Automatically
- Manually Assigning Templates to Nodes
- Creating New Templates
- Copying Templates
- Exporting and Importing Templates
- Deleting Templates
- Managing Component Monitors Within Templates
- Tagging Templates

Discovering Applications Automatically

Orion APM can scan nodes for you and automatically assign the application monitors it deems suitable for each scanned node. You control the nodes to be scanned, the application templates used in the scan, and the scanning parameters that determine a match.

To use the application discovery:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **Start Scanning Nodes**.
4. Follow the instructions in the Select Nodes wizard.
5. Follow the instructions in the Select Applications wizard.
6. Follow the instructions in the Enter Credentials wizard.
7. Follow the instructions in the Review & Start Scan wizard.
8. Follow the instructions in the Add User Experience Monitors wizard.

Select Nodes

Click [+] in the list to expand the node groups and to select the nodes you want to scan.

Select Applications

To keep the time it takes to scan to a minimum, we recommend you initially scan for only a limited number of application templates. To see more application templates, select a different template group from the **Show Only** list.

To adjust the template assignment criteria, expand **Advanced Scan Settings** and move the slider to the desired setting:

Exact Match

All the components must match to assign the template.

Strong Match

Most of the components must match to assign the template.

Partial Match

Some of the components must match to assign the template.

Minimal Match

At least one component must match to assign the template.

Enter Credentials

Some application templates require credentials either to access restricted resources, or to run within the context of a specific user. To scan for these templates, add the necessary credentials to the list. If a template you are scanning for requires credentials, the credentials in this list are tried in the order in which they appear.

Warning!: Credentials are tried several times over the course of a scan, so an incorrect password is likely to lock out an account. To avoid potential account lockouts that affect actual users, we recommend you create and use service accounts.

If you have domains sharing user names with different passwords, we recommend you run separate application discoveries for each domain.

Review & Start Scan

The scan runs in the background. Scanning progress is displayed at the top of the Orion APM menu bar. You are notified after scanning is completed.

If the automatic discovery matches templates that are already assigned to the node, the template is not assigned a second time. If you want to assign duplicate templates, select **Yes, Assign Anyway** from the **Do you want to assign duplicates** list.

Add User Experience Monitors

You cannot scan for user experience monitors, but you can assign them to nodes manually. Adding monitors from this page does not affect your scan.

Manually Assigning Templates to Nodes

The quickest way to assign application monitors to nodes is through the **Add New Application Monitors** wizard, but you can also assign them through the **Manage Application Monitor Templates** page.

To assign a template using the wizard:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Start Assigning Application Monitors**.
5. Select the application monitor template you want to apply, and then click **Next**.
6. Select the server node or nodes to which you want to apply the application monitor template, and then click **Next**.
7. ***If suitable credentials already exist,*** choose the credential from the **Choose Credential** list.
8. ***If suitable credentials do not exist,*** choose **<New Credential>** from the **Choose Credential** list, and then add the new credential by filling out the credential details.
9. Click **Test** to test the credentials and component monitors against the test node..
10. ***If the test fails,*** troubleshoot the problem based on the error messages, and then retest the node.
11. ***If the test passes,*** click **Assign Application Monitors.**

To assign a template through the Manage Application Monitor Templates page:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Check the checkbox next to the template you want to assign.
6. Click **Assign to Node**.

7. Select the server node or nodes to which you want to apply the application monitor template, and then click **Next**.
8. ***If suitable*** credentials ***already exist,*** choose the credential from the **Choose Credential** list.
9. ***If suitable credentials do not exist,*** choose **<New Credential>** from the **Choose Credential** list, and then add the new credential by filling out the credential details.
10. Click **Test** to test the credentials and component monitors against the test node..
11. ***If the test fails,*** troubleshoot the problem based on the error messages, and then retest the node.
12. ***If the test passes,*** click **Assign Application Monitors.**

Creating New Templates

Orion APM allows you to create new templates by bundling component monitors together. There are two ways of creating a template from scratch. The traditional method allows you to create any kind of template. The browsing method only creates templates monitoring services, processes, and performance counters.

To create a new template using the traditional method:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Click **Create New Template**.
6. Type a name for your template in the **Template Name** field.
7. Specify the values for the **Polling Frequency** and **Polling Timeout** fields.

   Note: Setting a polling frequency below 30 seconds can result in erratic monitor behavior.
8. Click **Add a component**.
9. Expand the component groups and check all the component monitors you want to add.
10. Click **Submit**.
11. Configure the component monitor settings, and then click **Submit**.

To create a new template using the browsing method:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Find Processes, Services, and Performance Counters**.
5. Select the component monitor type that you want to browse, then click **Next**.
6. Type the IP address of the node you want to browse, or click **Browse** and select the node from the list.
7. ***If suitable credentials already exist,*** choose the credential from the **Choose Credential** list.
8. ***If suitable credentials do not exist,*** choose **<New Credential>** from the **Choose Credential** list, and then add the new credential by filling out the credential details.
9. Click **Next**.
10. ***If you selected a performance counter monitor type,*** select a performance object from **Performance Object** to populate the list.
11. Check the checkboxes next to one or more found items to add as a component monitor.
12. Click **Next**.
13. Configure the component monitor settings, and then click **Next**.
14. Select **New Application Monitor Template**.
15. Type a name for your template in the **Application Monitor Template Name** field.
16. Click **Next**.
17. ***If you want to assign the template to nodes,*** select the nodes.
18. ***If you only want to create the template,*** do not select any nodes.
19. Click **Next**, and then click **Ok, Create**.

Copying Templates

After successfully creating a complicated template, instead of having to recreate it over for a similar application, consider copying the template. This will allow you to only modify those properties that differ.

To copy an application template:

1. Log on to your Orion NPM Web Console with an Administrator account.

2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Check the application template you want to copy, and then click **Copy**.

Exporting and Importing Templates

You can export and import templates to and from your file system for your own use, or to the SolarWinds community site (thwack.com) where templates can be shared with the network engineering community.

Note: thwack.com import and export operations require Internet connectivity to thwack.com and thwack.api.solarwinds.com. In addition, thwack export operations require a valid thwack.com user account.

To export a template:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. ***If you want to export a template to a file,*** complete the following procedure:
    a. Check the application template you want to export, and then click **Export as File**.
    b. Confirm that you want to save the file by clicking **Save**.
    c. If you are prompted for a path, specify or browse to one and then click **Save**.
6. ***If you want to export a template to thwack.com***, complete the following procedure:
    a. Check the application template you want to share, and then click **Export to thwack**.
    b. Type your thwack.com user name and password, and then click **Log In**.

To import a template from a file:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.

5. Click **Import**.
6. Click **Choose File**, select the template file, and then click **Submit**.

To import a template from thwack:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Import Application Monitor Templates from thwack**.
5. Select the templates you want to import, and then click **Import to Orion APM**.

Deleting Templates

If you no longer need a template, you can delete it. Deleting a template also deletes all the data associated with it, so ensure you no longer need either the template or the associated data before deleting the template.

Notes:

- Deleting a template also deletes all of its assigned applications, both modified and unmodified.
- To speed user interface interaction, data is not immediately removed from the database, but systematically groomed every few minutes in the background.

To delete a template:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Check the template you want to delete, and then click **Delete**.
6. Confirm that you want to delete the template by clicking **OK**.

Managing Component Monitors Within Templates

You can manipulate and manage the component monitors that are inside the application monitor templates in several ways.

Listing the Component Monitors Defined in a Template

To quickly see the different component monitors within your templates:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Click **Manage Component Monitors within Templates**.
6. Select **Template** in the **Group By** list.

Creating a New Template from Existing Component Monitors

To create a new template that contains copies of existing component monitors:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Click **Manage Component Monitors within Templates**.
6. Check the checkbox next to the component monitors you want in the new template.
7. Click **Create New Template**, and then click **Submit**.

Creating Assigned Application Monitors from Existing Component Monitors

To create assigned application monitors from existing component monitors:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Click **Manage Component Monitors within Templates**.
6. Check the checkbox next to the component monitors you want in the assigned application monitors.
7. Click **Assign to Node**.
8. Select the nodes for which you want to create the assigned application monitors.
9. ***If suitable credentials already exist,*** choose the credential from the **Choose Credential** list.

10. ***If suitable credentials do not exist,*** choose **<New Credential>** from the **Choose Credential** list, and then add the new credential by filling out the credential details.
11. Click **Test** to test the credentials and component monitors against the test node..
12. ***If the test fails,*** troubleshoot the problem based on the error messages, and then retest the node.
13. ***If the test passes,*** click **Assign Application Monitors.**

Copying a Component Monitor

To copy a component monitor to a template or an assigned application monitor:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Click **Manage Component Monitors within Templates**.
6. Check the checkbox next to the component monitors you want to copy.
7. Click **Copy To**.
8. ***If you want to copy to an assigned application monitor,*** click **Copy to Assigned Application Monitor**.
9. ***If you want to copy to a template,*** click **Copy to Application Monitor Template**.
10. Check the checkboxes next to the template or assigned application monitors to which you wish to copy the component monitors, and then click **Done**.

Tagging Templates

Tags are descriptive labels that help you classify and sort your application templates on the Manage Application Monitor Templates page. The application templates included in Orion APM have already been tagged with several descriptive labels that you can modify as you see fit.

To add tags:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.

5. Select the templates you want to tag.
6. Click **Tags**.
7. ***If you want to add existing tags,*** follow these instructions:
    a. Click **Add existing tag(s)**.
    b. Select the tags from the list.
8. ***If you want to add new tags,*** follow these instructions:
    a. Click **Add new tag(s)**.
    b. Type the tags in the **Add new tag(s)** field, separating multiple tag entries with commas.
9. Click **Submit**.

To remove tags:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Select the templates you want to tag.
6. Click **Tags**.
7. Click **Remove tag(s).**
8. Select the tags from the list.
9. Click **Submit**.

Editing an Assigned Application Monitor

You can override the template inheritance relationship by editing the components of an assigned application monitor.. Any modifications you make to an application's components or component properties are independent from the template, including: adding new components, removing existing components

New components that you add to the application are not governed by the original template used to create the application. Modified component properties override the original template settings.

To edit an individual application:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.

4. Click **Manage Assigned Application Monitors**.
5. Click the group containing the application you want to edit.
6. Check the application you want to edit, and then click **Edit Properties**.
7. Expand the component you want to modify, and then click **Override Template** and specify new values.
8. If you want to add components unique to this specific application, click **Add a component**.
9. Click **Submit** to apply your changes.

Scripting Custom Component Monitors

The following sections provide information and guidance to help you create some of the more complicated types of component monitors.

- "Creating a Linux/Unix Script Monitor" on page 23
- "Creating a Windows Script Monitor" on page 26

For general information about the settings for each component monitor, click the **More Information** help link in the Orion APM component monitor description.

Creating a Linux/Unix Script Monitor

Linux/Unix Script component monitors allow you to execute a command line script that can return statistical data. When collecting information for this monitor, Application Performance Monitor runs the script with the credentials you define with the Credential Library.

To adapt an existing Perl script to a Linux/Unix Script component monitor in a new template:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Click **Create New Template**.
6. Type a name for your template, and then click **Add a component**.
7. Expand the **Custom Component Monitors** group, and then check **Linux/Unix Script Monitor**.
8. Click **Add Component Monitor**.
9. Select credentials with SSH permissions in the **Credentials for Monitoring** field.

10. Copy the script into the **Script Body** field
11. Type the Linux command that runs the script in the **Command Line** field. It should be similar to the following: `perl ${SCRIPT}`
12. Type a valid working directory in the **Script Working Directory** field.
13. Specify the critical and warning thresholds.
14. Click **Submit**.

Linux/Unix Scripts

Linux/Unix scripts are uploaded by SSH and then run on the remote server using the string from the **Command Line** field.

You can use the following variable in the command line field:

${SCRIPT}

Replaced with the script body.

You can use the following variables in the script body field:

${IP}

Replaced with the target node's IP address.

${USER}

Replaced with the user name from the credential.

${PASSWORD}

Replaced with the password from the credential.

Linux/UnixScripts Report Status Through Exit Codes

Scripts must report their status by exiting with the appropriate exit code:

Exit Code	Meaning
0	Up
1	Down
2	Warning
3	Critical
Any other value	Unknown

Linux/UnixScripts Must Have Text Output

Scripts report additional details by sending text to the script's standard output. Each line of output can contain a single detail in the following format:
`DetailType:Value`

Detail Type	Required	Meaning
Message	No	An error or information message to be displayed in the monitor status details.
Statistic	Yes	A numeric value used to determine how the monitor compares to its set thresholds.

Example output:

```
# Script output comment

Message: The directory contains too many files.

Statistic: 5
```

Example Scripts

There are several sample scripts are installed with Orion APM you can use to create Linux/Unix script component monitors. These sample scripts are installed on your Orion APM server, in the folder:
`C:\Program Files\Solarwinds\Orion\APM\SampleScriptMonitors`

ScriptProcessorForNagios(tm).pl

Processes Nagios scripts.

1. Download the Nagios script you want to use to the server you want to monitor. Save the file in an appropriate path such as `/usr/local/bin/nagiosScriptName`.
2. Change the file system mode (`chmod`) to make the script executable.
3. Test the Nagios script to make sure it works, specifying any necessary command line parameters.
4. Add a Linux Script component monitor to an existing application monitor template.
5. Paste the contents of the `ScriptProcessorForNagios(tm).pl` file into the **Script Body** field.
6. Type `${Script} /usr/local/bin/nagiosScriptName` in the **Command Line** field, followed by any necessary command line parameters.

   For example: `${Script} /usr/local/bin/check_mysql_stats -H localhost -U MyUser -P MyPassword -w 80 -c 75 –t`

Creating a Windows Script Monitor

Windows Script component monitors allow you to execute a Visual Basic script on the Orion APM server that can return statistical data. When collecting information for this monitor, Application Performance Monitor runs the script with the credentials you define with the Credential Library.

