This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
## Contents

- **About vFabric AppInsight User's Reference** 5
- **1 General Concepts in vFabric AppInsight** 7
- **2 Best Practices in vFabric AppInsight** 9
- **3 Monitoring Data Using Complementary VMware Products** 11
  - Register Adapters for Integrating Complementary VMware Products 11
  - Integrating vCenter Chargeback to Monitor Application Cost 12
  - Integrating vFabric Hyperic to Monitor Application Performance 13
  - Integrating vFabric Application Director with AppInsight to Monitor Application Director Deployments 13
- **4 Integrating vCenter Orchestrator to Manage Remedial Actions** 19
  - Add Orchestrator Workflows 19
  - Delete an Orchestrator Workflow 20
- **5 Create Applications** 21
- **6 Adding Components** 23
  - Add a Mapped Component to an Application 23
  - Add Multiple Components to an Application 24
  - Add Components Using Hints 25
  - Add an Unmapped Component to an Application 26
  - Altering the Monitoring Method of a Component 26
- **7 Add Transactions to the Topology of an Application** 29
  - Manually Add a Transaction Element 30
- **8 Adding Tiers to the Topology** 31
- **9 Configuring KPI Thresholds** 33
  - Manually Configure KPI Metrics Thresholds 33
  - Enable AppInsight Dynamic Threshold Determination 34
- **10 Monitoring Application Performance** 37
  - vFabric AppInsight Dashboard 37
  - Application Module 38
  - Administration Module 43
11 Delete an Application  49

12 Delete a Tier  51

13 Managing AppInsight Users  53
   Add a New User  54
   Change a Password  54
   Unlock a User Account  54
   Delete a User Account  55

Index  57
About vFabric AppInsight User's Reference

vFabric AppInsight is a performance management product for application owners who deploy applications on hybrid clouds and in dynamic virtual environments. AppInsight monitors the availability, performance, and cost of those applications.

vFabric AppInsight provides you with an at-a-glance health state for your application. With AppInsight, you can focus on problematic areas in all levels of code, middleware, and Infrastructure. You can then apply one or more remedial actions.

Monitoring can include:

- Network-based monitoring
- Code-level monitoring
- Application middleware overview
- Application infrastructure overview
- Application cost monitoring

Intended Audience

This information is intended for anyone who wants to use vFabric AppInsight to monitor service levels such as availability, performance, and cost of applications.
vFabric AppInsight monitors the health of applications by collecting and analyzing metrics to generate key performance indicators (KPIs). Understanding AppInsight concepts and terms helps you to understand and use AppInsight.

vFabric AppInsight Overview

After installing AppInsight and deploying network probes and various code agents, you create an application and add components to logical tiers such as the Web tier or the Application tier.

Metrics are gathered by the network probes and code agents and key performance indicators are calculated. You can define alerts that generate notifications when behavior breaches specified thresholds. Optionally, you can also specify remedial actions in this situation.

AppInsight includes the following key objects.

**Application**

An application is a logical unit of Web software. For example, in a Web business program, you might define the processes related to the human resources department as one application and the processes related to accounting as another application.

**Tier**

A logical group of components.

**Component**

When you install AppInsight network probes, and optionally VMware code agents and complementary VMware products, they detect the computing traffic and suggest potential application components.

You must add at least one component to an application so that AppInsight can determine the entire application structure, study transactions, and show monitoring data.

Web Application components are Web servers for which the network traffic is monitored.

Code agent components are application server components that installed code agents detect. Each component represents an individual WAR file. For example, if you have three applications on a single server, the topology structure shows one application server and three application code agent components. If a code agent is not installed, the topology structure shows only the application server and a Web application component.

**Transaction**

A cross-tier action between transaction elements. For example, a login transaction.

**Transaction Element**

The smallest building block within a component.
Storage of Monitored Data

Over time, metrics become less relevant to the current state of an application and are discarded. The length of time for which data is stored in the AppInsight database depends on the time range over which it was acquired.

<table>
<thead>
<tr>
<th>Time Period During Which Metric was Gathered</th>
<th>Storage Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 seconds</td>
<td>30 minutes</td>
</tr>
<tr>
<td>2 minutes</td>
<td>7 days</td>
</tr>
<tr>
<td>10 minutes</td>
<td>1 month</td>
</tr>
<tr>
<td>1 hour</td>
<td>6 months</td>
</tr>
<tr>
<td>1 day</td>
<td>3 years</td>
</tr>
</tbody>
</table>

Viewing vFabric AppInsight Details

AppInsight functionality is organized into three modules. You select the required module from the menu bar.

Dashboard
The dashboard provides a high level overview of your applications and their health status. When you click on data in the dashboard, the Application module opens so that you can see more detailed information for the application to which the data in the dashboard applies.

Application
The Application module displays monitoring data for the selected application. You can manage the topology of the application, manage KPI thresholds, view notification logs, samples, and so on.

Administration
Use the Administration module to register adapters, deploy probes and define applications. You can also configure alerts, access technical support information, and manage users.

AppInsight includes several functions so that you can quickly see more details about items of interest.

- You can use the Time Picker to select the period for which you want to see data. The Time Picker pane also shows a graph for the Hit Rate metric over the period.
  
  Note that the server displays data for the closest resolution to the selected time.

- You can use a click and drag action in any graph to select a specific time range. Use the "handles" on either start of the selection to adjust the selected range. Click Zoom in the selected area to focus the graph on that area. The time displayed on the Time Picker matches that of the selected range.

- When you point to an application object, a pop-up window provides additional high-level detail.

- Many application objects are clickable links. When you select an application object, a new page or window opens that presents details of that object. Depending on the application object that you select, you can navigate through several layers of detail.
Best Practices in vFabric AppInsight

Use best practices to optimize the performance of vFabric AppInsight.

Virtual Machine Configuration

Consider the following points, related to configuring a virtual machine.

- In the event that the host of a virtual machine is stopped and restarted, it is important that the virtual machine is restarted as soon as possible, to minimize data loss. You set auto restart parameters for the machine in the vSphere Client.

- For accurate data monitoring, use VMware Tools in the vSphere Client to synchronize the time of the guest operating system on the virtual machine with the time of the host.

Adding Components

To limit skewed metrics, do not add network-monitored application components and code-monitored application components in the same tier. Such practice might affect latency calculations because network monitoring also includes the network overhead latency.

Monitoring Options

Consider the following points, related to monitoring applications.

- If possible, implement code monitoring through code agents to monitor application components. If you cannot use code monitoring, use network monitoring.

- You cannot monitor a virtual machine using both a network probe and the code agent. However, you can change the monitoring method after installation. See “Altering the Monitoring Method of a Component,” on page 26.
You can integrate complementary VMware products into AppInsight to increase the volume of information that is monitored, to define workflow actions, and to focus on specific areas of interest.

You install complementary VMware products as their respective documentation describes. You then must register an AppInsight adapter for the product, so that monitoring can occur.

- **vFabric Hyperic** Monitors the virtual machines and the services running on those virtual machines.
- **vFabric Application Director** Accelerates and automates the configuration and deployment of multitier applications.
- **vCenter Chargeback** Monitors the monetary cost of an application.
- **vCenter Orchestrator** Enables workflows, such as starting a virtual machine or sending a notification in the event of an alert, to be created to automate action performance in AppInsight.

This chapter includes the following topics:

- “Register Adapters for Integrating Complementary VMware Products,” on page 11
- “Integrating vCenter Chargeback to Monitor Application Cost,” on page 12
- “Integrating vFabric Hyperic to Monitor Application Performance,” on page 13
- “Integrating vFabric Application Director with AppInsight to Monitor Application Director Deployments,” on page 13

### Register Adapters for Integrating Complementary VMware Products

You can integrate complementary VMware products with AppInsight to enhance its monitoring capabilities. As part of the integration process, you must register adapters for each product.

**Prerequisites**

- Verify that you have registered the vCenter Server adapter. This is required for all complementary VMware products. See the *VMware vFabric AppInsight Installation Guide*.

- If you are adding vCenter Chargeback, the cost model that you want to apply in AppInsight must be set in vCenter Chargeback.