To adapt an existing Visual Basic script to a Windows Script component monitor in a new template:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Click **Create New Template**.
6. Type a name for your template, and then click **Add a component**.
7. Expand the **Custom Component Monitors** group, and then check **Windows Script Monitor**.
8. Click **Add Component Monitor**.
9. Select credentials with appropriate permissions to run the script on the Orion APM server, and that also has appropriate permissions to do whatever else the script requires.
10. Copy the Visual Basic script into the **Script Body** field
11. Type any script arguments into the **Script Arguments** field.
12. Specify the critical and warning thresholds.
13. Click **Submit**.

Windows Scripts

You can specify script arguments in the Script Arguments field. You can use the following tokens as script arguments:

${IP}

Replaced with the target node's IP Address.

${USER}

Replaced with the user name from the credential set

${PASSWORD}

Replaced with the password from the credential set.

Visual Basic Scripts Report Status Through Exit Codes

Scripts must report their status by exiting with the appropriate exit code:

Exit Code	Meaning
0	Up
1	Down
2	Warning
3	Critical
Any other value	Unknown

For example, if you want to inform Orion APM that a script reports Up status, you would exit the script using code similar to the following:

```
Wscript.quit(0)
```

Visual Basic Scripts Must Have Text Output

Scripts report additional details by sending text to the script's standard output. Each line of output can contain a single detail in the following format:
`DetailType:Value`

Detail Type	Required	Meaning
Message	No	An error or information message to be displayed in the monitor status details.
Statistic	Yes	A numeric value used to determine how the monitor compares to its set thresholds.

Example output:

```
# Script output comment

Message: The directory contains too many files.

Statistic: 5
```

Example Scripts

There are several examples of Windows Script component monitors included in templates. These include: File Count, File Modified, LDAP Connection Monitor, Run 3rd Party Application, and Windows Event Log Count.

Custom Application Monitor Template Example: Creating an Orion NPM Template

The following procedure creates an Orion NPM application monitor template that monitors a locally installed SQL Server instance. The template is simplified by using the Windows Service component monitors, a TCP port monitor for your SQL Server, and an HTTP monitor for the local Web Console. You do not need to know the specific names of the processes, and you are not limited to a single process per application. With Application Performance Monitor you can group multiple component monitors into a single application and monitor these groupings as one mission critical application.

While completing this procedure, you will create an application template with the following component monitors:

- TCP port component monitor to monitor port 1433, the port through which Orion NPM communicates with the SQL Server.
- Service component monitors for the following windows services:
  - SolarWinds Alerting Engine
  - SolarWinds Custom MIB Poller
  - SolarWinds Network Performance Monitor
  - SolarWinds Orion Job Engine
  - SolarWinds Orion Job Scheduler
  - SolarWinds Orion Module Engine
  - SolarWinds Syslog Service
  - SolarWinds Trap Service
- HTTP component monitor to monitor port 80, the port through which you access the Orion NPM Web Console.

To create an Orion NPM application template:

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Application Performance Monitor** in the Modules toolbar.
3. Click **APM Settings**.
4. Click **Manage Application Monitor Templates**.
5. Click **Create New Template**.
6. Type a name for your application template, and then click **Add a component**. For example, type `Orion NPM`.

7. Expand the Network Service Protocol Component Monitors list, and then check **TCP Port Monitor**.
8. Click **Add Component**.
9. Click **Rename**, type a name for the TCP port monitor, and then click **OK**. For example, type `Orion NPM SQL Server Port`.
10. Ensure the **Port Number** field corresponds to the port used to communicate with the Orion NPM SQL Server instance. By default, this is port `1433`.
11. Click **Save**.
12. Click **Add a component**.
13. Expand the Process and Service Component Monitors, and then check **Windows Service Monitor** and click **Add Component**.
14. Click **Rename**, type a name for the SolarWinds Alerting Engine monitor, and then click **OK**. For example, type `SW Alerting Engine`.
15. Select the credential set you want to use when accessing the Windows service information. For more information about creating a credential set, see “Understanding the Credential Library” on page 11.
16. Type the name of the service in the **Service Name** field.

    Note: This name must exactly match the name of the service as displayed in the Windows Service Control Manager (`services.msc`). For the SolarWinds Alerting Engine, this is typically `SolarWindsAlertingEngine`.
17. Click **Save**.
18. Repeat **Steps 14 through 21** for each of the Orion NPM Windows services:
    - SolarWinds Custom MIB Poller
    - SolarWinds Network Performance Monitor
    - SolarWinds Orion Job Engine
    - SolarWinds Orion Job Scheduler
    - SolarWinds Orion Module Engine
    - SolarWinds Syslog Service
    - SolarWinds Trap Service
19. Expand the Network Service / Port Monitors list, and then check **HTTP Monitor**.
20. Click **Add Component**.
21. Click **Rename**, type a name for the HTTP port monitor, and then click **OK**. For example, type `Orion NPM Web Console`.

22. Ensure the **Port Number** field corresponds to the port you use for the Orion NPM Web Console port, and then click **Save**.
23. Click **Submit**.

Unmanaging Applications

If you need to deactivate an assigned application monitor for a period of time, you can do so by unmanaging them. Changes you make to the managed or unmanaged status of an application take affect after the next polling cycle.

To unmanage an application:

1. Click **APM Settings > Manage Assigned Application Monitors**.
2. Select the monitor and then click **Unmanage**.
3. Set the duration of the unmanaged state, and then click **OK**.

-or-

1. Click an assigned application monitor in any resource to view its APM Application Details page.
2. Click **Unmanage** in the Application Details section.
3. Set the duration of the unmanaged state, and then click **OK**.

Note: Unmanaging a node in Orion NPM automatically unmanages its assigned Orion APM applications for the same duration.

To remanage an application:

1. Click **APM Settings > Manage Assigned Application Monitors**.
2. Select the monitor and then click **Remanage**.

-or-

1. Click an assigned application monitor in any resource to view its APM Application Details page.
2. Click **Remanage** in the Application Details section.

Chapter 5

Monitoring Your Applications

After creating your application templates and modifying any individual components as needed, you are ready to start monitoring application performance. The following sections provide a short list and overview of the views and resources provided with Application Performance Monitor. When you install Application Performance Monitor, the setup program adds these views and resources to the SolarWinds Orion Web Console.

Enabling Orion APM-Specific Node Resources

To avoid interfering with your currently configured Node Details pages, enabling Application Performance Monitor resources in the node details pages is optional.

To enable Orion APM-specific resources:

Click **Yes** when APM ask on first log on whether you want to include APM resources on the Node Details page.

- or -

1. Log on to your Orion NPM Web Console with an Administrator account.
2. Click **Admin** in the Views toolbar, and then click **Manage Views**.
3. Select **Node Details** on the Manage Views page, and then click **Edit**.
4. Click **+** next to the column in which you want to display APM resources.
5. Click **+** to expand the Node Details Reports category, and then check the APM resources you want to add, for example:
   - All Applications Tree
   - Top XX Components by Response Time
   - Top XX Processes by CPU Load
6. Click **Submit**.
7. Click **Done** on the Customize Node Details page.
8. Navigate to a node with which you have associated an application and review the new resources.

Upon completing the previous procedure, the following resources are available.

Active Application Alerts

Provides a list of the active application alerts.

All Applications Tree

Provides an expandable list of applications that allows custom grouping.

Top XX Components by Response Time

Provides a list of the monitors with the slowest response time on the selected node.

Top XX Processes by CPU Load

Provides a list of the monitors consuming the most CPU on the selected node.

Top XX Processes by Physical Memory

Provides a list of the monitors consuming the most physical memory on the selected node.

Top XX Processes by Virtual Memory

Provides a list of the monitors consuming the most virtual memory on the selected node.

For more information about a resource, click **Help** in the resource.

Exploring the APM Application Summary view

The APM Application Summary view provides the following resources. You can customize which of these resources appear on the page by clicking **Customize Page**.

Down Applications

Provides a list of applications with the status of down, including a list of how many of the monitors in each application are down and how long each application has been down.

All Applications Tree

Provides an expandable list of applications that allows custom grouping.

Active Application Alerts

Provides a list of the active alerts associated with applications.

Application Health Overview

Provides an overview of the status of all assigned application monitors.

Last 25 Application Events

Provides a list of the last twenty-five events associated with applications. For more information about creating alerts for these events, see “Creating Alerts for Applications” on page 36.

Thwack Community Latest Application Monitor Templates

Provides a list of the newest application monitor templates that have been added to the Thwack community web site. Click a template to open its download web page.

Active Application Alerts

Provides a list of the active application alerts.

Top XX Components by Response Time

Provides a list of the monitors with the slowest response time on the selected node.

Top XX Processes by CPU Load

Provides a list of the monitors consuming the most CPU on the selected node.

Top XX Processes by Physical Memory

Provides a list of the monitors consuming the most physical memory on the selected node.

Top XX Processes by Virtual Memory

Provides a list of the monitors consuming the most virtual memory on the selected node.

For more information about a resource, click **Help** in the resource.

Exploring the APM Application Details

The APM Application Details view provides the following resources. You can customize which of these resources appear on the page by clicking **Customize Page**.

Note: You can also add Orion NPM node resources to the application details view. For example, you can add the CPU Load & Memory Utilization charts or Packet Loss gauges. For more information about adding resources to views, see the *Orion NPM Administrator Guide*.

Application Details

Provides a list of application properties, including the application name, application status, application server status, component names, component types, and component status.

Last XX Application Events

Provides a customizable list of the most current *XX* events specific to the application.

Active Application Alerts

Provides a list of the active alerts specific to the application.

Components

Provides a list of the components included in the application and their response times.

Processes and Services

Provides a list of the process and service monitors included in the application and the response time for the application you are viewing.

Application Availability

Provides a bar chart of the application availability percentage. To modify the chart, click the title of the chart. Ensure you adjust your polling to less than the interval you want displayed in charts. Not adjusting your polling will result in gaps in your charts. For more information about adjusting your polling, see “Scripting Custom Component Monitors” on page 23.

For more information about a resource, click **Help** in the resource.

Exploring Orion APM Component Details

The Component Details view provides the following resources. You can customize which of these resources appear on the page by clicking **Customize Page**.

Component Statistics

Provides a number of gauges that pertain to the selected component. Response time is provided for port components. CPU load, physical memory, and virtual memory gauges are provided for process and service components.

Note: SNMP process components do not include the virtual memory gauge.

Component Details

Provides a number of details about the component, including application status, component status, component type, component-specific properties, last up time, next poll time, and any warning or critical thresholds.

Component Availability

Provides a chart of component availability. To modify the chart, click the chart title. Ensure you adjust your polling to less than the interval you want displayed in charts. Not adjusting your polling will result in gaps in your charts. For more information about adjusting your polling, see “Scripting Custom Component Monitors” on page 23.

Last 25 Component Events

Provides the last 25 events specific to the component.

Min/Max Average Response Time

Provides a chart of the minimum, maximum, and average response times of the component. To modify the chart, click the chart title. This chart is available for port components only. Ensure you adjust your polling to less than the interval you want displayed in charts. Not adjusting your polling will result in gaps in your charts. For more information about adjusting your polling, see “Scripting Custom Component Monitors” on page 23.

Min/Max Average CPU Load

Provides a chart of the minimum, maximum, and average CPU loads of the component. To modify the chart, click the chart title. This chart is available for access and process components only. Ensure you adjust your polling to less than the interval you want displayed in charts. Not adjusting your polling will result in gaps in your charts. For more information about adjusting your polling, see “Scripting Custom Component Monitors” on page 23.

Min/Max Average Physical Memory

Provides a chart of the minimum, maximum, and average physical memory of the component. To modify the chart, click the chart title. This chart is available for access and process components only. Ensure you adjust your polling to less than the interval you want displayed in charts. Not adjusting your polling will result in gaps in your charts. For more information about adjusting your polling, see “Scripting Custom Component Monitors” on page 23.

Min/Max Average Virtual Memory

Provides a chart of the minimum, maximum, and average virtual memory of the component. To modify the chart, click the chart title. This chart is available for access and process components only. Ensure you adjust your polling to less than the interval you want displayed in charts. Not adjusting your polling will result in gaps in your charts. For more information about adjusting your polling, see “Scripting Custom Component Monitors” on page 23.

Min/Max Average Statistic Data

Provides a chart of the minimum, maximum, and average statistic data of the component. To modify the chart, click the chart title. This chart is available for access and process components only. Ensure you adjust your polling to less than the interval you want displayed in charts. Not adjusting your polling will result in gaps in your charts. For more information about adjusting your polling, see “Scripting Custom Component Monitors” on page 23.

For more information about a resource, click **Help** in the resource.

Creating Alerts for Applications

Orion APM provides a number of Orion APM-specific alerts you can use with Orion NPM Advanced Alert Manager to actively monitor and respond to detected issues. The Orion NPM Advanced Alerts Manager also allows you to designate actions in response to alerts.

Note: Only advanced alerts may be used for Orion APM-specific purposes. Basic alerts cannot be configured to trigger on Orion APM conditions or events.

Configuring Orion APM Alerts

Configuring an alert for Orion APM is similar to configuring an alert for Orion NPM.

To configure a new alert:

1. Log on to Windows server hosting Orion NPM.
2. Start the Advanced Alert Manager in the SolarWinds Orion program folder.
3. Click Configure Alerts. This opens the Manage Alerts window.

Example Orion APM Alert

This example sets up an alert triggered when a component's status is Critical, and logs the alert to the NetPerfMon event log.

To set up this alert trigger condition:

1. Click **New** in the **Manage Alerts** window.
2. Type **Alert me when a component goes critical** in the **Name of Alert** field.
3. Click the **Trigger Condition** tab.
4. Select **APM: Component** from the **Type of Property to Monitor** list.
5. Click **Add**, and then click **Simple Condition** from the shortcut menu.
6. Click the first asterisk (*) in the statement `* is equal to *`.
7. Point to **APM Component Monitors** and then click **Component Status** in the shortcut menu.
8. Click the remaining asterisk (*) in the statement `Component Status is equal to *`.
9. Type **Critical** in the list box.