- Verify that you have appropriate login details and server machine details for the adapter that you are adding.
**Product** | **Minimum Required User Permissions**  
---|---  
vCenter Chargeback | Report Generator, or an equivalent custom role  
vCenter Orchestrator |  
  - Execute rights for running workflows.  
  - Read rights on the Root object to search for vCenter objects through the Soap API  
vFabric Hyperic | Super User

**Procedure**

1. In the **Administration** module, click the **Adapters** tab.
2. Click **Add** and select the type of adapter to configure.
3. Type a name for your adapter in the **Adapter Name** text box.
   - The additional text boxes that appear depend on the adapter type that you select.
   - When default values are specified, the values appear in the text boxes. The values are editable, but VMware recommends that you do not change them unnecessarily.
4. Type appropriate information in all the other text boxes.
   - Enter user name and password credentials that already exist for the agent or complementary VMware product for which you are configuring the adapter.
   - The user that you specify must have sufficient permissions to read and write to the complementary product. Minimum permissions for each product are provided in its product-specific integration topic.
5. Click **Save** and when prompted, select the check box to accept the certificate.
6. Click **Save**.
   - The adapter appears in the list at the top of the **Adapters** tab.

AppInsight starts monitoring using the installed product, or in the case of Orchestrator, is available to perform actions as required.

**Integrating vCenter Chargeback to Monitor Application Cost**

vCenter Chargeback is an application that helps you see the cost of virtual machines. You can integrate vCenter Chargeback with AppInsight to compute the cost of virtual machines, tiers, applications, and components, and to identify correlations between application performance indicators and application cost. You can also receive notifications when operational costs exceed threshold specifications.

When vCenter Chargeback is integrated with AppInsight, it can calculate the cost of each application. It can also calculate the individual cost of the following computing resources of an application:

- CPU
- Disk read and write
- Memory
- Storage
- vCPU

Costs are calculated over one hour, for example between 13:00 and 14:00, and for 24-hour periods, from 00:00 to 23:59 according to the vCenter Chargeback server time. You can see the costs by opening the **Application** module and selecting the **Cost** KPI in the **Metrics** tab.

The cost currency is taken from the vCenter Chargeback cost model that you specify.

When you first integrate vCenter Chargeback with AppInsight, it might take up to two hours before you can view data.
Requirements for vCenter Chargeback Integration

You configure the virtual machines on which to monitor application cost in vCenter Chargeback.

- All of the virtual machines that are being monitored for cost must be part of a hierarchy in vCenter Chargeback. Data does not appear for virtual machines that are not configured in this manner.
  - It is good practice to locate all the virtual machines for AppInsight in a single hierarchy in vCenter Chargeback.
- AppInsight supports vCenter Chargeback v. 2.0.
- Verify that the cost model that you want to use in AppInsight is available in vCenter Chargeback.

You must register vCenter Server adapter before you can use this product.

To use vCenter Chargeback with AppInsight, you must register vCenter Chargeback in the AppInsight Adapter Manager. See, “Register Adapters for Integrating Complementary VMware Products,” on page 11.

Integrating vFabric Hyperic to Monitor Application Performance

vFabric Hyperic is an application that helps you view the performance of servers and the services that run on them. You can integrate vFabric Hyperic 5.0, or later, with AppInsight to monitor virtual machines and the servers running on those virtual machines.

You install a Hyperic agent on each of the virtual machines to monitor.

Note that when configuring a Hyperic adapter to retrieve data from the Hyperic server, the collection intervals of the Hyperic “Availability” metrics might change to one collection per minute.

For information about how to deploy agents, see the vFabric Hyperic documentation set appropriate to your version.

- You must register vCenter Server adapter before you can use this product.
- AppInsight supports vFabric Hyperic 5.0, and higher.
- To use vFabric Hyperic with AppInsight, you must register vFabric Hyperic in the AppInsight Adapter Manager. See “Register Adapters for Integrating Complementary VMware Products,” on page 11.
- You can only connect AppInsight to a single instance of Hyperic server.
- It is good practice to install the AppInsight server and the Hyperic server in the same data center or cluster.
- If you have multiple instances of AppInsight server that you are connecting to the vFabric Hyperic server, you require a unique Hyperic user name and password for each connection.
- Ensure that the Hyperic server and AppInsight server are time synchronized with the Hyperic agents.

Integrating vFabric Application Director with AppInsight to Monitor Application Director Deployments

vFabric Application Director accelerates and automates the configuration and deployment of enterprise applications. You can import application deployments from Application Director 5.0 and monitor them using AppInsight.

After you import an Application Director deployment, AppInsight discovers and synchronizes the deployed application. All monitored components appear in the AppInsight application topography in a single tier. You can perform actions such as moving components between tiers, as with other AppInsight components. When you import Application Director clusters, they appear as clusters in AppInsight. The installed probes and agents return monitoring data to AppInsight.
After you have imported an Application Director deployment to AppInsight, the application's topology is synchronized with Application Director. All code- and network-monitored components that are discovered in the deployed Application Director virtual machines are added to the application. Hyperic-monitored middleware data is also added as a metric.

A synch icon appears next to each monitored component in the topology. An additional synch icon appears next to the application name at the top of the AppInsight page. You can point to the icon to see the AppInsight application description.

If you scale out a cluster in Application Director that is monitored in AppInsight, the update is reflected in the application topology.

You can configure an alert to scale out an Application Director cluster if the number of hits on a specific component group exceed a defined threshold. See “Use an Alert to Scale Out an Application Director Cluster,” on page 45.

You can add hints for external services such as databases, LDAP, and so on to applications that are imported from Application Director.

If a deployment is torn down in Application Director, it is also deleted in AppInsight. Any platforms that are monitored by the Hyperic server are also deleted.

Requirements for vFabric Application Director Integration

Several conditions must be satisfied before Application Director applications can be imported to AppInsight.

- You must register the vCenter Server adapter before you can use Application Director with AppInsight. Verify that the vCenter Server adapter is the adapter for the vCenter server on which the deployments are located.
- To use vFabric Application Director with AppInsight, you must register vFabric Application Director in the AppInsight Adapter Manager. Verify that the SSL checkbox is selected. The credentials that you specify when registering the adapter must be sufficient to allow you to perform administrative tasks. See “Register Adapters for Integrating Complementary VMware Products,” on page 11.
- You must be using Application Director 5.0.
- You must configure the Hyperic HQ service in Application Director.
- Verify that the AppInsight server machine and Application Director machine are time synchronized.

Configure Code Agent Service for Application Director Integration

Before you can import a vFabric Application Director deployment for monitoring in AppInsight, you must configure the AppInsight Code Agent Installer service in the blueprint of the Application Director Application Server instances.

Prerequisites

- Verify that Application Director is installed and that you are familiar with its use.
- It is good practice to configure one AppInsight Code Agent Installer service for each application server. If you are installing more than one instance on an application server, and you intend to use the same AppInsight Code Agent Installer service, add a server_restart_consecutive number property in the Manage Catalog Items window in Application Director. See “Create a Property When Using a Code Agent Installer Service on Multiple Instances,” on page 15.
- Verify that the Linux operating system template that you are using has cURL installed.
Procedure

1. In Application Director, open the blueprint of the application version on which to install the AppInsight Code Agent Installer service.
   a. Click the required application.
   b. Click the required version.
   c. Click the blueprint.

   The blueprint topology appears.

2. Drag the AppInsight Code Agent Installer service from the Services list to the OS template of the component to monitor in AppInsight.

3. Click the installer service in the topology.

   The details of the service appear in a pane below the topology.

4. Edit the installer service properties' blueprint values.
   a. On the Details tab, change the name of the installer service, if necessary.
   b. On the Properties tab, double-click each of the properties to enter appropriate values.

   The `apm_user` and `apm_pass` values are secure.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>apm_pass</code></td>
<td>Password for AppInsight user interface login.</td>
</tr>
<tr>
<td><code>apm_user</code></td>
<td>User name for AppInsight user interface login.</td>
</tr>
<tr>
<td><code>apm_ip</code></td>
<td>IP address of the AppInsight instance.</td>
</tr>
<tr>
<td><code>install_paths</code></td>
<td>Array of paths to locations on which you can install the code agent. Enclose the array in square brackets. Enclose each location in quotation marks. Separate each location by a comma. [&quot;path&quot;,&quot;path&quot;,&quot;path&quot;]</td>
</tr>
<tr>
<td><code>server_restart_1</code></td>
<td>Server restart command. You can bind the value to other properties in the blueprint.</td>
</tr>
</tbody>
</table>

5. Click Save.

6. Repeat steps Step 1 through Step 5 for each Application Director deployment that you are importing.

   The Application Director deployment is configured to import to AppInsight.

What to do next

Import the deployment to AppInsight. See “Import an Application Director Deployment,” on page 17.

Create a Property When Using a Code Agent Installer Service on Multiple Instances

When you are using the code agent installer service on multiple instances of Application Director deployments, you must add a consecutively numbered Server Restart property for each instance.

Prerequisites

Verify that you have Application Director installed and that you are familiar with its use.