To set up the alert trigger action:

1. Click the **Trigger Actions** tab.
2. Click **Add New Action**.
3. Select **Log the Alert to the NetPerfMon Event Log**, and then click **OK**.
4. Type "`The component `" in the message field, and then click **Insert Variable**.
5. Select **APM:Component** from the **Variable Category** list, select **ComponentName** from the **Select a Variable** list, and then click **Build Selected Variable**.
6. Type "` of node `" in the message field, and then click **Insert Variable**.
7. Select **General** from the **Variable Category** list, select **NodeName** from the **Select a Variable** list, and then click **Build Selected Variable**.
8. Type "` is `" in the message field, and then click **Insert Variable**.
9. Select **APM:Component** from the **Variable Category** list, select **ComponentStatus** from the **Select a Variable** list, and then click **Build Selected Variable**.

Note: The full message should read "`The component ${ComponentName} of node ${NodeName} is ${ComponentStatus}`".

10. Click **OK** to close the **Log Alert** window.

11. Click **OK** to close the **Edit Alert** window.

If any of your components go into a critical state, you will now see a line item for it in the Orion NPM Event Log.

Orion APM Alerts

Your installation of Orion APM supplements the alerting abilities of Orion NPM with a number of Orion APM-specific configurable alerts.

The following list provides the Orion APM properties on which you can trigger alerts:

Component Monitor Alerting Properties

Provides the following alert possibilities:

Component Name

Allows you to base your alert criteria on component names.

Component Type

Allows you to base your alert criteria on component types. Specify the component monitor type by value.

Component Monitor Type	Value
None	0
DHCP User Experience Monitor	35
Directory Size Monitor	38
DNS Monitor - TCP	4
DNS Monitor - UDP	5
DNS User Experience Monitor	15
Download Speed Monitor	25
File Age Monitor	36
File Change Monitor	23
File Count Monitor	39
File Existence Monitor	28
File Size Monitor	22
FTP Monitor	7
FTP User Experience Monitor	24
HTTP Form Login Monitor	27
HTTP Monitor	6
HTTPS Monitor	14
IMAP4 Monitor	13
IMAP4 User Experience Monitor	30
LDAP User Experience Monitor	34
Linux/Unix Script Monitor	21
MAPI User Experience Monitor	31
NNTP Monitor	11
ODBC User Experience Monitor	16
Oracle User Experience Monitor	18
Performance Counter Monitor	37
POP3 Monitor	12
POP3 User Experience Monitor	29
Process Monitor – SNMP	8
Process Monitor - WMI	1
SMTP Monitor	10
SNMP Monitor	32
SQL User Experience Monitor	17
TCP Port Monitor	2
Tomcat Server Monitor	33
Web Link Monitor	26
Windows Script Monitor	20
Windows Service Monitor	9
WMI Monitor	19

Component Status

Allows you to alert on Critical, Down, Unknown, Up, and Warning status.

Response Time

Allows you to alert on response time.

Statistic Data

Allows you to alert on statistic data.

Process (Service) Name

Allows you to alert on the process or service name. For example: *dns.exe*, or *AlertingEngine*.

Process Instance Count

Allows you to alert on the instance count of a process.

Percent CPU

Allows you to alert on the percentage of CPU in use.

Percent Physical Memory

Allows you to alert on the percentage of physical memory in use.

Percent Memory Used

Allows you to alert on the percentage of total memory in use.

Percent Virtual Memory

Allows you to alert on the percentage of virtual memory in use.

Virtual Memory Used

Allows you to alert on the amount of virtual memory in use, in bytes.

Application Monitor Alerting properties

Provides the following alert possibilities:

Application Name

Allows you to select the names of currently configured application templates as values.

Application Status

Allows you to select whether the application is in a Critical, Down, Unknown, Up, and Warning status.

Application Monitor Variables for Alerts

Orion APM adds the following variables to the core SolarWinds Orion variables when selecting APM-Application as the property type.

Application Variable	Definition
${Availability}	Provides the status of the application.
${ComponentsWithProblems}	Provides a comma-delimited list of components in a down, unknown, warning, or critical state.
${ComponentsWithStatus}	Provides a comma-delimited list of all components and their current status.
${ID}	Provides the numeric application ID of the specific application.
${LastTimeUp}	Provides the date and time the application was last seen in an Up state.
${Name}	Provides the name of the component, for example, `SW Orion Module Engine.`
${NodeID}	Provides the numeric node ID of the server on which the application is monitored.
${TimeStamp}	Provides the last polling date and time of an application.

Component Monitor Variables for Alerts

Orion APM adds the following variables to the core SolarWinds Orion variables when selecting APM-Component as the property type.

Component Monitor Variable	Definition
${ApplicationId}	Provides the unique numeric identifier of the application. This value is analogous to the node ID.
${ApplicationName}	Provides the name of the monitored application.
${ApplicationStatus}	Provides the status of the application.
${ComponentId}	Provides the numeric component ID of the specific application.
${ComponentName}	Provides the name of the component, for example, `SW Orion Module Engine`.
${ComponentStatus}	Provides the status of the specific component.
${ComponentType}	Provides the numeric component type. For more information, see “Orion APM Alerts” on page 38.
${DisplayType}	Provides the display type, for example, Windows Service, for the specific monitor.
${LastTimeUp}	Provides the date and time a component was last seen in the Up state.
${MemoryUsed}	Provides the memory used by a component, in bytes.
${NodeID}	Provides the numeric node ID of the server on which the application is monitored.

Component Monitor Variable	Definition
${PercentApplicationAvailability}	Provides the availability of an application as a percentage.
${PercentComponentAvailability}	Provides the availability of a component as a percentage.
${PercentCPU}	Provides the CPU used by a component as a percentage.
${PercentMemory}	Provides the memory used by a component as a percentage.
${PercentVirtualMemory}	Provides the virtual memory used by a component as a percentage.
${ProcessInstanceCount}	Provides the instance count of a process.
${ProcessName}	Provides the process name.
${ResponseTime}	Provides the response time of a component.
${StatisticData}	Provides the statistics data value of a component.
${StatusOrErrorDescription]	Provides the status of the component, including the full text of any error messages.
${Threshold-CPU-Critical}	Provides the critical threshold for CPU.
${Threshold-CPU-Warning}	Provides the warning threshold for CPU.
${Threshold-PhysicalMemory-Critical}	Provides the critical threshold for physical memory.
${Threshold-PhysicalMemory-Warning}	Provides the warning threshold for physical memory.
${Threshold-ResponseTime-Critical}	Provides the critical threshold for response time.
${Threshold-ResponseTime-Warning}	Provides the warning threshold for response time.
${Threshold-Statistic-Critical}	Provides the critical threshold for statistics.
${Threshold-Statistic-Warning}	Provides the warning threshold for statistics.
${Threshold-VirtualMemory-Critical}	Provides the critical threshold for virtual memory.
${Threshold-VirtualMemory-Warning}	Provides the warning threshold for virtual memory.
${TimeStamp}	Provides the last polling date and time of a component.
${VirtualMemoryUsed}	Provides the virtual memory used by a component, in bytes.

For more information about using Advanced Alerts within Orion Network Performance Monitor, see the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

Restarting Windows Services with an Alert Action

You can use the alert trigger action "Execute program" to restart a Windows service that is down. Orion APM restarts the service by running an included program named `APMServiceControl.exe` . When given the Component ID number of a Windows Service monitor, this program restarts the service using the service name and credential defined in the monitor.

The Component ID number of a monitor is an internal designation. Use the ${ComponentId} variable to pass the ComponentID to the program.

Example Alert Manager Trigger Action to Restart a Windows Service

```
Execute program: APMServiceControl.exe ${ComponentId}
```

Using the Preconfigured Restart a Service Alert

The SolarWinds Orion Alert Manager includes a pre-configured alert called **Restart a Service** that has a recovery action to restart a service if a Windows service component monitor is down. You must enable this alert manually because it is disabled by default.

To enable the Restart a Service alert:

1. Start **Advanced Alert Manager** in the **Alerting, Reporting, and Mapping** program group.
2. Click **Configure Alerts** from the **View** menu.
3. Check **Restart a Service**.
4. Click **Done**.

Creating APM-Specific Reports

Because Orion APM is an integrated module of Orion Network Performance Monitor (Orion NPM), Orion APM information is easily presented in a variety of formats using Orion NPM Report Writer. SolarWinds provides Report Writer as a quick and easy way for you to extract data from your database, including Orion APM statistics, for presentation in a useful form. A number of predefined Orion APM-specific reports are available with your installation of Orion APM. Report Writer also enables custom Orion APM report creation, as necessary, using criteria and conditions you choose. When you have finished editing your reports, you can view them through the Web Console and print them with the click of a button.

A report scheduling application is available to all customers with a current maintenance agreement. This tool schedules automatic email reports that can be sent to individual users or groups of users. Log in to the customer portal of www.solarwinds.com and download the Report Scheduler.

Report Writer capabilities are further enhanced when they are used in conjunction with the Custom Property Editor. Custom properties are available for report sorting and filtering. For more information about using custom properties, see the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

Using Predefined Orion APM Reports

The following historical Orion APM reports are immediately available with your Orion APM installation. Access these reports either by clicking **Reports** on the Web Console Views toolbar. You can modify reports to suit your application monitoring report requirements. For more information about using Orion NPM Report Writer, see “Viewing Application Performance Monitor Reports” on page 45.

Current Application and Component Status

The following reports are predefined for reporting current data on your monitored applications.

Average Response Time of each Component

Generates a report including the node, application, component and the component average and maximum response time.

Current CPU Load of each Component

Generates a report including the node, application, component, and percent of CPU load.

Current Memory Utilization of each Component

Generates a report including the node, application, component, actual and percent of physical and virtual memory used.

Current Status of each Application

Generates a report including the application and its status, for example, up or down.

Current Status of each Component

Generates a report including the node, application, component, and the individual status of the component, for example, up or down.

Daily Application Availability

The following reports are predefined for reporting daily monitored application availability.

Application Availability – Last Month

Generates a report that includes all applications and their average availability over the last month.

Application Availability – This Month

Generates a report that includes all applications and their average availability during the current month.

Application Availability – This Year

Generates a report that includes all applications and their average availability over the last year.

Historical Application CPU and Memory Reports

The following reports are predefined for reporting historical on your monitored applications.

CPU Load for each Application Monitor – This Month

Displays the average CPU load for each monitor, grouped by node and application name, for the current month.

CPU Load for each Application Monitor – Last Month

Displays the average CPU load for each monitor, grouped by node and application name, through the previous month.

CPU Load for each Application Monitor – This Year

Displays the average CPU load for each monitor, grouped by node and application name, through the previous month.

Memory Load for each Application Monitor – This Month

Displays the average memory load for each monitor, grouped by node and application name, for the current month.

Memory Load for each Application Monitor – Last Month

Displays the average memory load for each monitor, grouped by node and application name, through the previous month.

Memory Load for each Application Monitor – This Year

Displays the average memory load for each monitor, grouped by node and application name, through the previous month.

Viewing Application Performance Monitor Reports

Before you can use Report Writer, you must have collected at least a few minutes worth of data in a database that is populated with the devices that you want to monitor. A variety of reports are included with Report Writer, and icons that precede report names distinguish the different types of reports that are available. The following procedure starts Report Writer.

To start Report Writer:

1. Click **Start > All Programs > SolarWinds Orion > Report Writer**.
2. Click **File > Settings**.
3. In the General tab of the Report Writer Settings window, select either of the following as a default viewing mode:
   - **Preview** displays the report as it will appear in printed form.
   - **Report Designer** is the report creation and editing interface.

   Note: You can toggle between Preview and Report Designer modes at any time by clicking **Preview** or **Design**, respectively, on the toolbar.
4. ***If you want to separate the data for individual network objects with horizontal lines,*** click **Report Style,** and then check **Display horizontal lines between each row.**
5. Click **OK** to exit Report Writer Settings.
6. ***If you want to open a predefined report,*** select one from the list in the left pane of the main window.

   Note: Application Performance Monitor supplies the following predefined reports:
   - Current Application and Component Status
     - Average Response Time of each Component
     - Current CPU Load of each Component
     - Current Memory Utilization of each Component
     - Current Status of each Application
     - Current Status of each Component
   - Daily Application Availability
     - Application Availability – Last Month
     - Application Availability – This Month
     - Application Availability – This Year
   - Historical Application CPU and Memory Reports:

- CPU Load for each Application Monitor – This Month
- CPU Load for each Application Monitor – Last Month
- CPU Load for each Application Monitor – This Year
- Memory Load for each Application Monitor – This Month
- Memory Load for each Application Monitor – Last Month
- Memory Load for each Application Monitor – This Year

7. ***If you want to create a new report,*** click **File > New Report**.

   Note: For more information on how to use the Orion NPM Report Writer application, see the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

Filtering and Grouping Data in Resources

You can reorganize and filter application data within a resource using SolarWinds Query Language (SWQL), a SQL-like filter syntax.

Grouping Applications

The following procedure walks you through changing the way node data is grouped in a resource.

To group resource data by category:

1. Log on to the Orion APM Web Console.
2. Click **Edit** on the resource with the grouping you want to change.
3. Select the category that you want to group by from the **Level 1** list.
4. If you want to group by more subcategories, select additional categories from the **Level 2** and the **Level 3** lists.
5. Click **Submit**.

Filtering Data Using SWQL Filter Criteria

The following procedure explains how to limit the data sources in a resource by setting filter criteria in SWQL syntax. For more information about the filter syntax, see “SWQL Syntax” on page 48.

To filter node data using filter syntax:

1. Log on to the Orion APM Web Console.
2. Click **Edit** on the resource that you want to change.
3. Type your filter criteria in the **Filter Nodes SQL** field.
4. Click **Save**.