Procedure

1. In Application Director, select Services from the dropdown menu.

2. Click the AppInsight Code Agent Installer service.

3. Select the appropriate version of the service.
4 Click **Edit**.

5 In the **Properties** pane, click **New**.

6 Type `server_restart_consecutive_number` in the **Property Name** column.
   - The number must be the next consecutive number after the last existing `server_restart` property number in the installer.

7 Verify that the **Required** check box is not selected.

8 Click **Save**.

The property is visible in every installer in Application Director.

Do not delete the property because doing so might affect other Application Director deployments that use the same installer service.

**What to do next**

Configure the AppInsight Code Agent Installer service in the Application Director blueprint. See “Configure Code Agent Service for Application Director Integration,” on page 14.

**Configure Hyperic HQ Agent Service for Application Director Integration**

Before you can import a vFabric Hyperic metrics on Application Director deployments to AppInsight, you must configure the Hyperic HQ Agent service in the blueprint of the Application Director Application Server instances.

**Prerequisites**

- Verify that Application Director is installed and that you are familiar with its use.
- Verify that the Linux operating system template that you are using has cURL installed.
- Verify that the Hyperic server is in a routable location.

**Procedure**

1 In Application Director, open the blueprint of the application version on which to install the Hyperic HQ Agent service.
   a Click the required application.
   b Click the required version.
   c Click the blueprint.
   - The blueprint topology appears.

2 Drag the HQ Agent service from the Monitoring list to the operating system template of the component to monitor in AppInsight.

3 Click the HQ Agent service in the topology.
   - The details of the service appear in a pane below the topology.
4 Edit the installer service properties.
   a On the **Details** tab, change the name of the HQ Agent service if necessary.
   b On the **Properties** tab, double-click each of the properties to enter appropriate values.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBAL_CONF</td>
<td>Location from which Application Director can download the agent artifact. The default catalog value is a valid location.</td>
</tr>
<tr>
<td>HQ_PACKAGE_64</td>
<td>Location from which Application Director can download the agent artifact. The default catalog value is a valid location.</td>
</tr>
<tr>
<td>HQ_PACKAGE_32</td>
<td>Location from which Application Director can download the agent artifact. The default catalog value is a valid location.</td>
</tr>
<tr>
<td>ip_address</td>
<td>IP address of the monitored platform. You can bind the value to the self:ip value.</td>
</tr>
<tr>
<td>HQ_server_ip</td>
<td>IP address on which the Hyperic server that works with AppInsight is located.</td>
</tr>
</tbody>
</table>

5 Click **Save**.

6 (Optional) Repeat steps Step 1 through Step 5 for each Application Director deployment that you are importing to AppInsight.

The Hyperic HQ Agent service is configured for the Application Director deployment. When you import the deployment to AppInsight, the Hyperic metrics are also imported.

**Import an Application Director Deployment**

You can add enterprise applications in AppInsight by importing them as Application Director deployments. Importing Application Director deployments provides you with an end-to-end workflow, from provisioning applications in Application Director to monitoring and remediating them in AppInsight.

**Prerequisites**

- You must register the vCenter Server adapter before you can use Application Director with AppInsight. See *vFabric AppInsight Installation Guide*.
- To use vFabric Application Director with AppInsight, you must register vFabric Application Director in the AppInsight Adapter Manager. The credentials that you specify when registering the adapter must be sufficient to allow you to perform administrative tasks. See “Register Adapters for Integrating Complementary VMware Products,” on page 11
- Verify that the last task that was performed on the Application Director deployment completed successfully.

**Procedure**

1 On the **Applications** tab of the **Administration** module, click **Import**.

2 Select the deployment to import.

   Only deployments with the status Deployment Success or Update Success appear in the list of deployments for import.

3 (Optional) Specify the name for the AppInsight application.

4 (Optional) Add a description for the application.

5 Click **Import**.

The application appears in AppInsight and monitoring begins.
What to do next

- If you have not already done so, deploy a network probe.
- If the AppInsight Code Agent installer service was not already added to the application blueprint in Application Director, deploy the service manually.
Integrating vCenter Orchestrator to Manage Remedial Actions

vCenter Orchestrator, which is installed with the vCenter Server, provides a library of extensible workflows for creating and running processes that you can use to manage remedial actions in AppInsight.

After you register the Orchestrator adapter, you can select default actions, or select other Orchestrator workflows as additional actions for use in AppInsight. For example, actions might generate an alert email when the state of an application changes, or might stop services running on a virtual machine when high redundancy is detected.

You must use an SSL connection to manage Orchestrator workflows in AppInsight. When you add an Orchestrator adapter in AppInsight, ensure that the SSL Connection check box is selected.

Add Orchestrator Workflows on page 19
You can add Orchestrator workflows that are not included in the default workflow actions provided in AppInsight.

Delete an Orchestrator Workflow on page 20
You can delete the Orchestrator workflows that you added to AppInsight.

Add Orchestrator Workflows

You can add Orchestrator workflows that are not included in the default workflow actions provided in AppInsight.

You can also define actions in the Administration module, in the Alerts view. You can add actions to provide email notifications when a change in state occurs. If an action requires a user to enter data, a dialog box appears with relevant prompts.

Prerequisites

- Verify that you have vCenter Orchestrator version 4.2, or higher installed, and that it is registered in AppInsight and uses an SSL connection.
- Verify that any actions that you want to add in AppInsight have been specified in Orchestrator. Refer to the Orchestrator documentation if you need assistance.

Procedure

1. Navigate to the Manage Orchestrator Workflows area in the Support tab of the Administration module, and click Add.
2. Select the required workflow from the dropdown list.
   Depending on the workflow that you add, you might be required to specify parameter values.
3   Click OK.

The workflow is added to the list of actions in the Manage Orchestrator Workflows area.

The actions that appear in the Actions and VM Actions menus, are context-specific.

Delete an Orchestrator Workflow

You can delete the Orchestrator workflows that you added to AppInsight.

Procedure

1   Navigate to the Manage vCenter Orchestrator Workflows area in the Support tab of the Administration module.

2   Select the workflow to remove and click Delete.

The workflow is deleted from AppInsight.
You create applications in the Administration module. After you create the application, you must add one or more components so that monitoring can begin.

**Procedure**

1. (Optional) In the Applications tab of the Administration module, click **New Application**.
2. In the Add New Application dialog box, type a name for the new application in the **Name** text box.
3. (Optional) Add a description of the application.
4. Click **OK**.

The application is created.

**What to do next**

Add one or more components to the application. See Chapter 6, “Adding Components,” on page 23.
Adding Components

Before AppInsight can start to monitor your application, you must add at least one component.

For network probe monitoring, MSSQL, MySQL, PostgreSQL, Oracle, HTTP and HTTPS protocols are supported. For the code agent, MSSQL, MySQL, Oracle, HSQLDB, PostgreSQL, SQLFire, HTTP and HTTPS are supported. Code agent monitoring is also supported using plug-ins to various external resources. See vFabric AppInsight Developer’s Guide.

After you add the first component to an application, you can toggle the lightbulb icon at the top of each tier in the topology map to display or hide hints about other potential components that you can add to the application.

Tiers are not visible in the topology until after the first component is added to the application.

To limit skewed metrics, do not add network-monitored application components and code-monitored application components in the same tier. Such practice might affect latency calculations because network monitoring also includes the network overhead latency.

- Add a Mapped Component to an Application on page 23
  You can add components to your application that AppInsight has detected.

- Add Multiple Components to an Application on page 24
  You can select several components to add simultaneously to a tier in the application. You can also merge the components so that you can monitor them as a single entity.

- Add Components Using Hints on page 25
  Hints are dependencies between IP addresses that are detected by AppInsight. Each hint represents a potential component of an application. You can click on a hint to map it as a component of the application.

- Add an Unmapped Component to an Application on page 26
  You can add components that AppInsight has not detected to your application.

- Altering the Monitoring Method of a Component on page 26
  You can change a network-monitored component to become a code-monitored component.

Add a Mapped Component to an Application

You can add components to your application that AppInsight has detected.

Prerequisites

Verify that you created an application. See Chapter 5, “Create Applications,” on page 21.

Procedure

1. Select the application to which you are adding a component.
2 On the **Topology** tab of the **Application** module, verify that the Mapped Components table is visible on the left of the page.

The Mapped Components table lists all of the components that AppInsight has detected.

A map of the application's topology appears on the right, showing components and the tiers to which they are added. Before you add the first component to the application, the map area is blank.

3 Select an object in the Mapped Components table, and click **Add to Application**.

4 Select the tier to which the component is to be added from the tier menu.

If you are adding the first component to the application, type a name for the first tier in the **New Tier Name** text box.