SWQL Syntax

You can filter data by both built-in and custom properties.

Filtering by Built-in Properties

Many properties have the same name between data types. To prevent ambiguity, Orion APM prefixes the property names with the data type.

Example filter to show data from Cisco devices:

```
Node.Vendor = 'Cisco'
```

Example filter to show data from Windows Server 2003-2008 applications:

```
Application.Name = 'Windows Server 2003-2008'
```

Example filter to show data from devices beginning with "AX3":

```
Node.Caption Like 'AX3-*'
```

Example filter to show data from Process Monitor – SNMP type component monitors:

```
Monitor.ComponentType = 8
```

Filtering by Status Property

To filter by the Status property, you must know the valid status levels.

Level	Status
0	Unknown
1	Up
2	Down
3	Warning

Example filter to only show monitors that are not down:

```
MonitorStatus.Availability<>2
```

Filtering by Custom Property

The property syntax to filter by custom property is:

dataType`.CustomProperty.`*propertyName*

Example filter to only show nodes with the custom property City that matches Atlanta:

```
Node.CustomProperty.City = 'Atlanta'
```

Built-in Properties for Applications

Application.ID	Application.Name	Application.NodeID
Application.TemplateID	Application.JobId	Application.Unmanaged
Application.UnmanageFrom	Application.UnmanageUntil	Application.Created
Application.LastModified		

Built-in Properties for Application Status

ApplicationStatus.ApplicationID	ApplicationStatus.Availability
ApplicationStatus.TimeStamp	ApplicationStatus.LastTimeUp

Built-in Properties for Monitors

Monitor.ApplicationID	Monitor.ComponentType	Monitor.ID
Monitor.JobId	Monitor.Name	Monitor.TemplateID

Built-in Properties for Monitor Status

MonitorStatus.ApplicationID	MonitorStatus.Availability	MonitorStatus.ComponentID
MonitorStatus.ComponentStatusID	MonitorStatus.LastTimeUp	MonitorStatus.TimeStamp

Built-in Properties for Nodes

Node.AvgResponseTime	Node.CPULoad	Node.Caption
Node.Contact	Node.DNS	Node.Description
Node.GroupStatus	Node.IOSImage	Node.IOSVersion
Node.IPAddress	Node.LastBoot	Node.LastSync
Node.Location	Node.MachineType	Node.MaxResponseTime
Node.MemoryUsed	Node.MinResponseTime	Node.NodeID
Node.ObjectSubType	Node.OrionID	Node.PercentLoss
Node.PercentMemoryUsed	Node.ResponseTime	Node.Severity
Node.Status	Node.StatusDescription	Node.SysName
Node.SysObjectID	Node.SystemUpTime	Node.TotalMemory
Node.Vendor	Node.VendorIcon	

Appendix A

Additional Poller and Website-Only Install

Additional pollers and the installation of additional websites help you extend your Application Performance Monitor implementation. You can install additional pollers to aid you in load balancing and configure additional websites to ensure redundant access through more than one web server.

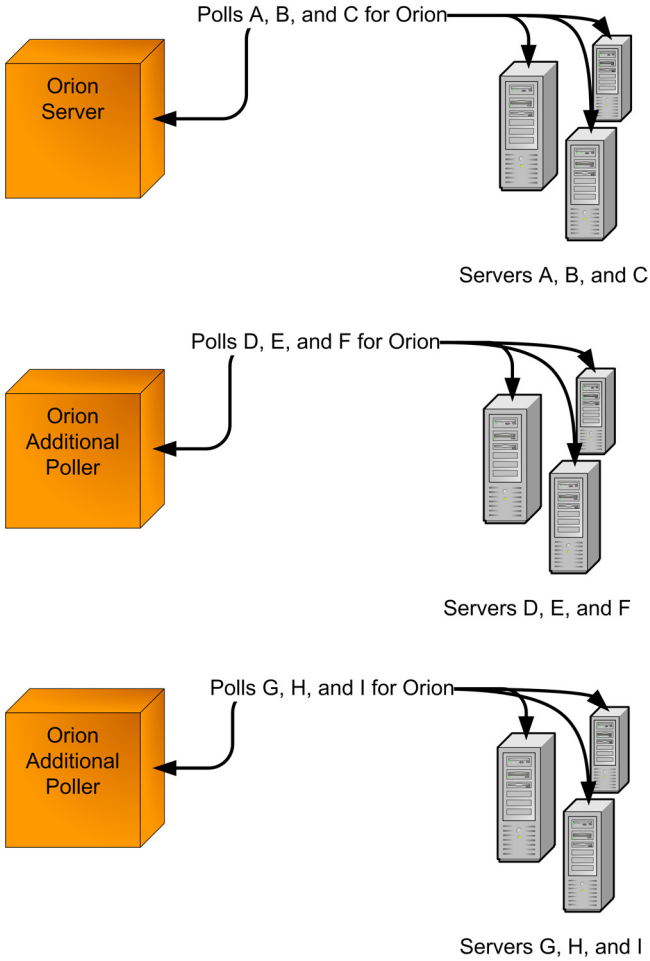
The following sections provide installation procedures for adding pollers and websites. These components are licensed and purchased separately from your main Application Performance Monitor install and require the installation of the matching Orion NPM component. For example, if you want to install an APM additional poller, you must install it on an Orion NPM additional poller. For more information about purchasing licenses, contact your sales representative or customer service (sales@solarwinds.com).

Understanding How Pollers Work

Before you install an additional Application Performance Monitor (Orion APM) poller, review the following diagrams and ensure you understand how Application Performance Monitor polls when first installed and how Orion APM additional pollers work.

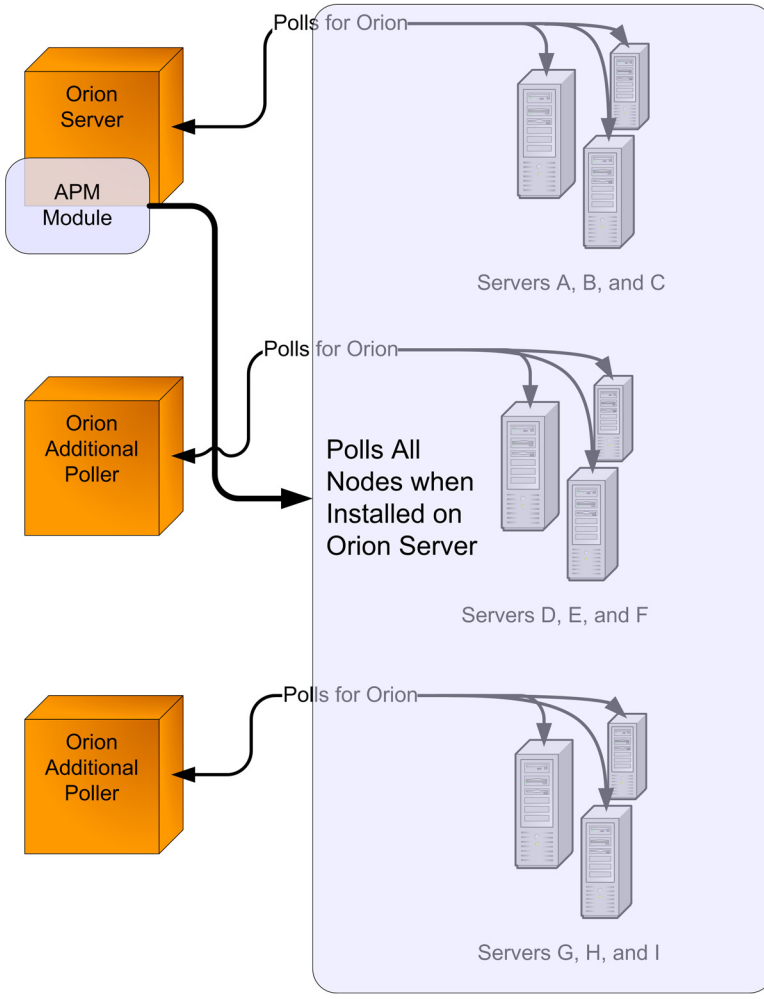
Orion NPM Additional Pollers are Poller-Aware

When you install an additional Orion NPM poller, the pollers are automatically *aware*. *Poller-aware* means each poller, including the Orion NPM server, polls only those nodes associated with it.



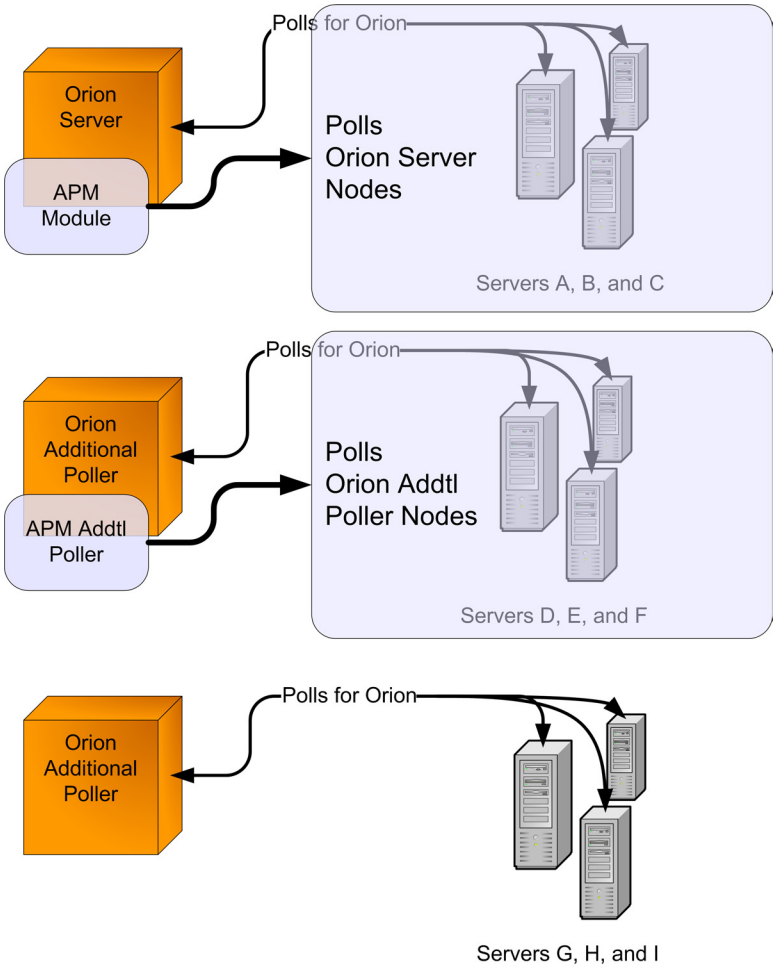
Application Performance Monitor is Poller-Unaware

When you add Application Performance Monitor (Orion APM) to your Orion NPM server, APM is poller-unaware and can poll any node.



Application Performance Monitor Pollers Made Poller-Aware

After you add an Application Performance Monitor (Orion APM) additional poller and change the polling engine mode on your Orion NPM server, the Orion APM additional poller becomes poller-aware, mimicking the behavior of Orion NPM. If you do not have an Orion APM additional poller on an Orion NPM additional poller, the nodes polled by that poller are not polled by Orion APM. For more information about changing the polling engine mode on your Orion NPM server, see “Installing an Additional Poller” on page 55.



Installing an Additional Poller

You must install the Application Performance Monitor additional poller on a computer where you have already installed an Orion NPM additional poller. At this time, this additional poller must exist within the same domain or in a domain with a full (two-way) trust with the Orion NPM server. For more information about Orion NPM additional poller requirements, see the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

Note: After completing the following procedure, Orion APM pollers emulate the same behavior as Orion NPM additional pollers. They monitor only those applications on nodes associated with the Orion NPM additional poller.

To install the additional poller:

1. Log on to your current Orion NPM additional poller with an administrator account.
2. Navigate to and run the additional poller executable.
3. Review the Welcome window, and then click **Next**.
4. Accept the license agreement, and then click **Next**.
5. Click **Install**.
6. ***If you are prompted to license the product,*** enter your customer information on the License Key window. For more information, see “Activating Your License” on page 4. Click **Continue**.
7. Click **Finish** to complete the Installation wizard.
8. Review the Configuration wizard Welcome window, and then click **Next**.
9. Ensure you check the appropriate services, including the **APM Job Engine Plugin** and the **SolarWinds Job Engine**, and then click **Next**.
10. Review the Configuration wizard Summary window, and then click **Next**.
11. Click **Finish** to complete the Configuration wizard.
12. ***If this is the first additional poller you have installed,*** complete the following procedure:

a. Log on to your Orion NPM Web Console with an Administrator account.

b. Click **Application Performance Monitor** in the Modules toolbar.

c. Click **APM Settings**.

d. Click **Data & Database Settings**.

e. Select **Poller-Bound** as the Polling Engine Mode.

f. Click **Submit**.

g. Log on to the Orion NPM server with a Windows administrator account.

h. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager**.

i. Select **SolarWinds Orion Module Engine**, and then click **Restart**.

Installing the Website-Only Package

You must install the Application Performance Monitor website-only expansion on a previously installed version of an Orion NPM website-only install. The additional requirements for the Application Performance Monitor expansion should require no upgrades to your existing install. At this time, the additional website must exist within the same domain or in a domain with a full (two-way) trust with the Orion NPM server, and TCP port 17777 must be open on both the Orion NPM server and the website.

Additional Web Console installations do not include the default APM reports. To ensure your default APM reports are available on your Additional Web Console install, copy the `Reports` folder to your Additional Web Console server. By default, you can find the `Reports` folder in `\Program Files\SolarWinds\Orion`.