5 (Optional) If the component uses HTTPS protocol, select an SSL key.

AppInsight supports the following PEM and PKCS cipher suites.

- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA

6 (Optional) If the component uses HTTPS protocol, and you have set the SSL key, you can set a password for the key.

7 Click **OK**.

The component is added to the map. If the tier was not already in the map, it is added.

### Add Multiple Components to an Application

You can select several components to add simultaneously to a tier in the application. You can also merge the components so that you can monitor them as a single entity.

**Prerequisites**

Verify that you created an application. See Chapter 5, “Create Applications,” on page 21.

**Procedure**

1 On the **Topology** tab of the **Application** module, click **Manage** to open the Management View window.

   The Mapped Components table on the left of the page lists all of the components that AppInsight has detected.

   A map of the application’s topology appears on the right, showing components and the tiers to which they are added. Before you add the first component to the application, the map area is blank.

2 Select multiple components in the Mapped Components table and click **Add to Application**.

   The selected components can be of different types and monitored in different ways.

3 Select the **Add the mapped component as a cluster?** check box to merge the selected components as a cluster that can be monitored as a single entity.

   You cannot add network-monitored components and code-monitored components in the same cluster.

   You must specify a name for the cluster.
4 Select the tier to which the cluster is to be added from the tier menu.
   If you are adding the first components to the application, type a name for the first tier in the New Tier Name text box.

5 (Optional) If one or more components in the cluster uses HTTPS protocol, select the SSL key.
   AppInsight supports PEM and PKCS format SSL keys.
   When you use this method of creating a cluster, all HTTPS components in the cluster must use the same SSL key.

6 (Optional) To add HTTPS components with different SSL keys, add them individually to the tier, then click Actions and select Cluster to add them to the cluster.

7 (Optional) If the component uses HTTPS protocol, and you have set the SSL key, you can set a password for the key.

8 Click OK.

The cluster is added to the map. If the tier was not already in the map, it is added.

Add Components Using Hints

Hints are dependencies between IP addresses that are detected by AppInsight. Each hint represents a potential component of an application. You can click on a hint to map it as a component of the application.

When dependencies between IP addresses are discovered, a hint appears to indicate the dependencies. Hints are displayed in the Management View window of an application.

Each endpoint has a separate hint.

Hints appear on the left or right side of a virtual machine, depending on whether they relate to incoming or outgoing dependencies. A hint that is located to the left of the virtual machine indicates an incoming dependency. A hint that is located to the right of the virtual machine indicates an outgoing dependency.

You can select multiple hints simultaneously, to add potential components to a tier.

Although a hint appears whenever an IP address is detected, you cannot add the component until the port is known.

Hints related to databases, queues, Web services, and so on appear only as hints. They cannot be added as potential components because AppInsight monitors only calls to external resources, not the external resources.

Prerequisites

You must have added at least one component to an application. See Chapter 6, “Adding Components,” on page 23.

Procedure

1 In the Topology tab of the Application module, click Manage.

2 In the topology table in the Management View window, verify that you can see hints.
   You can display or hide hints using the light bulb icon on the tier title bar.

3 Click the expand icon to show the properties of the virtual machine to which the hint relates.
   If a port for incoming traffic is detected for the virtual machine, the hint includes a plus sign (+).

4 Select one or more hints and click the plus sign + to add them as components.

5 If more than one port is discovered for a single IP address, a component is added for each port.

The hints become components in the tier in which they were added and their transactions are monitored.
Add an Unmapped Component to an Application

You can add components that AppInsight has not detected to your application.

You can add a new component in either the map or table view.

Procedure

1. On the **Topology** tab of the **Application** module, verify that the Mapped Components table is visible on the left of the page.
   
   The Mapped Components table lists all of the components that AppInsight has detected.
   
   A map of the application’s topology appears on the right, showing components and the tiers to which they are added. Before you add the first component to the application, the map area is blank.

2. Below the Mapped Components table, click the **Add an unmapped component** link.

3. Type data in the **Name**, **IP**, and **Port** text boxes.

4. Select the tier for the component from the menu.
   
   If you are adding the first component to the application, type a name for the first tier in the **New Tier Name** text box.

5. Select the protocol for the component from the menu.

6. Click **OK**.
   
   The component is added to the map. If the tier was not already in the map, it is added.

7. (Optional) If you selected the HTTPS protocol, you must set the SSL key.
   
   a. Click **Actions**, and select **Set SSL key**.
   
   b. Select the SSL key.
   
   c. (Optional) Set a password for the key.
   
   d. Click **OK**.

Altering the Monitoring Method of a Component

You can change a network-monitored component to become a code-monitored component.

A virtual machine can be monitored by the code agent or a network probe, not both.

You can use the code agent to monitor the code of HTTP- or HTTPS-type application components. Code monitoring uses metrics that provide you with a more in-depth view of your application component than network monitoring provides.

When you switch the method by which a component is monitored, the existing component is removed from the topology and becomes available in the Mapped Components table. The component with the new monitoring method is added to the tier in place of the one that was removed.

When the network-monitored component is removed from the application topology, all its transactions that have their root in the component are also removed. The code agent must detect and monitor the transactions following the switch.

To change the monitoring method of an application component that is part of a cluster, remove the component from the cluster to switch monitoring methods, then re-add it to the cluster.
Change the Component Monitoring Method

You can switch a component to code monitoring to increase the number of monitored metrics.

Prerequisites

Verify that the code agent is installed on the application server on which the application is running. See the VMware vFabric Installation Guide.

Procedure

◆ Change the component monitoring type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Change the component monitoring type in the application's topology map. | a In the Topology tab of the Application module, click Manage to open the Topology Management window.  
  b Select the application component to be monitored with the code agent and click Actions.  
  The component cannot be part of a cluster.  
  c Select Switch to Code Monitoring.  
  The network monitored component is deleted from the application topology and replaced with a code monitored component.  
  The network monitored component appears in the Mapped Components table. |
| Change the component monitoring type from the Mapped Components table. | a In the Mapped Components table select a code monitored component for the same virtual machine as a network monitored component that is already in the application's topology and click Add Component.  
  The component cannot be part of a cluster.  
  You are prompted to confirm that you want to replace the network monitored component with the code monitored component.  
  b Click OK.  
  The code monitored component appears in the application's topology. The network monitored component appears in the Mapped Components table. |
Add Transactions to the Topology of an Application

Some transactions are detected and monitored by AppInsight. Other detected potential transactions are not automatically monitored, but you can add them and have AppInsight calculate their KPIs.

Procedure

1. In the Summary tab of the Application module, click Manage in the Transactions widget.
   You can also access the Transactions management page by clicking Transactions in the Applications tab of the Administration module.
   The tables in the Transactions management page provide the following information.

   **Table 7-1. Transactions Tables**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the potential transaction or active transaction. You can change the name of an active transaction by selecting it and clicking Rename.</td>
</tr>
<tr>
<td>Tier</td>
<td>Left-most tier on which the transaction begins.</td>
</tr>
<tr>
<td>Component</td>
<td>Left-most component to which the transaction relates.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of hits on the transaction.</td>
</tr>
<tr>
<td>Latency</td>
<td>Latency of the transaction.</td>
</tr>
</tbody>
</table>

2. (Optional) Select the tier for which you want to see potential transactions from the dropdown menu on the Potential table menu bar.
   The potential transactions that appear are transactions that begin in the selected tier.

3. In the Transactions management page, select a transaction from the Potential table and move it to the Active table to start AppInsight monitoring.
   A maximum of fifteen active transactions is available. If you add another transaction, the first one in the table is deleted.
   The active transactions appear in the topology map below the two tables.

4. (Optional) Select transactions that you do not want AppInsight to monitor from the Active table and move them to the Potential table.
   The transaction is no longer visible in the topology map.
Manually Add a Transaction Element

For network components, you can add a transaction element manually using JMX.

Prerequisites

Verify that you are logged in to AppInsight. If you are not already logged in, you are prompted to do so before you can access the JMX Web page and add actions.

Procedure


2. On the JMX Web page, locate the `addWebTransactionElementByComponentName` operation.
   a. In the Parameters `ComponentName` text box, type the name of the component to which the transaction element relates.
   b. In the Parameters `URL` text box, type the URL of the transaction element.

   You can group multiple URLs and add them as a single transaction element by using wildcards for specific sections of the URL. For example, `/inbox/john /inbox/tim /inbox/<username>` might be grouped to one transaction element using the URL `inbox/*`.

3. Click the `addWebTransactionByComponentName Hit Me!` button.

   A new tab appears in the browser to confirm that the workflow was successfully created.