Ensure you schedule an appropriate maintenance window in which to install the additional Web Console. For more information about implementing the Orion NPM website-only install, see the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

To install the website-only package:

1. Log on to your current Orion NPM website-only server with an administrator account.

2. Navigate to and run the website-only executable.

3. Review the Welcome window, and then click **Next**.

4. Accept the license agreement, and then click **Next**.

5. Click **Install**.

6. Click **Finish** to complete the Installation wizard.

7. Review the Configuration wizard Welcome window, and then click **Next**.
8. Specify the appropriate information on the Database Settings window, and then click **Next**.
9. Specify the appropriate database to use, and then click **Next**. Ensure you have stopped your polling engines before continuing.
10. Specify the appropriate database account on the Database Account window, and then click **Next**.
11. Select the IP address, port, and Website root directory on the Website Settings window, and then click **Next**.
12. Review the configuration summary, and then click **Next**.
13. Click **Finish** to complete the Configuration wizard.

Appendix B

Templates Reference

Orion APM contains pre-defined application monitor templates to help get you started monitoring applications. For instructions on how to assign templates to nodes, see "Manually Assigning Templates to Nodes" on page 15.

Added to Version 3.0

- "Tomcat Server Template" on page 142
- "Windows Print Services" on page 148

Added to Version 2.5

- "Active Directory" on page 62
- "Apache" on page 63
- "DNS User Experience" on page 85
- "Download Speed Monitor" on page 86
- "File Age Monitor" on page 106
- "File Change Monitor" on page 107
- "File Count Script" on page 108
- "File Existence Monitor" on page 109
- "File Size Monitor" on page 110
- "Finger Port Monitor" on page 112
- "FTP User Experience" on page 113
- "Generic DNS" on page 114
- "Gopher Port Monitor" on page 117
- "HTTP" on page 118
- "HTTP Form Login" on page 119
- "IMAP4 Round Trip Email" on page 120
- "IRC Port Monitor" on page 122
- "LDAP Connection Monitor" on page 123
- "MAPI Round Trip Email" on page 126
- "POP3 Round Trip Email" on page 130
- "Run 3rd Party Application" on page 131
- "RWHOIS Port Monitor" on page 133
- "SNPP Port Monitor" on page 136
- "SQL Server 2008 Database" on page 139
- "SQL Server Query" on page 140
- "Web Link" on page 143

Added to Version 2.0

- "Exchange 2007" on page 87
- "Exchange 2007 WMI Counters" on page 100
- "Exchange Server 2000 and 2003" on page 104
- "FileModified (vbscript)" on page 111
- "Internet Information Services" on page 121
- "Linux/Unix Operating System" on page 124
- "Oracle Database" on page 128
- "Orion Server" on page 129
- "SQL Server 2005 Database" on page 138
- "Windows Event Log Count" on page 145
- "Windows Server 2003-2008" on page 149

Added to Version 1.0

- "CiscoSecure ACS (via SNMP)" on page 70
- "Exchange Server (via SNMP)" on page 103
- "Generic Mail Server" on page 115
- "Generic Web Server" on page 116
- "SQL Server (via SNMP)" on page 137
- "thwack.com - User Experience Monitor Example" on page 141
- "Windows DNS Server (via SNMP)" on page 144
- "Windows FTP Server (via WMI)" on page 147

Active Directory

This template assesses the overall health of Active Directory services on a domain controller.

Prerequisites: WMI access to domain controller.

Credentials: Windows Administrator on domain controller.

Monitored Components

Active Directory

Address Book Client Sessions

Directory Service Notify Queue Size

Directory Service Threads in Use

Distributed File System Service

DNS Client Service

DNS Server Service

File Replication Service

Intersite Messaging Service

Kerberos Key Distribution Center Service

LDAP Active Threads

LDAP Bind Time

LDAP Client Sessions

LDAP Version Script

Net Logon Service

Remote Procedure Call (RPC) Service

Security Accounts Manager Service

Server Service

Windows Time Service

Workstation Service

Apache

This template retrieves Apache server statistics from the built-in Apache /server-status web page.

Prerequisites: Configure the Apache web server to allow itself access to the /server-status page.

Credentials: SSH account on the web server.

Configuring the Apache server for Orion APM monitoring:

1. Log on to your Apache server using an SSH or telnet client.
2. Grant yourself root permissions (`su root`).
3. Locate the Apache configuration file, typically in `/usr/local/apache/conf`.
4. Append the following lines to your `httpd.conf` Apache configuration file, substituting the IP address or host name of your Apache server for localhost. Use localhost only if the Apache server services the loopback interface.

```
<Location /server-status>
SetHandler server-status
Order Deny,Allow
Deny from all
Allow from "localhost"
</Location>
ExtendedStatus On
```

5. Restart the Apache server (`apachectl graceful`).

Monitored Components

BusyWorkers

IdleWorkers

ServerKbytesPerRequest

ServerKbytesPerSec

ServerRequestPerSecond

ServerUptime

TotalAccess

TotalTraffic

Blackberry Delivery Confirmation

This template tests the ability of a Blackberry handheld device to receive messages using the built-in delivery confirmation function. The script in this template sends a specially formed test email to the blackberry device, and then the script checks an email account for the confirmation reply from the blackberry device.

Note: The script in this template requires you to customize variables before it can be run.

Prerequisites: Access to an SNMP Server. MAPI access to a Microsoft Exchange server. MAPI Client and CDO Objects installed on Orion APM server.

Credentials: Windows credential valid on both the Orion APM server and the Microsoft Exchange server.

Customizing Script Variables

You must substitute your own values for many of the following variables in the script body:

`const SenderMailbox = "apm.test"`

Replace *apm.test* with the Exchange mailbox for sending and receiving the delivery confirmation messages.

`const SenderEmailAddress = apm.test@example.com`

Replace *apm.test@example.com* with the email address for sending and receiving the test and the confirmation messages.

`const BlackberryAddress = test.blackberry@example.com`

Replace *test.blackberry@example.com* with the email address of the user with the Blackberry handheld device.

`const ExchangeServer = "exchange.example.com"`

Replace *exchange.example.com* with the Microsoft Exchange server hosting the Exchange mailbox.

`const SenderSmtpServer = "smtp.example.com"`

Replace *smtp.example.com* with the SMTP Server for sending the test email.

`const SenderSmtpPort = 25`

The script uses port 25 on the SMTP server for sending the test email. If the SMTP server uses a different port, change this value.

`const MaxInboxScans = 300`

The script will scan for the confirmation message on the Exchange mailbox 300 times. If this is too many or too few, change this value.

`const MaxMessagesPerScan = 100`

The script will the most recent 100 messages in the Exchange mailbox for the confirmation message. If this is too many or too few, change this value.

`const MillisecondsBetweenScans = 1000`

The script will wait 1000 milliseconds between Exchange mailbox scans. If this is too long or too short, change this values.

Monitored Components

BlackBerry Delivery Confirmation

Blackberry Enterprise Server

This template monitors the status of services and server statistics related to the operation of Blackberry Enterprise Servers.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Blackberry Router Service

Net Service Name: Blackberry Router

Blackberry Alert Service

Net Service Name: Blackberry Alert

Blackberry Attachment Service

Net Service Name:Blackberry Attachment Service

Blackberry Collaboration Service

Net Service Name:Blackberry Collaboratin Service

Blackberry Controller Service

Net Service Name:Blackberry Controller

Blackberry MDS Connection Service

Net Service Name:Blackberry MDS Connection Service

Blackberry Policy Service

Net Service Name:Blackberry Policy Service

Blackberry Synchronization Service

Net Service Name:Blackberry Synchronization Service

Blackberry Convert Process

Process name: BBConvert.exe

Connection State

0 is disconnected, 1 is connected.

Messages Expired

The total number of expired messages.

Messages Queued for Delivery

The number of pending messages queued for handheld device delivery.

Messages Received per Minute

The average number of messages per minute received by handheld device.

Messages Sent per Minute

The average number of messages per minute sent by handheld device.

Cisco CallManager

This template monitors critical events generated by Cisco CallManager indicating possible service outages or configuration problems. Alerts are set to display the descriptions of events and the host name.

Prerequisites: SNMP access to target server.

Credentials: None

Monitored Components

CallManager Status

The current status of the CallManager. Status 1 is unknown, 2 is up, 3 is down.

Registered Phones

The number of phones registered with the local call manager.

Unregistered Phones

The number of phones not registered with the local call manager.

Rejected Phones

The number of phones refused registration by the local call manager.

Registered Gateways

The number of gateways registered with the local call manager.

Unregistered Gateways

The number of gateways not registered with the local call manager.

Rejected Gateways

The number of gateways refused registration by the local call manager.

Registered Media Devices

The number of media devices registered with the local call manager.

Unregistered Media Devices

The number of media devices not registered with the local call manager.

Rejected Media Devices

The number of media devices refused registration by the local call manager.

Registered CTI Devices

The number of CTI devices registered with the local call manager.

Unregistered CTI Devices

The number of CTI devices not registered with the local call manager.

Rejected CTI Devices

The number of CTI devices refused registration by the local call manager.

Registered Voice Messaging Devices

The number of voice messaging devices registered with the local call manager.

Unregistered Voice Messaging Devices

The number of voice messaging devices not registered with the local call manager.

Rejected Voice Messaging Devices

The number of voice messaging devices refused registration by the local call manager.

Citrix Licensing

Net Service Name: lmgrd

CiscoSecure ACS (via SNMP)

This template assesses the overall performance of a CiscoSecure ACS server by monitoring its key processes.

Prerequisites: SNMP access to target server.

Credentials: None.

Monitored Components

CS Admin - SNMP

Process Name: CSAdmin.exe

CS Auth - SNMP

Process Name: CSAuth.exe

CS Tacacs - SNMP

Process Name: CSTacacs.exe

CS Radius - SNMP

Process Name: CSRadius.exe

CS DBSync - SNMP

Process Name: CSDBSync.exe

CS Log - SNMP

Process Name: CSLog.exe

CS Mon - SNMP

Process Name: CSMon.exe

Citrix XenApp 5.0 Core WMI Counters

This template monitors critical events generated by Citrix XenApp 5.0 indicating possible service outages or configuration problems. Alerts are set to display the descriptions of events and the host name.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Citrix CPU Utilization Management: CPU Entitlement

The percentage of CPU the Citrix CPU Utilization Management has made available to users

Citrix CPU Utilization Management: CPU Reservation

The percentage of CPU the Citrix CPU Utilization Management has reserved for users if needed.

Citrix CPU Utilization Management: CPU Shares

The percentage of CPU assigned to a user.

Citrix CPU Utilization Management: CPU Usage

The percentage of CPU used by a user averaged over a short period of time.

Citrix CPU Utilization Management: CPU Long-term CPU Usage

The percentage of CPU used by a user averaged over a longer period of time.

Citrix IMA Networking: Bytes Received/sec

The data rate of incoming IMA network traffic.

Citrix IMA Networking: Bytes Sent/sec

The data rate of outgoing IMA network traffic.

Citrix IMA Networking: Network Connections

The number of active network IMA connections to IMA servers.

Citrix Licensing: Average License Check-In Response Time (ms)

The average response time for a license check-in operation.

Citrix Licensing: Average License Check-Out Response Time (ms)

The average response time for a license check-out operation.

Citrix Licensing: Last Recorded License Check-In Response Time (ms)

The last response time for a license check-in operation.

Citrix Licensing: Last Recorded License Check-Out Response Time (ms)

The last response time for a license check-out operation.

Citrix Licensing: License Server Connection Failure

The time in minutes that the Citrix XenApp server has been without a connection to the license server.

Citrix Licensing: Maximum License Check-In Response Time (ms)

The maximum response time for a license check-in operation.

Citrix Licensing: Maximum License Check-Out Response Time (ms)

The maximum response time for a license check-out operation.

Secure Ticket Authority: STA Bad Data Request Count

The number of unsuccessful ticket validation and data requests over the lifetime of the STA

Secure Ticket Authority: STA Bad Refresh Request Count

The number of unsuccessful ticket refresh requests over the lifetime of the STA.

Secure Ticket Authority: STA Bad Ticket Request Count

The number of unsuccessful ticket creation requests over the lifetime of the STA.

Secure Ticket Authority: STA Count of Active Tickets

The number of tickets currently in the STA.

Secure Ticket Authority: STA Good Data Request Count

The number of successful ticket validation and data requests over the lifetime of the STA.

Secure Ticket Authority: STA Good Refresh Request Count

The number of successful ticket refresh requests over the lifetime of the STA.

Secure Ticket Authority: STA Good Ticket Request Count

The number of successful ticket creation requests over the lifetime of the STA.

Secure Ticket Authority: STA Peak All Request Rate

The highest activities per second recorded for all activities over the lifetime of the STA.

Secure Ticket Authority: STA Peak Data Request Rate

The highest data requests per second recorded over the lifetime of the STA.

Secure Ticket Authority: STA Peak Ticket Refresh Rate

The highest ticket refresh requests per second recorded over the lifetime of the STA.

Secure Ticket Authority: STA Peak Ticket Request Rate

The highest ticket creation requests per second recorded over the lifetime of the STA.

Secure Ticket Authority: STA Ticket Timeout Count

The number of ticket request timeouts recorded over the lifetime of the STA.

Citrix XenApp 5.0 ICA Session WMI Counters

This template monitors critical events generated by Citrix XenApp 5.0 indicating possible service outages or configuration problems. Alerts are set to display the descriptions of events and the host name.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Input Audio Bandwidth

The client to server bandwidth used for audio in ICA sessions. Bits per second.

Input Clipboard Bandwidth

The bandwidth used for cut, paste, and other clipboard operations between ICA sessions and local windows. Bits per second.

Input COM 1 Bandwidth

The bandwidth used for printing to the client COM 1 port through an ICA session without print spooler support. Bits per second.

Input COM 2 Bandwidth

The bandwidth used for printing to the client COM 2 port through an ICA session without print spooler support. Bits per second.

Input COM Bandwidth

The client to server bandwidth used receiving data from the client COM port. Bits per second.

Input Control Channel Bandwidth

The client to server bandwidth used to execute the LongCommandLine parameters of published applications. Bits per second.

Input Drive Bandwidth

The client to server bandwidth used to perform file operations during ICA sessions. Bits per second.