After a few minutes, the transaction element appears in the topology.
You can add tiers to the topology of an application, to logically group components.

Tiers are not visible in an application's topology until the first component is added to the application. After one tier is added to the topology, additional tiers can be added on the left or right sides.

**Prerequisites**

Add a component to the application, so that a tier appears in the application's topology. See Chapter 6, “Adding Components,” on page 23.

**Procedure**

1. Click Actions and select Add Tier on Right or Add Tier on Left.
2. Type a name for the tier and click OK.

The tier appears in the topology.

**What to do next**

Add components to the tier. See Chapter 6, “Adding Components,” on page 23.
Configuring KPI Thresholds

Every key performance indicator (KPI) metric has a threshold defined that shows how it is behaving relative to expectation. You can set static thresholds or they can be dynamically configured by AppInsight. The thresholds that are set determine when the color of the KPI changes.

When the thresholds appear on a graph, the red threshold line might be above or below the yellow threshold line. The positioning of the thresholds depends on whether the seriousness of the state relates to a metric being too high or too low. For example, in the Cost KPI, a high cost is serious so the red threshold is above the yellow threshold. In a performance index score, a low score is more serious so the red threshold is below the yellow threshold.

When you change the value of a metric, the threshold lines change in the graph.

You can also change the value of a metric by dragging the threshold lines in the graph. You cannot drag a threshold line to an illogical position. For example, you cannot move a red threshold line that is above the yellow threshold line so that it is below the yellow threshold line.

Thresholds in the graph cover the period of the last seven days, assuming that the application has been installed for at least that time, and the predicted thresholds for the next seven days.

This chapter includes the following topics:

- “Manually Configure KPI Metrics Thresholds,” on page 33
- “Enable AppInsight Dynamic Threshold Determination,” on page 34

Manually Configure KPI Metrics Thresholds

You can set static thresholds for KPI metrics that show how they are behaving relative to expectation. The color of the KPI changes when the metrics breach the thresholds.

You set KPI thresholds in the Application module.

Procedure

1. In the Metrics tab, click the gear wheel icon in the top right corner of the KPIs menu to open the threshold editor.

2. Verify that the Calculate KPI State button is toggled On so that other settings can be edited.

   You can toggle the button Off after saving your changes, to prevent the KPI from being included in the monitored objects.
3 Click Static and adjust the thresholds as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance KPI</strong></td>
<td>Use the text boxes on the left of the graph to set the warning and critical thresholds.</td>
</tr>
<tr>
<td></td>
<td>In the Single Hit Time menu, you can set the acceptable time limit for a reply to be sent back to the origin of the request. The time that you select represents the length of time that is tolerated (t). The Frustrated time is four times t.</td>
</tr>
<tr>
<td><strong>Usage KPI</strong></td>
<td>In the Hits section, the text boxes on the left of the graph represent the low hits and high hits thresholds. Hits are counted per minute. Errors are counted as a percentage.</td>
</tr>
<tr>
<td></td>
<td>Use the Hits and Errors buttons to toggle between thresholds for hits and for errors. Set upper and lower thresholds for hits because too many or too few hits might cause a change in state.</td>
</tr>
<tr>
<td><strong>Middleware KPI</strong></td>
<td>Use the text boxes to set the warning and critical percentages for the total number of servers on which a component runs. If the stated percentage is equalled or exceeded, the color of the KPI changes.</td>
</tr>
<tr>
<td><strong>Infrastructure KPI</strong></td>
<td>Use the text boxes to set the warning and critical percentages. If the stated percentage of the total number of virtual machines is equalled or exceeded, the color of the KPI changes accordingly.</td>
</tr>
<tr>
<td><strong>Hits Per Component KPI</strong></td>
<td>Use the text boxes to set the warning and critical number of hits. If the stated number of hits is equalled or exceeded, the color of the KPI changes accordingly.</td>
</tr>
<tr>
<td><strong>Transaction Health KPI</strong></td>
<td>Use the text boxes to set the warning and critical percentages. If the stated percentage of the total number of an object's transactions is equalled or exceeded, the color of the KPI changes accordingly.</td>
</tr>
<tr>
<td><strong>Tier Health KPI</strong></td>
<td>Use the text boxes to set the warning and critical percentages. If the stated percentage of the total number of tiers is equalled or exceeded, the color of the KPI changes accordingly.</td>
</tr>
<tr>
<td><strong>Component Health KPI</strong></td>
<td>Use the text boxes to set the warning and critical percentages. If the stated percentage of the total number of objects is equalled or exceeded, the color of the KPI changes accordingly.</td>
</tr>
<tr>
<td><strong>Cost KPI</strong></td>
<td>Use the text boxes to set the warning and error values. The two fields on the left of the graph represent the warning and critical thresholds.</td>
</tr>
</tbody>
</table>

The thresholds appear on the graph as red and yellow lines.

4 Click **Save** to apply your changes.

**What to do next**

Configure when alerts are triggered and the actions to take. See “Edit an Alert,” on page 45. If you do not specify an alert action, you can still view alerts data in the Notification table.

**Enable AppInsight Dynamic Threshold Determination**

Thresholds can be dynamically configured by AppInsight. The thresholds that are set determine when the color of the KPI changes.

You enable AppInsight-determined KPI thresholds in the **Application** module.

Dynamic thresholds are calculated on the basis of historic data for the same hour of the same day.

A Warning threshold is calculated as twice the standard deviation.

A Critical threshold is calculated as four times the standard deviation.

**Procedure**

1 In the **Metrics** tab, click the gear wheels icon in the top right corner of the KPIs menu to open the threshold editor.
2 Click **Dynamic**.
3 Click **Save** to apply your changes.

AppInsight sets dynamic thresholds for the KPI.

**What to do next**

Configure when alerts are triggered and the actions to take. See “Edit an Alert,” on page 45. If you do not specify an alert action, you can still view alerts data in the Notification table.
By monitoring the performance of your applications, you can detect areas to adjust to achieve service level agreements. AppInsight comprises views that show different perspectives of the monitored data.

The Application module is divided into views. Within each view, you can focus on areas of information to see in-depth information.

AppInsight uses several modules to monitor application performance, and for administration purposes.

This chapter includes the following topics:
- “vFabric AppInsight Dashboard,” on page 37
- “Application Module,” on page 38
- “Administration Module,” on page 43

**vFabric AppInsight Dashboard**

The AppInsight dashboard provides you with a high-level overview of your applications and their health. You can select an application to view more detail.

The dashboard shows all of the applications that AppInsight is monitoring. The color next to an application name indicates its health state.

<table>
<thead>
<tr>
<th>Color</th>
<th>Health Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Item is within specified thresholds for acceptable performance</td>
</tr>
<tr>
<td>Yellow</td>
<td>Item is within the specified thresholds for warning about performance</td>
</tr>
<tr>
<td>Red</td>
<td>Item is outside specified thresholds for acceptable performance</td>
</tr>
</tbody>
</table>

You can hover over the graph in an application box, to view latency and hit rate details, or click the extension arrow to show KPI and performance status.

In addition to the applications, widgets list the most used applications, the slowest applications, and the most prominent notifications for the monitored applications. You can select an application in a widget to focus in on more detail.

When you select an application, the Application module Summary view appears. You can click Manage in the Transactions widget title bar to modify the application’s structure, or manage its transactions.
Application Module

In the Application module, you can view summary data, metrics, topology mapping, event notifications and samples for your application.

Key User Interface Elements in the Application Module

Some user interface elements are common to all views in the Application module.

Table 10-2. User Interface Elements in the Application Module

<table>
<thead>
<tr>
<th>User Interface Element</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Picker button</td>
<td>Expands the Time Picker pane, which shows a graph of the period of time for which data is provided. In the Time Picker pane, you can select alternative time periods. By default, the Time Picker button name is the range of time related to the time period that you selected. If you have not selected a time period, the default of ten minutes is used.</td>
</tr>
<tr>
<td>Inventory button</td>
<td>Shows a group of icons for tiers, transactions, components, and virtual machines that represent the items on which data is monitored. The number next to each icon indicates how many instances of the item are being monitored. You can click the Inventory button to expand the Navigation pane, which shows a table listing the names of the monitored items and their health status.</td>
</tr>
</tbody>
</table>

Customizing Views in the Application Module

- You can click Customize in the title bar of a line graph widget in the Application module to select additional metrics to show in the graph. Note that selecting additional metrics might change the default colors of the display.
- You can click Notifications in the title bar of a KPI graph to display or hide notification markers on the graph. When you click a notification marker, information relevant to the notification appears. You can click the link in the notification description dialog box to open the Notifications view, to see additional information.

The letter that appears in the notification marker indicates its type.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Alert notification</td>
</tr>
<tr>
<td>I</td>
<td>Infrastructure notification</td>
</tr>
<tr>
<td>C</td>
<td>Configuration notification</td>
</tr>
</tbody>
</table>

You can filter the notifications that you see on a graph by clicking the filter arrow on the left of the Notifications button and selecting the checkboxes for the notification types that you want to see. The filter list contains only the notification types that exist in the application in the selected time range.

The Application module includes several views.

- Summary View on page 39

  In the Summary view, you see widgets that provide an overview of the AppInsight object that you selected, for the selected period.
- **Metrics View** on page 39
  
  In the **Metrics** view, you can see summaries of the KPI metrics, including performance, usage, cost, the health of transactions, and so on.

- **Topology View** on page 40
  
  In the **Topology** view, you see the virtual machines, components, and transactions of your application, including the identities of the virtual machines on which the application is running and their location. You also see the vFabric Hyperic services that are running.

- **Notifications View** on page 41
  
  In the **Notifications** view, a table shows information related to AppInsight alerts and configuration changes in your application.

- **Samples View** on page 42
  
  AppInsight samples transactions that network probes or code agents monitor. Transactions with high latency are prioritized for collection. A sample traces a transaction element to identify its topology and monitoring data.

### Summary View

In the **Summary** view, you see widgets that provide an overview of the AppInsight object that you selected, for the selected period.

The widgets that appear depend on the type of AppInsight object that you select. Generally, the following widgets appear.

- **General Details Widget**
  
  The General Details widget provides high level information about the object, including average latency, performance index score, hits and errors rates, and so on.

- **State Over Time Widget**
  
  The State Over Time Widget provides information about the changes in the state of the object that have occurred during the specified period.

- **Transactions Widget**
  
  When an application or component is selected, this widget represents transactions data. When a tier or virtual machine is selected, the widget represents component data. When a transaction is selected, the widget represents transaction element data.

  The data changes dependent on the selection. For example, the Transactions widget provides health, performance index, latency, hits and errors data for each of the selected application or component's transactions.

- **Key Metrics Widget**
  
  The Key Metrics widget provides information about the average latency, hit rate, and error rate for the object.

You can click a link in a widget to focus in on a detail of interest.

### Metrics View

In the **Metrics** view, you can see summaries of the KPI metrics, including performance, usage, cost, the health of transactions, and so on.

The type of information that is available depends on the KPI metric that you select.

Depending on the KPI metric that you select, you can click the icons at the bottom of the page to view the metric by various breakdowns. For example, in the Usage KPI, you can view the data as application usage over time, or as usage by components. The name of the breakdown type appears when you point to the selection icon.
## Table 10-3. Description of KPI Metrics

<table>
<thead>
<tr>
<th>KPI Metric</th>
<th>Description</th>
</tr>
</thead>
</table>
| Performance    | The Performance KPI represents the performance index score, calculated as the response time of all the transaction elements of the selected object, relevant to the thresholds.  
A performance index score is an industry standard used for reporting and comparing the performance of software applications in computing. |
| Usage          | The Usage KPI comprises the Hits KPI and the Errors KPI. The Usage KPI is based on all the application’s hits. The KPI represents the worst case between the hit rate and the error percentage, relevant to the thresholds. |
| Middleware     | The Middleware KPI is available when the vFabric Hyperic agent is installed.  
- The Application Middleware KPI for the virtual machine is the availability and other metrics, taken from the vFabric Hyperic agent.  
- The Application Middleware KPI for an application component is the availability of the server.  
- The Application Middleware KPI for an application, tier or cluster is calculated as a percentage of its application component’s middleware states. |
| Infrastructure | The Infrastructure KPI is available when a virtual machine is either part of the vCenter Server that is configured in the adapter, or when a Hyperic agent is deployed on the virtual machine.  
- The Infrastructure KPI for a virtual machine, is the worst state between the vCenter Server health and the availability of the Hyperic agent.  
- The Infrastructure KPI for a component, is the infrastructure state of the virtual machine on which the component is running. |
| Hits Per Component | The Hits Per Component KPI is calculated as the average hit rate of all components in the cluster. In the case of a single component, it represents the hit rate of the component itself. |
| Transaction Health | The Transaction Health KPI is calculated as the percentage of transactions in warning/critical state, relevant to thresholds. |
| Tier Health    | The Tier Health KPI is calculated as the percentage of tiers in warning/critical state, relevant to thresholds. |
| Component Health | The Component Health KPI state is calculated as the percentage of components in warning/critical state, relevant to thresholds. |
| Cost           | The Cost KPI is available when the vCenter Chargeback agent is installed. The Cost KPI represents the cost of the selected object, relevant to thresholds. The cost is calculated per virtual machine. |

### Topology View

In the **Topology** view, you see the virtual machines, components, and transactions of your application, including the identities of the virtual machines on which the application is running and their location. You also see the vFabric Hyperic services that are running.

The information that you see depends on the object that you have selected.
The color of the icons in the map indicate their health status.

### Table 10-4. Health Status Indicator Colors

<table>
<thead>
<tr>
<th>Color</th>
<th>Health Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Item is within specified thresholds for acceptable performance</td>
</tr>
<tr>
<td>Yellow</td>
<td>Item is within the specified thresholds for warning about performance</td>
</tr>
<tr>
<td>Red</td>
<td>Item is outside specified thresholds for acceptable performance</td>
</tr>
</tbody>
</table>

You cannot edit information in the **Topology** view. To edit information, click **Manage**.

**Map**

Each box in the map represents an application component.

The map is divided by tier.

You can view the following data in the application component box, depending on the selected object.

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component health status indicator</td>
<td>yellow (warning)</td>
</tr>
<tr>
<td>Virtual machine health status indicator</td>
<td>green (OK)</td>
</tr>
<tr>
<td>Virtual machine on which the component is running</td>
<td>virtual machine #1</td>
</tr>
<tr>
<td>Server that the Hyperic agent on this virtual machine is monitoring, if relevant</td>
<td>tlv-apmdemo</td>
</tr>
<tr>
<td>IP address of the virtual machine on which the component resides and its port</td>
<td></td>
</tr>
<tr>
<td>Installation path (for a code monitored application component)</td>
<td></td>
</tr>
<tr>
<td>Hit rate per minute and latency metrics</td>
<td>461.5 h/m 2.5 ms</td>
</tr>
<tr>
<td>Monitoring level</td>
<td>network, code</td>
</tr>
<tr>
<td>Protocol</td>
<td>HTTP, JBoss, MySQL</td>
</tr>
</tbody>
</table>

Key monitored data for the application component appears in a bar across the bottom of the box. This information includes the number of hits per minute and can also include data about the latency and, for data monitored using complementary VMware products, the latency when calling external components.

When you are viewing the map of a transaction, you see the transaction element name in the application component box, and the transaction element's monitored data. You do not see virtual machine data.

With database components, the transaction elements are the structure of the queries.

**Notifications View**

In the **Notifications** view, a table shows information related to AppInsight alerts and configuration changes in your application.

The information that you see includes a variety of data.
<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Whether the notification was generated by an alert, or because of a detected code, configuration or infrastructure change.</td>
</tr>
<tr>
<td>Description</td>
<td>■ In the case in which KPI thresholds have been defined, when a threshold has been exceeded you see details of the deterioration or improvement.</td>
</tr>
<tr>
<td></td>
<td>■ In the case of a configuration change, for example if the Tomcat server.xml file changes, you see the original text and the changed text.</td>
</tr>
<tr>
<td></td>
<td>■ In the case of WAR or JAR files, the list of files within the archive that changed.</td>
</tr>
<tr>
<td>Alert On</td>
<td>The name of the object for which the notification was generated.</td>
</tr>
<tr>
<td>Time</td>
<td>Time that the action that caused the notification occurred.</td>
</tr>
<tr>
<td>Generator</td>
<td>The source from which the notification originated, including vFabric AppInsight, vSphere and vFabric Hyperic.</td>
</tr>
</tbody>
</table>

When you click on an Alert-type entry in the Notifications List table, additional details about the notification appear in the Notification Details pane. The time that the details are based on is shown in the Notification Details pane.

**Samples View**

AppInsight samples transactions that network probes or code agents monitor. Transactions with high latency are prioritized for collection. A sample traces a transaction element to identify its topology and monitoring data.

In the case of network monitoring, the sample data includes the content of its requests and replies. In the case of code agent monitoring, the sample data includes internal calls and methods.

Sample data appears in tabular format. When you select a sample in the table, additional details appear in the Sample Details pane.