Input Font Data Bandwidth

The bandwidth used to initiate the font changes in ICA sessions with SpeedScreen. Bits per second.

Input Licensing Bandwidth

The bandwidth used to negotiate session licensing. Bits per second. This counter normally contains no data.

Input LPT1 Bandwidth

The virtual channel bandwidth used for printing to the client LPT1 port through an ICA session without print spooler support. Bits per second.

Input LPT2 Bandwidth

The virtual channel bandwidth used for printing to the client LPT2 port through an ICA session without print spooler support. Bits per second.

Input Management Bandwidth

The bandwidth used to perform management tasks. Bits per second.

Input PN Bandwidth

The Program Neighborhood bandwidth used to obtain details about application sets. Bits per second.

Input Printer Bandwidth

The bandwidth used for printing to a client printer through a client with print spooler support. Bits per second.

Input Seamless Bandwidth

The bandwidth used for published applications not embedded in a session window. Bits per second.

Input Session Bandwidth

The client to server bandwidth used for a session. Bits per second.

Input Session Compression

The client to server compression ratio used for a session.

Input Session Line Speed

The client to server line speed for a session. Bits per second.

Input SpeedScreen Data Channel Bandwidth

The client to server bandwidth used for data channel traffic. Bits per second.

Input Text Echo Bandwidth

The client to server bandwidth used for text echo. Bits per second.

Input ThinWire Bandwidth

The client to server bandwidth used for ThinWire traffic. Bits per second.

Input VideoFrame Bandwidth

The client to server bandwidth used for traffic over virtual channels. Bits per second.

Latency - Last Recorded

The last recorded latency value of the session.

Latency - Session Average

The average latency over the session lifetime.

Latency - Session Deviation

The difference between the minimum and the maximum session latency values.

Output Audio Bandwidth

The server to client bandwidth used for audio in ICA sessions. Bits per second.

Output Clipboard Bandwidth

The bandwidth used for cut, paste, and other clipboard operations between ICA sessions and local windows. Bits per second.

Output COM 1 Bandwidth

The bandwidth used for printing to the client COM 1 port through an ICA session without print spooler support. Bits per second.

Output COM 2 Bandwidth

The bandwidth used for printing to the client COM 2 port through an ICA session without print spooler support. Bits per second.

Output COM Bandwidth

The server to client bandwidth used receiving data from the client COM port. Bits per second.

Output Control Channel Bandwidth

The server to client bandwidth used to execute the LongCommandLine parameters of published applications. Bits per second.

Output Drive Bandwidth

The server to client bandwidth used to perform file operations during ICA sessions. Bits per second.

Output Font Data Bandwidth

The bandwidth used to initiate the font changes in ICA sessions with SpeedScreen. Bits per second.

Output Licensing Bandwidth

The bandwidth used to negotiate session licensing. Bits per second. This counter normally contains no data.

Output LPT1 Bandwidth

The bandwidth used for printing to the client LPT1 port through an ICA session without print spooler support. Bits per second.

Output LPT2 Bandwidth

The bandwidth used for printing to the client LPT2 port through an ICA session without print spooler support. Bits per second.

Output Management Bandwidth

The bandwidth used to perform management tasks. Bits per second.

Output PN Bandwidth

The Program Neighborhood bandwidth used to obtain details about application sets. Bits per second.

Output Printer Bandwidth

The bandwidth used for printing to a client printer through a client with print spooler support. Bits per second.

Output Seamless Bandwidth

The bandwidth used for published applications not embedded in a session window. Bits per second.

Output Session Bandwidth

The server to client bandwidth used for a session. Bits per second.

Output Session Compression

The server to client compression ratio used for a session.

Output Session Line speed

The server to client line speed used for a session. Bits per second.

Output SpeedScreen Data Channel Bandwidth

The server to client bandwidth used for data channel traffic. Bits per second.

Output Text Echo Bandwidth

The bandwidth used for text echo. Bits per second.

Output ThinWire Bandwidth

The server to client bandwidth used for ThinWire traffic. Bits per second.

Output VideoFrame Bandwidth

The server to client bandwidth used for traffic on virtual channels. Bits per second.

Citrix XenApp 5.0 Presentation Server WMI Counters

This template monitors critical events generated by Citrix XenApp 5.0 indicating possible service outages or configuration problems. Alerts are set to display the descriptions of events and the host name.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Application Enumeration/sec

The number of application enumerations per second.

Application Resolution Time (ms)

The time in milliseconds that a resolution took to complete.

Application Resolutions Failed/sec

The number of application resolutions failed per second.

Application Resolutions/sec

The number of resolutions completed per second.

DataStore Connection Failure

The number of minutes that the XenApp server has been disconnected from the data store.

DataStore bytes read

The number of bytes read from the data store.

DataStore bytes read/sec

The number of bytes of data store data read per second.

DataStore bytes written/sec

The number of bytes of data store data written per second.

DataStore reads

The number of times data was read from the data store.

DataStore reads/sec

The number of times data was read from the data store per second.

DataStore writes/sec

The number of times data was written to the data store per second.

DynamicStore bytes read/sec

The number of bytes of dynamic store data read per second.

DynamicStore bytes written/sec

The number of bytes of dynamic store data written per second.

DynamicStore Gateway Update Count

The number of dynamic store update packets sent to remote data collectors.

DynamicStore Gateway Update Bytes Sent

The number of bytes of data sent across gateways to remote data collectors.

DynamicStore Query Count

The number of dynamic store queries that were performed.

DynamicStore Query Request Bytes Received

The number of bytes of data received in dynamic store query request packets.

DynamicStore Query Response Bytes Sent

The number of bytes of data sent in response to dynamic store queries.

DynamicStore reads/sec

The number of times data was read from the dynamic store per second.

DynamicStore Update Bytes Received

The number of bytes of data received in dynamic store update packets.

DynamicStore Update Packets Received

The number of update packets received by the dynamic store.

DynamicStore Update Response Bytes Sent

The number of bytes of data sent in response to dynamic store update packets.

DynamicStore writes/sec

The number of times data was written to the dynamic store per second.

Filtered Application Enumerations/sec

The number of filtered application enumerations per second.

LocalHostCache bytes read/sec

The number of bytes of IMA local host cache data read per second.

LocalHostCache bytes written/sec

The number of bytes of IMA local host cache data written per second.

LocalHostCache reads/sec

The number of times data was read from the IMA local host cache per second.

LocalHostCache writes/sec

The number of times data was written to the IMA local host cache per second.

Maximum number of XML threads

The maximum number of threads allocated to service Web-based sessions since the server restarted.

Number of busy XML threads

The number of busy threads.

Number of XML threads

The number of threads allocated to service Web-based sessions.

Resolution WorkItem Queue Executing Count

The number of resolution work items that are currently being executed.

Resolution WorkItem Queue Ready Count

The number of resolution work items that are ready to be executed.

WorkItem Queue Executing Count

The number of work items that are currently being executed.

WorkItem Queue Pending Count

The number of work items that are not yet ready to be executed.

WorkItem Queue Ready Count

The number of work items that are ready to be executed.

Zone Elections

The number of zone elections that occurred. This value starts at zero each time the IMA Service starts and is incremented each time a zone election takes place.

Zone Elections Won

The number of times the server won a zone election.

Citrix XenApp 5.0 Services

This template monitors critical events generated by Citrix XenApp 5.0 indicating possible service outages or configuration problems. Alerts are set to display the descriptions of events and the host name.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Citrix ActiveSync Service

Net Service Name: ctxactivesync

Citrix ADF Installer Service

Net Service Name: agentsvc

Citrix Client Network

Net Service Name: cdmsvc

Citrix CPU Utilization Management CPU Rebalancer

Net Service Name: ctxcpubal

Citrix CPU Utlization Management Resource Management

Net Service Name: ctxcpusched

Citrix CPU Utilization Management User Session Sync 4.0 only

Net Service Name: ctxcpuusync

Citrix Diagnostic Facility COM Server

Net Service Name: cdfsvc

Citrix Encryption Service

Net Service Name: encsvc

Citrix Health Monitoring and Recovery 4.5 only

Net Service Name: hcaservice

Citrix Independent Management and Architecture

Net Service Name: lmasrv

Citrix License Management Console

Net Service Name: tomcat

Citrix Licensing WMI

Net Service Name: Citrix_gtlicensingprov

Citrix MFCOM Service

Net Service Name: mfcom

Citrix Print Manager Service

Net Service Name: cpsvc

Citrix Resource Manager Mail

Net Service Name: mailservice

Citrix Services Manager 4.5 only

Net Service Name: imaadvancesrv

Citrix SMA Service

Net Service Name: smaservice

Citrix Strreaming Service 4.5 only

Net Service Name: radesvc

Citrix Virtual Memory Optimization

Net Service Name: ctxsfosvc

Citrix WMI Service

Net Service Name: ctxwmisvc

Citrix XTE Server

Net Service Name: xte

DNS User Experience

This template tests the ability of a DNS server to respond to a record query, and measures its responsiveness.

Prerequisites: None.

Credentials: None.

Monitored Components

DNS User Experience Monitor

Download Speed Monitor

This template tests the available bandwidth between the Orion APM server and another node on the network.

Prerequisites: A character generator service running on target server.

Credentials: None.

Installing the Microsoft Windows Character Generator Service

The Character Generator service is part of the Microsoft Windows Simple TCP/IP Services component.

To install the Simple TCP/IP Services component on a Windows 2000, XP, and 2003 computers:

1. Log in to target server with an administrator-level account.
2. Open **Add or Remove Programs** in the **Control Panel**.
3. Click **Add/Remove Windows Components**.
4. Click **Networking Services**.
5. Click **Details**.
6. Select **Simple TCP/IP Services**.
7. Click **OK, Next**, and then click **Finish** to complete the Wizard.

Enabling the Unix/Linux Character Generator Service

The character generator service `chargen` is built into the standard Unix/Linux `inetd` daemon. If the service is not enabled, add the following lines to the `/etc/inetd.conf` configuration file, and then restart `inetd`.

```
chargen stream tcp nowait root internal
chargen dgram udp wait root internal
```

Monitored Components

Download Speed Monitor

Exchange 2007

This template assesses the status of Windows services related to Microsoft Exchange 2007.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

IIS Admin Service

Microsoft Exchange Active Directory Topology

Microsoft Exchange ADAM

Microsoft Exchange Credential Service

Microsoft Exchange File Distribution Service

Microsoft Exchange IMAP4

Microsoft Exchange Information Store

Microsoft Exchange Mail Submission Service

Microsoft Exchange Mailbox Assistants

Microsoft Exchange POP3

Microsoft Exchange Replication Service

Microsoft Exchange Search Indexer

Microsoft Exchange Service Host

Microsoft Exchange Speech Engine

Microsoft Exchange System Attendant

Microsoft Exchange Transport

Microsoft Exchange Transport Log Search

Microsoft Exchange Unified messaging

Microsoft Search (Exchange)

World Wide Web Publishing Service

Exchange 2007 Client Access Role Services

This template assesses the status of Windows services related to Microsoft Exchange 2007.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Exchange Active Directory Topology

Net Service Name: MSExchangeADTopology

Exchange File Distribution Service

Net Service Name: MSExchangeFDS

Exchange IMAP4

Net Service Name: MSExchangeImap4

Exchange Monitoring

Net Service Name: MSExchangeMonitoring

Exchange POP3

Net Service Name: MSExchangePop3

Exchange Service Host

Net Service Name: MSExchangeServiceHost

Exchange 2007 Client Access Role WMI Counters

This template assesses the status of Windows services related to Microsoft Exchange 2007.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

ActiveSync Average Request Time

The average time in seconds it takes to complete a request

ActiveSync Ping Commands Pending

The number of ping commands pending in the queue.

ActiveSync Requests/sec

The number of ASP.NET HTTP requests received per second is an indicator of current user load.

ActiveSync Sync Commands/sec

The number of sync commands processed per second is an indicator of current user load.

Autodiscover Requests/sec

The number of autodiscover requests processed per second is an indicator of current user load.

Availability requests/sec

The number of free/busy availability requests processed per second.

Average Time to Process a Free Busy Request

The average time in seconds it takes to process a free/busy request. This value should always be less than 5.

Disk Reads/sec

The number of disk reads per second can indicate paging issues because data was read from disk instead of memory. This value should always be less than 50.

Disk Writes/sec

The number of disk writes per second can indicate paging issues because data was written to disk instead of memory. This value should always be less than 50.

MSExchangeWS Requests/sec

The number of requests processed per second indicates current user load.

OAB Download Task Queued

This value is 1 if a task is queued for execution. Should always be 0. Higher values indicate OAB data could not be copied from Mailbox servers.

OAB Download Tasks Completed

The number of OAB download tasks completed since the File Distribution service was started or restarted. By default, this service is started every 8 hours. This values should be 3 or less per day with the default schedule.

OWA Average Response Time

The time in milliseconds between the start and end of an OEH or ASPX request. This value should always be less than 100ms.

OWA Average Search Time

The average time in milliseconds it takes to complete an Outlook Web Access search. This value should always be less than 100ms.

OWA Current Unique Users

The number of unique users logged on Outlook Web Access indicates user load.

OWA Requests/sec

The number of requests per second processed by Outlook Web Access indicates user load.

Exchange 2007 Common WMI Counters

This template assesses the status of Windows services related to Microsoft Exchange 2007.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

.NET CLR Exceptions thrown / sec

The number of managed exceptions thrown per second indicates possible performance degradation.

.NET CLR Memory bytes in all heaps

The memory in bytes currently allocated on all the garbage collection heaps.

.NET CLR Memory percent time in GC

The percentage of time spent in garbage collection as measured from the end of the last garbage collection.

LDAP Read Time

The time in milliseconds it takes to service a Lightweight Directory Access Protocol (LDAP) read request.

LDAP Search Time

The time in milliseconds it takes to service an LDAP search request. This value should always be less than 100ms.

LDAP Searches Timed out / minute

The number of LDAP searches in the past minute that returned LDAP_TIMEOUT.