**Table 10-5. Samples Table Content**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>The time at which the sample was taken.</td>
</tr>
<tr>
<td>Transaction Element</td>
<td>The name of the transaction element from which the sample was taken.</td>
</tr>
<tr>
<td>Component</td>
<td>The component of which the transaction element is a part.</td>
</tr>
<tr>
<td>VM</td>
<td>The virtual machine on which the component is running.</td>
</tr>
<tr>
<td>Latency</td>
<td>The time in milliseconds that elapsed from the time the request was sent until a response was received.</td>
</tr>
<tr>
<td>Bytes</td>
<td>The number of bytes received in the response.</td>
</tr>
<tr>
<td>Error Status</td>
<td>OK or Error, according to the sample. An error sample is a sample that received an HTTP 5xx error code reply, or had an exception in its execution.</td>
</tr>
<tr>
<td>Sample Type</td>
<td>Network HTTP, Code HTTP or Code Internal, depending on how the data was detected.</td>
</tr>
<tr>
<td>Client</td>
<td>The client name or IP address of the component that initiated the request.</td>
</tr>
</tbody>
</table>
Administration Module

In the Administration module, you can register adapters for agents and complementary VMware products so they can be integrated in AppInsight and view the adapters' status, access the probe deployment page, view and configure alerts, download the client log for troubleshooting purposes, manage users and configure auto refresh options.

Getting Started

Use the links on the Getting Started tab to navigate through the basic configuration tasks that are necessary for starting the monitoring process.

Adapters

Use the Adapters tab to register or delete adapters and complementary VMware products.

Agents

Use the Agents tab to stop or start code agents and to view the code agents that are deployed, their state, and the components and applications that they are monitoring. Click the double arrow icon in the More column to view additional details.

You also download the AppInsight Code Agent on this tab.

Applications

Use the Applications tab to add, edit, or delete applications.

Alerts

Use the Alerts tab to define new alerts, or edit or cancel existing ones and to view data about configured alerts.

Support

Use the Support tab to:

- Download the client log for troubleshooting.
- Go to the Support page and download the support package.
- Enable auto refresh and specify the number of milliseconds between refresh cycles.
- Manage vCenter Orchestrator workflows.

Users

Use the Users tab to add or delete users, allocate permissions and create passwords.

Non-Administrator users can change their own password in this tab.

Define Alerts

You can define the conditions under which AppInsight generates an alert, and specify one or more actions to take when an alert is triggered. Alerts can be triggered for a single AppInsight application or for every application, tier, component, virtual machine, or transaction that has a state.

You can define new alerts, or edit or cancel existing ones. If you are defining a new alert, follow all the steps in the procedure. If you are editing an existing alert, follow the appropriate steps in the procedure to make the necessary changes.
When you add more than one alert condition to the Alert Conditions table, an alert is only triggered when all the conditions are satisfied.

**Procedure**

1. In the **Administration** module, click **Alerts**.  
   A table appears with key data for all active alerts.
2. Click **New Alert**.
3. Type a name for the alert in the **Alert Name** text box.
4. Select the AppInsight object type from the **Alert on** menu.
5. (Optional) If you select **Application**, also select the relevant application from the **Application** sub-list.
6. In the **Calculated over periods of** menu, select the timeframe over which the state change is to be calculated.  
   AppInsight analyses the behavior of the object over the entire period to determine the state.
7. Click **Add condition** and add the details of the conditions to trigger the alert.
   
   a. (Optional) If you selected **Application** in the **Alert on** menu, select an application object in the **Choose application object** menu.
   
   b. Select the key performance indicator to which the alert applies in the **KPI** menu.
   
   c. Select the state change that triggers the alert in the **Triggered when state changes to/from** menu.
   
   d. Click **Add**.

   The condition is added to the Alert Conditions table.

The alert appears in the Alert Conditions table.

**What to do next**

Define the actions to occur when an alert is triggered. See “Define Alert Actions,” on page 44.

**Define Alert Actions**

You can define actions to be taken when alerts are triggered. You can also view alerts in the Notifications table.

It is not mandatory that you specify actions when alerts are triggered. If you do not specify an action, you can still view notifications of alerts in the Notifications table.

**Procedure**

1. Specify the actions to occur when an alert is triggered.

   You can specify actions for alerts that are triggered when a state deteriorates and for when a state improves.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Action in the State Deteriorates pane</strong></td>
<td>Specifies an action when an alert is triggered because a state deteriorates.</td>
</tr>
<tr>
<td><strong>Add Action in the State Improves pane</strong></td>
<td>Specifies an action when an alert is triggered because a state improves.</td>
</tr>
</tbody>
</table>

2. Select an action from the **Choose Action** menu.

   The **Send notification** action is the default. You can customize the available actions if you have the vCenter Operations Manager plug-in installed.
3 Type the required information in each text box and click OK.
   The text boxes that appear depend on the action that you select.
   The action appears in the relevant Action pane for the alert.

**Edit an Alert**

You can change the details of an alert, including what aspect of an application is monitored, what conditions are specified to trigger the alert, and what action is taken when the alert is triggered.

**Procedure**

1 In the **Administration** module, click **Alerts**.
2 In the Configured Alerts table, select the alert to change and click **Edit**.
3 Make the required changes.
   You can delete conditions or actions by selecting the items in their table and clicking the **Delete Condition** or delete icon (x), respectively.
4 Click **Update** to save your changes.

**Use an Alert to Scale Out an Application Director Cluster**

You can create an AppInsight alert to trigger a scale out action on an Application Director cluster when the Hits per Component KPI thresholds are exceeded.

After you have configured this alert, when the threshold for the number of hits that a cluster in Application Director experiences is exceeded, AppInsight will trigger an Application Director scale out action that adds one or more virtual machines to the component group.

**Prerequisites**

The Hits per Component KPI must be enabled for the component group to which the scale out action relates.

You must have added a workflow to vCenter Orchestrator to scale out Application Director node arrays (clusters.) See “Create a Scale Out Workflow in vCenter Orchestrator,” on page 46.

**Procedure**

1 On the **Alerts** tab of the **Administration** module, click **New**.
2 Select a single application.
3 Click **Add Condition**.
   a In the **Select Application Object** menu, select **Components > Component Name**.
   b In the **KPI** menu, select **Hits Per Component**.
   c Click **Add Action**.
4 In the State Deteriorates pane, click **Add**.
5 In the **Choose Action** menu, select the vCenter Orchestrator workflow that you defined for scaling out Application Director clusters and click **OK**.
6 Click **Save**.

The alert appears in the Configured Alerts table.
Create a Scale Out Workflow in vCenter Orchestrator

Before you can create an AppInsight alert to scale out an Application Director node array, you must create a scale out workflow in vCenter Orchestrator.

Prerequisites

Before you create the workflow, verify that these prerequisites are satisfied.

- vCenter Orchestrator is installed, together with the HTTP-REST plug-in.
- You are familiar with creating vCenter Orchestrator workflows.
- The Application Director server certificate is imported and approved with the REST vCenter Orchestrator plug-in.

Procedure

1. Use the Add new REST host workflow provided with the REST plug-in to create a new REST host.
   Give the workflow a unique name, type the URL of your Application Director server in the URL text box, and accept the default values for the other properties.
2. Click Submit.
3. Use the Add REST operation workflow provided with the REST plug-in to create a new operation.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Use the name specified for the REST host.</td>
</tr>
<tr>
<td>Name</td>
<td>Type a unique name.</td>
</tr>
<tr>
<td>Template URL</td>
<td>Type <code>/darwin/api/1.0/deployment/{DeploymentId}/action/scale-out</code></td>
</tr>
<tr>
<td>HTTP Method</td>
<td>Type Post</td>
</tr>
<tr>
<td>Content Type</td>
<td>Type <code>application/json</code></td>
</tr>
</tbody>
</table>
4. Click Submit.
5. Download the scale out workflow from the Solution Exchange and import it to vCenter Orchestrator.
6. Configure the scale out workflow to point to the REST operation you created in Step 3.

What to do next

1. Add the scale out workflow to AppInsight. See “Add Orchestrator Workflows,” on page 19.
2. Create the scale out alert in AppInsight. See “Use an Alert to Scale Out an Application Director Cluster,” on page 45.

Create a vFabric AppInsight Support Package for Troubleshooting

An AppInsight support package is a collection of logs, configuration files, and internal databases. If you encounter difficulties with AppInsight, the VMware technical support representative might ask you to create and submit an AppInsight support package.

You access the support package creation page through the Deployment module.

Procedure

1. On the Support tab of the Administration module, click Go to Support page and download support package.
2 In the Diagnostic Support area, select either **Default** or a **Custom** option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Collects all of the logs, configuration, and server databases of the AppInsight server and its probes and agents for the previous four days.</td>
</tr>
<tr>
<td>Custom: Server only</td>
<td>Collects all of the logs, configuration, and server databases of the AppInsight server, excluding data from probes and agents.</td>
</tr>
<tr>
<td>Custom: Commands only</td>
<td>Includes server commands, but excludes probe data, logs, and database data.</td>
</tr>
<tr>
<td>Custom: Time delineated</td>
<td>Enables you to select a period of time in hours.</td>
</tr>
</tbody>
</table>

3 Click **Create Support Package**.
   Support package creation might take several minutes.

4 When the support package is created, click **Support Package Directory** to access the support package.
   The support packages are date stamped in the format `yyyyymmdd`. 
Delete an Application

If an application is no longer relevant, you can delete it from AppInsight.

**Prerequisites**

Open the application to delete.

**Procedure**

1. In the Applications tab of the Administration module, select an application and click Delete.
2. In the Confirm Deletion dialog box click Yes.

The application, its tiers, and all of its components, transactions, and transaction elements are deleted from AppInsight.
Delete a Tier

If a tier is no longer relevant, you can delete it from AppInsight.

Prerequisites
Open the application that contains the tier to delete.

Procedure
1. In the Topology tab of the Application module, click Manage to open the Topology Management window.
2. Select the tier to delete and click Actions.
3. Select Delete Tier.
4. In the Confirm Deletion dialog box, click Yes.

The tier and all of its components, transactions, and transaction elements are deleted.
Components revert to potential components. Transactions revert to potential transactions.
Managing AppInsight Users

You manage AppInsight users in the Administration module. Users can have either an Administrator or an Application Owner role.

General user management tasks, such as creating or deleting users, assigning permissions, and so on can only be performed by Administrator users. Application Owner users can change their passwords.

When you select a user in the Users table, their details appear in the User Details pane.

User Roles and Permissions

**Administrator**
A user with the Administrator role has read/write permissions for all parts of AppInsight. An Administrator cannot view other users' passwords, but can specify a new password for a user when necessary.

**Application Owner**
The permissions that an Application Owner has are specified by the Administrator.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>User can view content.</td>
</tr>
<tr>
<td>Perform VM Actions</td>
<td>User can perform AppInsight actions such as resetting virtual machines or reverting to the current snapshot.</td>
</tr>
<tr>
<td>Write</td>
<td>User can manage topology and thresholds, and can create and edit alerts.</td>
</tr>
</tbody>
</table>

For each application, the Administrator can specify certain permissions.

There are a number of actions an administrator can do on user accounts.
- **Add a New User** on page 54
  You create AppInsight users in the Users view of the Administration tab.
- **Change a Password** on page 54
  If you are an Administrator, you can change passwords on the Users tab of the Administration module.
- **Unlock a User Account** on page 54
  If a user enters an incorrect password multiple times, the account is locked.
- **Delete a User Account** on page 55
  You delete AppInsight user accounts on the Users tab of the Administration module. Only users with an Administrator role can delete users.
Add a New User

You create AppInsight users in the Users view of the Administration tab.

Procedure
1. On the Users tab, click New User.
2. Type a user name for the user.
3. Select either Application Owner or Administrator from the Role menu.
4. Type a password in the New Password text box and retype it in the Confirm Password text box.
5. Click Add.
   The new user name appears in the list in the Users table.
6. Ensure that the new user’s name is selected, and for each application, select the check boxes that define the permissions for the user.
   An unselected check box means that the user does not have that permission.
7. Click Save.

The new user account is created.

Change a Password

If you are an Administrator, you can change passwords on the Users tab of the Administration module.
If you have the Application Owner role, you can change your own password.

Procedure
1. In the Users table, select the name of the user whose password is being changed.
   The attributes for the user appear in the User Details pane.
2. Type a password for the user in the New Password text box.
3. Confirm the password in the Confirm Password text box.
4. Click Update Password.
5. Advise the user of the new password.

Unlock a User Account

If a user enters an incorrect password multiple times, the account is locked.
The account unlocks after 15 minutes.

Procedure
1. Wait for 15 minutes and enter the correct password.
2. (Optional) If you have forgotten your own password, contact your AppInsight Administrator to have a new password defined.

The lock is removed from the account.
Delete a User Account

You delete AppInsight user accounts on the Users tab of the Administration module. Only users with an Administrator role can delete users.

**Procedure**

1. On the Users tab, select the name of the user to delete.
2. Click Delete User.
3. Click Yes when you are prompted to confirm the action.

The user account is deleted from the table of users.
Index

A
about AppInsight 5
accounts, unlocking 54
actions
  managing with Orchestrator 19, 20
  remedial 19
actions for alerts 19
adapters, registering 11
add SSL key 23, 26
add tiers 31
adding components 23, 26
adding multiple components 24
adding new users 54
Administration module 43
alerts
  actions 44
  editing 43, 45
  notifications 44
  scale out Application Director cluster 45, 46
  specifying conditions 43
AppInsight
  about 5, 7
  best practices 9
  key terms 7
  optimizing 7
  support package 46
application cost, monitoring 12
Application Director, scale out cluster 45
Application module
  customizing views 38
    inventory pane 38
    overview 38
    time picker pane 38
application performance
  managing 13
  monitoring 37
applications
  about 7
  adding components 23, 26
  adding multiple components 24
  creating 21
  deleting 49
  deleting tiers 51
  monitoring Application Director deployments 13–17
  monitoring cost 12

B
best practices
  adding components 9
  configuring virtual machines 9
  monitoring options 9
complementary products
  code agent installer service, configure 14
  integrating 11
  registering 11
  user permissions 11
  vCenter Chargeback 11
  vCenter Orchestrator 11
  vFabric Hyperic 11
components
  about 7
  add transaction elements 30
  add using hints 25
  adding 23, 26
  adding multiple 24
  changing monitoring method 26, 27
  mapped 23, 24
  potential 23
  unmapped 26
  cost, monitoring 12
  creating
    AppInsight support package 46
    applications 21

D
dashboard
  adding applications 37
  most expensive applications 37
  most used applications 37
  slowest applications 37
data storage time 7
deleting
  applications 49
tiers 51
dynamic KPI thresholds 33, 34

G
getting started
  add components to an application 23
  create application 21
**H**
hints about potential components 25
HQ Agent service, configure 16

**I**
iintegrating
vCenter Chargeback 12
vCenter Orchestrator 19
vFabric Application Director 13, 17
vFabric Hyperic 13

**K**
key performance indicators, See KPIs
KPIs, configure thresholds 33, 34

**M**
managing performance 13
managing users
add new 54
change password 54
delete user account 55
permissions 53
roles 53
unlock account 54
Mapped Components table 23
metrics, See also KPIs
Metrics view 39
modules
  Administration 43
  Application 38
monitoring components 26, 27
monitoring cost 12
monitoring performance 37

**N**
notifications 41
Notifications view 41

**O**
optimizing AppInsight 9
Orchestrator
  add actions 19
  managing actions 19

**P**
passwords, changing 54
performance, managing 13
Potential Components table 23

**R**
registering complementary products 11
remedial actions 19
requirements
vCenter Chargeback integration 12
vFabric Application Director integration 13, 17
vFabric Hyperic integration 13

**S**
Samples view 42
scale out cluster workflow 46
SSL keys, adding 23, 26
static KPI thresholds 33
Summary view 39
support packages, AppInsight 46

**T**
tables
  Mapped Components 23
  Potential Components 23
  thresholds
    enabling dynamic 33, 34
    setting static 33
tiers
  about 7
  adding 31
  deleting 51
time picker 7
topology
  add tiers 31
  map view 40
  table view 40
Topology view 40
transaction elements
  about 7
  adding 30
  samples 42
transactions
  about 7
  active 29
  managing 29
  potential 29
  start monitoring 29
troubleshooting, create AppInsight snapshots 46

**U**
unlocking accounts 54
user accounts, deleting 55
user permissions, complementary products 11
users
  deleting accounts 55
  managing 53, 54
Index

V
vCenter Chargeback integration, requirements 12
vCenter Orchestrator
introducing 19
scale out cluster workflow 46
vFabric Application Director deployment
code agent installer service, create new property 15
HQ Agent service 16
import 17
vFabric Application Director integration, requirements 13
vFabric Hyperic integration, requirements 13
viewing samples 42
views
customizing 7
Metrics 39
Notifications 41
Samples 42
Summary 39
Topology 40

W
workflow actions, deleting 20