LDAP Searches/sec

The number of LDAP search requests received per second.

Long running LDAP operations/min

The number of LDAP operations per minute that have taken longer than 15 seconds to complete. A value higher than 100 can indicate network congestion or performance problems on your domain controller.

Exchange 2007 Edge Transport Role Services

This template assesses the status of Windows services related to Microsoft Exchange 2007.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Exchange ADAM

Net Service Name: ADAM_MSExchange

Exchange Anti-spam Update

Net Service Name: MSExchangeAntispamUpdate

Exchange Credential Service

Net Service Name: EdgeCredentialSvc

Exchange Monitoring

Net Service Name: MSExchangeMonitoring

Exchange Transport

Net Service Name: MSExchangeTransport

Exchange Transport Log Search

Net Service Name: MSExchangeTransportLogSearch

Exchange 2007 Hub Transport Role Services

This template assesses the status of Windows services related to Microsoft Exchange 2007.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Exchange Active Directory Topology

Net Service Name: MSExchangeADTopology

Exchange Anti-Spam Update

Net Service Name: MSExchangeAntispamUpdate

Exchange EdgeSync

Net Service Name: MSExchangeEdgeSync

Exchange Monitoring

Net Service Name: MSExchangeMonitoring

Exchange Transport

Net Service Name: MSExchangeTransport

Exchange Transport Log Search

Net Service Name: MSExchangeTransportLogSearch

Exchange 2007 Hub Transport Role WMI Counters

This template assesses the status of Windows services related to Microsoft Exchange 2007.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

The Exchange 2007 Hub Transport Role WMI Counters are described by in *Monitoring Hub Transport Services*, "Microsoft TechNet." http://technet.microsoft.com/en-us/library/bb201704.aspx

Average Agent Processing Time (sec)

Dumpster Deletes /sec

Dumpster Inserts /sec

Dumpster Item Count

Dumpster Size

SMTP Messages Received /sec

SMTP Messages Received Average bytes / message

SMTP Messages Sent /sec

Store Driver Inbound: Local Delivery Calls/sec

Store Driver Inbound: Message Delivery Attempts/sec

Store Driver Inbound: Recipients Delivered/sec

Store Driver Outbound: Submitted Mail items /sec

Total Agent invocations

Transport Mail Database: I/O Database Reads/sec

Transport Mail Database: I/O Database Writes/sec

Transport Mail Database: I/O Log Reads/sec

Transport Mail Database: I/O Log Writers/sec

Transport Mail Database: Log Generation Checkpoint Depth

Transport Mail Database:Log Record stalls/sec

Transport Mail Database:Log Threads Waiting

Transport Mail Database:Version Buckets Allocated

Transport Queues: Active Mailbox Delivery Queue Length

Transport Queues: Active Non-SMTP Delivery Queue Length

Transport Queues: Active Remote Delivery Queue Length

Transport Queues: Aggregate Delivery Queue Length (All Queues)

Exchange 2007 Mailbox Role Services

This template assesses the status of Windows services related to Microsoft Exchange 2007.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Exchange Active Directory Topology

Net Service Name: MSExchangeADTopology

Exchange Information Store

Net Service Name: MSExchangeIS

Exchange Mail Submission Service

Net Service Name: MSExchangeMailSubmission

Exchange Mailbox Assistance

Net Service Name: MSExchangeMailBoxAssistants

Exchange Monitoring

Net Service Name: MSExchangeMonitoring

Exchange Replication Service

Net Service Name: MSExchangeRepl

Exchange Search Indexer

Net Service Name: MSExchangeSearch

Exchange Service Host

Net Service Name:MSExchangeServiceHost

Exchange System Attendant

Net Service Name: MSExchangeSA

Exchange Transport Log Search

Net Service Name: MSExchangeTransportLogSearch

Microsoft Search (Exchange Server)

Net Service Name: MSFTESQL-Exchange

Exchange 2007 Mailbox Role WMI Counters

This template assesses the status of Windows services related to Microsoft Exchange 2007.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

The Exchange 2007 Mailbox Role WMI Counters are described by in *Monitoring Mailbox Servers*, "Microsoft TechNet." http://technet.microsoft.com/en-us/library/bb201689.aspx

Assistants: Average Event Processing Time (sec)

Assistants: Events in queue

Assistants: Events polled/sec

Assistants: Mailboxes Processed/sec

Calendar Attendant: Average Calendar Attendant Processing Time

Calendar Attendant: Requests Failed

Client Directory Access: LDAP Reads/sec

Client Directory Access: LDAP Searches/sec

Information Store Client: RPCs Failed Server Too Busy

Information Store Client: RPCs Failed Server Too Busy/sec

Information Store Mailbox: Categorization Count

Information Store Mailbox: Messages Queued for Submission

Information Store Search Task Rate

Information Store Slow Findrow Rate

Information Store Public: Messages Queued for Submission

Information Store: Database Cache Hit %

Information Store: Database Cache Size (MB)

Information Store: Database Page Fault Stalls/sec

Information Store: I/O Database Reads Average Latency

Information Store: I/O Database Writes Average Latency

Information Store: Log bytes Write/sec

Information Store: Log Record Stalls/sec

Information Store: Log Threads Waiting

Information Store: RPC Average Latency

Information Store: RPC Averaged Latency

Information Store: RPC Client Backoff/sec

Information Store: RPC Number of Slow Packets

Information Store: RPC Operations

Information Store: RPC Operations/sec

Information Store: RPC Requests

Information Store: Version Buckets Allocated

JET Log Records/sec

JET Pages Read/sec

Log Generation Checkpoint Depth

Mail Submission/Failed submissions/sec

Mail Submission: Hub servers in retry

Mail Submission: Successful submissions/sec

Mail Submission: Temporary Submission Failures/sec

Messages Delivered/sec

Messages Sent/sec

Slow QP Threads

Slow Search Threads

Store: RPC latency average (msec)\

Store: RPC requests failed %

Store: RPC requests outstanding

Store: RPC requests sent/sec

Store: RPC slow requests %

Store: RPC slow requests latency average (msec)

Exchange 2007 Unified Messaging Role Services

This template assesses the status of Windows services related to Microsoft Exchange 2007.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Exchange Active Directory Topology

Exchange File Distribution Service

Exchange Monitoring

Exchange Speech Engine

Exchange Unified Messaging

Exchange 2007 WMI Counters

This template assesses the overall performance of a Microsoft Exchange 2007 server. The critical threshold values for the performance counters are values recommended by Microsoft.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Unavailable Component Monitors

Some of the Windows Management Instrumentation (WMI) performance counters monitored in this template are only available to Microsoft Exchange 2007 servers that fill Hub Transport Server and/or Mailbox Server roles. Assigning this template to a server that does not fill one or both of these roles results in an Unknown status for the unavailable WMI component monitors.

Monitored Components

The critical thresholds for these monitors are derived from guidance provided by "Monitoring Without System Center Operations Manager," Microsoft Technet. http://technet.microsoft.com/en-us/library/bb201720(EXCHG.80).aspx

Role: Hub Transport Server

Aggregate Delivery Queue Length (AllQueues)

Statistic Critical Threshold: 5000

Active Remote Delivery Queue Length

Statistic Critical Threshold: 250

Active Mailbox Delivery Queue Length

Statistic Critical Threshold: 250

Submission Queue Length

Statistic Critical Threshold: 100

Active NonSmtp Delivery Queue Length

Statistic Critical Threshold: 250

Retry Mailbox Delivery Queue Length

Statistic Critical Threshold: 100

Retry NonSmtp Delivery Queue Length

Statistic Critical Threshold: 100

Retry Remote Delivery Queue Length

Statistic Critical Threshold: 100

Unreachable Queue Length

Statistic Critical Threshold: 100

Largest Delivery Queue Length

Statistic Critical Threshold: 200

Poison Queue Length

Statistic Critical Threshold: 0

Role: Mailbox Server

RPCAveragedLatency

Statistic Critical Threshold: 25

RPCNumofSlowPackets

Statistic Critical Threshold: 3

RPCRequests

Statistic Critical Threshold: 70

MessagesQueuedForSubmission

Statistic Critical Threshold: 50

Public: MessagesQueuedForSubmission

Statistic Critical Threshold: 20

ReplicationReceiveQueueSize

Statistic Critical Threshold: 100

SearchTaskRate

Statistic Critical Threshold: 10

SlowFindRowRate

Statistic Critical Threshold: 10

Averagedocumentindexingtime

Statistic Critical Threshold: 30

Exchange Server (via SNMP)

This template assesses the status of Windows services related to Microsoft Exchange Server.

Prerequisites: SNMP access to target server.

Credentials: None.

Monitored Components

MS Exchange Event – SNMP

MS Exchange IMAP4 – SNMP

MS Exchange Information Store – SNMP

MS Exchange Management – SNMP

MS Exchange MTA Stack – SNMP

MS Exchange Routing engine – SNMP

MS Exchange Site Replication – SNMP

MS Exchange System Attendant – SNMP

MS SMTP Monitor

MS POP3 Monitor

MS IMAP4 Monitor

Exchange Server 2000 and 2003

This template assesses the status and the overall performance of Microsoft Exchange Server 2000 and 2003. The critical threshold values for the performance counters are values recommended by Microsoft.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Processor Queue Length

Number of Processes

Mailbox Send Queue

Mailbox Receive queue

Public Send Queue

Public Receive Queue

SMTP Local Queue

SMTP Remote Queue

SMTP Categorizer Queue

Average RPC Latency

Address List Queue Length

Percent Free Space

Disk Read Bytes per Second

Disk Write Bytes per Second

MS Exchange Event

MS Exchange IMAP4

MS Exchange Information Store

MS Exchange Management

MS Exchange MTA Stacks

MS Exchange POP3

MS Exchange Routing Engine

MS Exchange Site Replication

MS Exchange System Attendant

MS SMTP Monitor

MS POP3 Monitor

MS IMAP4 Monitor

File Age Monitor

This template determines when a file was last modified. The statistic is the number of elapsed hours since the file modification date.

Prerequisites: None.

Credentials: Windows credential with read access to the network share and file.

Monitored Components

File Age Monitor

File Change Monitor

This template tests if the contents of a file has changed. The component monitor performs an MD5 checksum comparison on the file to verify it matches a previously known state. The statistic is the number of hours since the file was modified.

Prerequisites: None.

Credentials: Windows credential with read access to the network share and file.

Monitored Components

File Change Monitor

File Count Script

This template monitors the number of files in a directory. Specify the path as the script argument. The statistic is the number of files in the directory.

Prerequisites: None.

Credentials: Windows credential valid on both Orion APM and target server.

Monitored Components

File Count

File Existence Monitor

This template tests if a file exists at the given file path.

Requirement: None.

Credentials: Windows credential with read access to the network share.

Monitored Components

File Existence Monitor

File Size Monitor

This template measures the size of a file at the given file path. The statistic is the file size in bytes.

Prerequisites: None.

Credentials: Windows credential with read access to the network share.

Monitored Components

File Size Monitor

FileModified (vbscript)

This template tests if a file has been modified. This template has been superseded by the File Change Monitor template.

Prerequisites: None.

Credentials: Windows credential valid on both Orion APM and target server.

Monitored Components

FileModified

Finger Port Monitor

This template tests the ability of the Finger service to accept incoming sessions on port 79.

Prerequisites: None.

Credentials: None.

Monitored Components

Finger Port Monitor

FTP User Experience

This template tests the ability of an FTP server to accept incoming sessions, process user logins, and then transmit the requested file. The component monitor performs an MD5 checksum comparison on the downloaded file to verify content integrity

Prerequisites: None.

Credentials: FTP account with read permissions on target server.

Monitored Components

FTP User Experience Monitor

Generic DNS

This template tests a DNS server's ability to respond to a record query and measures its response time. The component monitor passes if it receives a valid DNS response (positive or negative) within the response time threshold.

Prerequisites: None.

Credentials: None.

Monitored Components

DNS Monitor – UDP

Generic Mail Server

This template tests the ability of a mail server to accept incoming SMTP, NNTP, POP3, and IMAP4 connections and respond with the correct codes.

Prerequisites: None.

Credentials: None.

Monitored Components

SMTP Monitor

NNTP Monitor

POP3 Monitor

IMPA4 Monitor

Generic Web Server

This template tests the ability of a web server to respond to HTTP and HTTPS requests.

Prerequisites: None.

Credentials: None.

Monitored Components

HTTP Monitor

HTTPS Monitor

Gopher Port Monitor

This template tests the ability of a Gopher server to accept incoming sessions on port 70.

Prerequisites: None.

Credentials: None.

Monitored Components

Gopher Port Monitor

HTTP

This template tests the ability of a web server to respond to HTTP requests.

Prerequisites: None.

Credentials: None.

Monitored Components

HTTP Monitor

HTTP Form Login

This template tests the ability of a web server to serve web pages secured behind a forms-based login page.

Prerequisites: None.

Credentials: A valid user name and password for the forms-based login page.

Monitored Components

Form Login Monitor

IMAP4 Round Trip Email

This template simulates an email round trip to test the ability of your SMTP server to receive and distribute email, and the ability of your users to retrieve messages from IMAP4-enabled email clients.

Prerequisites: None.

Credentials: Windows credential valid on both the Orion APM server and the Microsoft Exchange server.

Monitored Components

IMAP 4 User Experience Monitor

Internet Information Services

This template assesses the status and overall performance of a Microsoft Internet Information Services server.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

ASP.NET State Service

Bytes Received/sec Counter

Bytes Sent/sec Counter

Bytes Total/sec Counter

Connection Attempts/sec Counter

Current Connections Counter

Generic HTTP Monitor

Get Requests/sec Counter

HTTP Port Monitor

HTTP SSL Service

IIS Admin Service

Measured Async I/O Bandwidth Usage Counter

Network News Transfer Protocol Service

Simple Mail Transfer Protocol Service

Total Allowed Async I/O Requests Counter

URI Cache Flushes Counter

URI Cache Hits Counter

URI Cache Hits Percent Counter

URI Cache Misses Counter

WinHTTP Web Proxy Auto-Discover Service

World Wide Web Publishing Service

IRC Port Monitor

This template tests the ability of an IRC server to accept incoming sessions on port 6667.

Prerequisites: None.

Credentials: None.

Monitored Components

IRC Port Monitor

LDAP Connection Monitor

This template tests the ability of an LDAP server to respond to an LDAP query. The statistic returned is the LDAP version.

Prerequisites: None.

Credentials: Windows Administrator credential valid on both Orion APM and target server.

Monitored Components

LDAP Connection Monitor

Linux/Unix Operating System

This template monitors memory and drive space usage on a Linux/Unix server.

Prerequisites: SNMP tools installed on target server, specifically snmpget and snmpwalk.

Credentials: SSH account on Linux/Unix server.

Monitored Components

Available Memory

Drive Space

Lotus Domino Server

This template assess the overall health of a Lotus Domino server y monitoring its key performance indicators.

Prerequisites: SNMP access to target server.

Credentials: None.

Monitored Components

This template uses SNMP component monitors to monitor the following performance indicators:

Available Resources (%)

OID: 1.3.6.1.4.1.334.72.1.1.6.3.19.0

Open User Sessions

OID: 1.3.6.1.4.1.334.72.1.1.6.3.6.0

Peak Open User Sessions

OID: 1.3.6.1.4.1.334.72.1.1.6.3.11.0

Dropped Session Count

OID: 1.3.6.1.4.1.334.72.1.1.6.3.1.0

DB Cache Rejection Count

OID: 1.3.6.1.4.1.334.72.1.1.10.21.0

LDAP Tasks Running

OID: 1.3.6.1.4.1.334.72.1.1.21.10.0

Peak Transactions per Minute

OID: 1.3.6.1.4.1.334.72.1.1.6.3.3.0

Max Mail Delivery time (seconds)

OID: 1.3.6.1.4.1.334.72.1.1.4.12.0

Pending Mail Messages

OID: 1.3.6.1.4.1.334.72.1.1.4.31.0

MAPI Round Trip Email

This template simulates an email round trip to test the ability of your SMTP server to receive and distribute email, and the ability of your users to retrieve messages from MAPI-enabled email clients.

Prerequisites: MAPI access to a Microsoft Exchange server. MAPI Client and CDO Objects installed on Orion APM server.

Credentials: Windows credential valid on both the Orion APM server and the Microsoft Exchange server.

Monitored Components

MAPI User Experience Monitor

MySQL

This template assesses the status and performance of a MySQL database server by retrieving the server status variables from the built-in INFORMATION_SCHEME_GLOBAL_STATUS tables.

Prerequisites: MySQL 5.1.12 or later.

Credentials: Database user name and password.

Monitored Components

Total Memory Used

Bytes Received

Bytes Sent

Created Temporary Disk Tables

Created Temporary Files

Created Temporary Tables

Opened Table Definitions

Opened Tables

Opened Files

Statements Executed

Key Reads

Key Writes

Table Locks Immediate

Table Locks Waited

Threads Cached

Threads Connected

Threads Created

Threads Running

Up Time

Oracle Database

This template assesses the status and performance of an Oracle database by retrieving performance data from the built-in Oracle statistics views.

Prerequisites: Oracle client installed on Orion APM server, available from the SolarWinds customer portal under Additional Downloads.

Credentials: Oracle user name and password.

Monitored Components

Available continuous free space

Available free memory

Available free space

Buffer cache hit ratio

Dictionary cache hit ratio

Library cache hit ratio

Number of connected users to the database through SQL Net

Sort ratio, disk vs. memory

Orion Server

This template assesses the status of Windows services related to SolarWinds Orion servers.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

SW Alerting Engine

SW Network Performance Monitor

SW Orion Job Engine

SW Orion Job Scheduler

SW Orion Module Engine

SW Syslog Service

SW Web Console – UE

POP3 Round Trip Email

This template simulates an email round trip to test the ability of your SMTP server to receive and distribute email, and the ability of your users to retrieve messages from POP3-enabled email clients.

Prerequisites An SMTP server and a POP3 server.

Credentials: POP3 mailbox account. If the SMTP server requires authentication, the POP3 mailbox and the SMTP server must have identical user names and passwords.

Monitored Components

POP3 User Experience Monitor

Run 3rd Party Application

This template demonstrates using a Windows script to run an executable program. The statistic is the return value of the executable program. The Windows Script component monitor in this template is preset to run the Windows notepad.exe executable program on the Orion APM server.

Prerequisites: None.

Credentials: Windows Administrator credential valid on both Orion APM and target server.

Usage

To run an executable program locally on the Orion APM server:

Type the program name in the **Script Arguments** field.

To run an executable program on a remote server:

Specify all of the following arguments in the **Script Arguments** field:

`hostname workingdirectory executablefile username password`

hostname

The hostname or IP address of the remote server where the program resides.

workingdirectory

The local path or Universal Naming Convention path to a folder on the remote server that the program can use as its working directory.

executablefile

The local path or UNC path to the executable program.

username

The user name of a Windows administrator account on the remote server.

password

The password of the Windows administrator account.

Example of Running a Program Locally on the Orion APM Server

This argument runs the executable program notepad.exe on the Orion APM Server.

```
notepad.exe
```

Example of Running a Program on a Remote Server

These arguments run the executable program `C:\temp\testantivirus.exe` on the remote host, and use the `C:\temp` folder as the working directory. The paths are in UNC syntax.

```
remotehost \\remotehost\c$\temp\testantivirus.exe
\\remotehost\c$\temp\ username password
```

Example of Using Credentials Variables to Run a Program on a Remote Server

These arguments run the same executable program as the previous example, but hide the Windows administrator credentials from plain sight by substituting `${USER}` and `${PASSWORD}` variables. If you use these variables, you must set the **Credential** field of this component to a credential with administrator rights to the remote server.

```
remotehost \\remotehost\c$\temp\testantivirus.exe
\\remotehost\c$\temp\ ${USER} ${PASSWORD}
```

RWHOIS Port Monitor

This template tests the ability of an RWHOIS server to accept incoming sessions on port 4321.

Prerequisites: None.

Credentials: None.

Monitored Components

RWHOIS Port Monitor

SharePoint Server (MOSS) 2007

This template assess the overall health and performance of Microsoft Office SharePoint Server 2007.

Prerequisites: WMI access to SharePoint server.

Credentials: Windows Administrator on SharePoint server.

Monitored Components

ASP.NET: Requests/sec

ASP.NET: Worker Processes Restarts

Document Conversions Launcher

Document Conversions Load Balancer

Search Gatherer: Crawls in progress

Search Gatherer: Document Add Rate

Search Gatherer: Document Entries

Search Gatherer: Documents Filtered Rate

Search Gatherer: Error Rate

Search Gatherer: Filtering Threads

Search Gatherer: Incremental Crawls

Search Gatherer: Processed Documents Rate

Search Gatherer: Retries

Search Gatherer: Threads Accessing Network

Search Gatherer: Waiting Documents

Search Gatherer: Queries

SharePoint Server Search

Single Sign-on

SharePoint Services (WSS) 3.0

This template assess the overall health and performance of Windows SharePoint Services 3.0.

Prerequisites: WMI access to SharePoint server.

Credentials: Windows Administrator on SharePoint server.

Monitored Components

ASP.NET Worker Process Restarts

Internet Information Services

ISAPI Connection Count

ISAPI Request / sec

SharePoint Services Search

SharePoint Services Timer

SharePoint Services Tracing

SNPP Port Monitor

This template tests the ability of an SNPP server to accept incoming sessions on port 444.

Prerequisites: None.

Credentials: None.

Monitored Components

SNPP Port monitor

SQL Server (via SNMP)

This template assesses the status of Windows services related to Microsoft SQL Server servers.

Prerequisites: SNMP access to target server.

Credentials: None.

Monitored Components

SQL Server Browser - SNMP

SQL Server Port

SQL Server Process – SNMP

SQL Server 2005 Database

This template assesses the status and performance of a Microsoft SQL Server 2005 database.

Prerequisites: WMI access to the target server.

Credentials: Windows Administrator on target server.

Note: Named instances of SQL Server may have custom class names that do not match the built-in templates. You must manually change the class name in any WMI Monitor monitoring a named SQL Server instance. For example, if the named instance is "NAMED", you must change Win32_PerfFormattedData_MSSQLSERVER_SQLServerBufferManager to Win32_PerfFormattedData_MSSQLNAMED_SQLNAMEDServerBufferManager.

Monitored Components

Buffer cache-hit ratio

Full scans

Latch waits

SQL Page Reads per Second

SQL Page Writes per Second

SQL Server Browser - WMI

SQL Server Port

SQL Server Process – WMI

SQL Server 2008 Database

This template assesses the status and performance of a Microsoft SQL Server 2008 database.

Prerequisites: WMI access to the target server.

Credentials: Windows Administrator on target server.

Note: Named instances of SQL Server may have custom class names that do not match the built-in templates. You must manually change the class name in any WMI Monitor monitoring a named SQL Server instance. For example, if the named instance is "NAMED", you must change Win32_PerfFormattedData_MSSQLSERVER_SQLServerBufferManager to Win32_PerfFormattedData_MSSQLNAMED_SQLNAMEDServerBufferManager.

Monitored Components

Buffer cache-hit ratio

Full scans

Latch waits

SQL Page Reads per Second

SQL Page Writes per Second

SQL Server Browser - WMI

SQL Server Port

SQL Server Process – WMI

SQL Server Query

This template assesses the performance of a Microsoft SQL Server database by retrieving performance data from the built-in master..sysperfinfo pseudo-table.

Prerequisites: None.

Credentials: SQL Server user name and password.

Monitored Components

Buffer cache hit ratio

Lazy writes/sec

Lock Wait Time (ms)

Local Waits/sec

Logins/sec

Page Life Expectancy

Page reads/sec

Page writes/sec

Target Server Memory %

Total Server Memory (KB)

User Connections

thwack.com - User Experience Monitor Example

This template demonstrates using the HTTP Monitor to monitor the operational status of the thwack.com search function.

Prerequisites: None.

Credentials: None.

Monitored Components

Thwack.com – UE

Tomcat Server Template

This template assess the performance of an Apache Tomcat Server by retrieving information from the Tomcat Web Application Manager.

Prerequisites: Tomcat Server configured with Tomcat Web Application Manager.

Credentials: Tomcat Server Manager

Monitored Components

Tomcat Free Memory

Tomcat Max Memory

Tomcat Total Bytes Received

Tomcat Total Bytes Sent

Tomcat Total Errors Count

Tomcat Total Memory

Tomcat Total Processing Time

Tomcat Total Request Count

Web Link

This template validates the hyperlinks on the web page served by the target web server. If any hyperlinks are invalid or unreachable, the test fails. The statistic is the number of invalid or unreachable hyperlinks.

Prerequisites: None.

Credentials: None.

Monitored Components

Web Link Monitor

Windows DNS Server (via SNMP)

This template assesses the status of Windows services related to Windows DNS servers.

Prerequisites: SNMP access to target server.

Credentials: None.

Monitored Components

DNS Monitor - TCP

DNS Server – SNMP

Windows Event Log Count

This template contains a Windows Script that searches the Windows Event log on a computer for specific events that may have occurred during a specified time frame, and reports the number of occurrences as an Orion APM statistic.

Prerequisites: None.

Credentials: Windows Administrator credential valid on both Orion APM and target server.

Monitored Components

Windows Event Log Script

Script Arguments

[`-computer` *`computerName`*] [`-area` *`eventArea`*] [`-type` *`eventType`*]
[`-id` *`eventID`*] [`-source` *`eventSource`*] [`-exclusions` *`findExclusionText`*]
[`-match` *`findMatchText`*] [`-timespan` *`timeSpanMins`*]
[`-failmode` *`failmodeType`*]

computerName

Name of the computer whose event logs you want to read. If not specified, the default value is localhost.

eventArea

Name of the Windows NT Event Log File: Application, Security, or System.

eventType

Name of the event type: Error, Warning, Information, Success, or Failure.

eventID

Identifier of the event, specific to the source that generated the event log entry. Used together with the eventSource to uniquely identify a Windows NT event type. The default value is 0.

eventSource

Name of the source (application, service, driver, or subsystem) that generated the entry. Used together with eventID to uniquely identify a Windows NT event type.

findExclusionsText

A string of text which, if located by the script, prohibits that event from being counted towards the APM statistic.

findMatchText

A string of text which, if located by the script, counts towards the APM statistic.

timeSpanMins

The age, in minutes, of the oldest event that the script attempts to locate.

Example

These arguments return the number of events in the localhost Application event log that have an ID of 1 and that have occurred within the last 5 minutes. If any events are found, the component is put into a down state.

```
-computer localhost -area Application -id 1 -timespan 5
```

Windows FTP Server (via WMI)

This template monitors the Windows FTP Publishing Service and tests the ability of the F*TP* server to accept incoming sessions on port 21.

Prerequisites: None.

Credentials: Windows Administrator on target server.

Monitored Components

FTP Monitor

FTP Publishing Service

Windows Print Services

This template assess the status of Windows Print services.

Prerequisites: WMI access to print server.

Credentials: Windows Administrator on print server.

Monitored Components

Job Errors

Jobs

Jobs Spooling

Not Ready Errors

Out of Paper Errors

Print Server Spooler Service

Print Server Thread Count

Total Jobs Printed

Total Pages Printed

Windows Server 2003-2008

This template assesses the status and overall performance of a Microsoft Windows Server 2003 or Windows Server 2008 operating system.

Prerequisites: WMI access to target server.

Credentials: Windows Administrator on target server.

Monitored Components

Disk Queue Length

Distributed Transaction Coordinator

Network Connections

Page File Usage

Protected Storage

Remote Registry

Total Available Memory (MB)

Virtual Memory

Index

T

U

W