Contact Information
Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

About the Documentation
- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice
© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.
Table of Contents

About VMware vSphere Integration ................................................................. 6
   About Certification Compliance Mode ...................................................... 6
   Use Cases ............................................................................................... 6
   Data Center Visibility ............................................................................. 6
   Data Center Assessment & Compliance .................................................. 7
   Data Center Control .............................................................................. 7
   Additional VMware Documentation ....................................................... 8

About this Plugin .......................................................................................... 8
   Concepts, Components, Considerations ................................................ 8
   What to Do ............................................................................................. 9

Requirements ............................................................................................... 10
   Forescout Requirements ....................................................................... 10
   Networking Requirements ................................................................... 10
   Supported Vendor Requirements ......................................................... 10
   About Support for Dual Stack Environments ....................................... 11

Define Forescout Users in the VMware Environment .................................. 11
   Define a vSphere Role .......................................................................... 11
   Define Users with a Forescout Role ...................................................... 13
   Define Users with Read-Only Permissions .......................................... 14

Configure the Plugin ................................................................................... 16
   Define Target ESXi Host or vCenter Server ........................................ 16
   Add VMware Advanced Properties .................................................... 21
   Verify That the Plugin Is Running ....................................................... 23

Test the VMware Connection .................................................................... 23

View the VMware vSphere Connection ..................................................... 23

Work with VMware vSphere Policy Templates ........................................... 24
   VMware Classification Template ......................................................... 26
   Prerequisites ....................................................................................... 26
   Create a VMware Classification Policy ............................................... 26
   How Endpoints are Detected and Handled .......................................... 28
   VMware ESXi Host Firewall Compliance .......................................... 30
   Prerequisites ....................................................................................... 30
   Create a VMware ESXi Host Firewall Compliance Policy ................ 30
   How Endpoints are Detected and Handled .......................................... 32
   VMware ESXi Host Lockdown Compliance ....................................... 33
   Prerequisites ....................................................................................... 34
   Create a VMware ESXi Host Lockdown Compliance Policy ................ 34
   How Endpoints are Detected and Handled .......................................... 36
VMware ESXi Host Log Persistent Compliance .............................................. 37
Prerequisites............................................................................................... 37
Create a VMware ESXi Host Log Persistent Compliance Policy .................... 37
How Endpoints are Detected and Handled ................................................... 39

VMware ESXi Host Profile Compliance ......................................................... 40
Prerequisites............................................................................................... 41
Create a VMware ESXi Host Profile Compliance Policy ................................. 41
How Endpoints are Detected and Handled ................................................... 43

VMware Low Usage Virtual Machines Template ............................................ 44
Prerequisites............................................................................................... 44
Create a VMware Low Usage Virtual Machines Policy .................................. 45
How Endpoints are Detected and Handled ................................................... 47

VMware Tools Compliance Template .......................................................... 48
Prerequisites............................................................................................... 48
Create a VMware Tools Compliance Policy .................................................. 48
How Endpoints are Detected and Handled ................................................... 51

VMware VM CPU Ready Template .............................................................. 53
Prerequisites............................................................................................... 53
Create the VMware VM CPU Ready Policy ................................................... 54
Sub-Rules ..................................................................................................... 54

VMware Disk Highest Latency Template ....................................................... 54
Prerequisites............................................................................................... 54
Create a VMware Disk Highest Latency Policy .............................................. 55
Sub-Rules ..................................................................................................... 55

VMware VM Disk Usage Template ............................................................... 55
Prerequisites............................................................................................... 56
Create a VMware VM Disk Usage Policy ...................................................... 56
Sub-Rules ..................................................................................................... 56

VMware Virtual Machines by ESXi Server Template ....................................... 57
Prerequisites............................................................................................... 57
Create a VMware Virtual Machines by ESXi Server Policy ............................ 57
Main Rule .................................................................................................... 59

Create Custom VMware vSphere Policies ..................................................... 60
Properties ..................................................................................................... 60
Actions ......................................................................................................... 61
VMware vSphere Plugin Properties and Actions .......................................... 61

Detect Virtual Devices – Host Properties ..................................................... 61
VMware vSphere Advanced Properties ......................................................... 62
VMware Guest OS Properties ..................................................................... 64
VMware vSphere Server Properties ............................................................. 64
VMware Virtual Machine Properties ........................................................... 66
Display IPv6 Addresses ............................................................................. 67

Manage Virtual Devices – Policy Actions ..................................................... 67

Use the VMware vSphere Plugin ................................................................. 69
Access the Asset Inventory ........................................................................... 69
View Advanced Properties .......................................................................... 70
Review Admission Events ........................................................................... 71
Hybrid Cloud Module Information ................................................................. 72

Additional Forescout Documentation .............................................................. 73
  Documentation Downloads ............................................................................. 73
  Documentation Portal .................................................................................. 74
  Forescout Help Tools .................................................................................... 74
About VMware vSphere Integration

The VMware vSphere® Plugin is a component of the Forescout® Hybrid Cloud Module. See Hybrid Cloud Module Information for details about the module.

Forescout integration with VMware vSphere brings the detailed visibility, control, and compliance capabilities of the Forescout platform to virtualized data center environments. Flexible policy capabilities over campus endpoints are now extended to VMware ESXi™ hosts and virtual machines (VM) in the data center. This includes:

- Visibility into ESXi™ hosts and associated guest VMs with granular detail into various ESXi™ and guest operating system properties.
- Additional inspection of virtual servers through the use of agentless remote inspection or agent-based Secure Connector.
- Control policies over virtual machine state and network access similar to those applied to campus endpoints.

About Certification Compliance Mode

Forescout Hybrid Cloud Module: VMware vSphere Plugin supports Certification Compliance mode. For information about this mode, refer to the Forescout Installation Guide.

Use Cases

This section describes the use cases supported by this module. Be sure to review Concepts, Components, Considerations.

Data Center Visibility

The Forescout platform collects a range of virtual machine properties from vSphere environments to help enterprise IT gain greater data center visibility. This includes context, from basic virtual machine operating system properties to the more advanced virtual machine port group properties. This integration also allows the Forescout platform to recognize an ESXi™ host and associated virtual machines without needing to rely on other Forescout discovery and classification services (for example, span ports for data center traffic).

Regarding visibility of ESXi hosts, the Forescout platform can gather a range of operational context directly from the vCenter Server managing individual ESXi hosts. This includes the option to collect context from multiple vCenter Server environments.

Regarding visibility of guest virtual machines, the Forescout platform can gather insight into what is lost through the abstraction of the virtual layer as well as some properties that are not readily available from physical systems by default. The Forescout platform can gather guest properties related to resources, state, port group, operating system, and health, even if the guest is currently offline or is unreachable due to routing or a security block to the managing CounterACT® Appliance. Additionally, the Operating System classification property captured
through this integration is leveraged by the Device Profile Library Plugin to assist with primary classification conditions. See VMware Classification Template.

**Data Center Assessment & Compliance**

When moving from visibility to assessment and compliance, some ESXi and virtual machine properties are already collected, for example, host profile compliance and host firewall enablement. Beyond these, a range of different policy goals over the data center virtual environment can be enabled.

When addressing VMware ESXi or vCenter servers, properties to consider are:

- Orphaned guest virtual machines
- Server software version
- SSH service running
- Account lockout failure
- Non-standard configurations

Regarding the operating systems of guest virtual machines, one could look at VMware Tools or the correlation of the system with its port group. For additional inspection, agentless remote inspection or agent-based Secure Connector can be used. To move beyond this, VMware NSX® Security Groups provide the ability to limit the exposure of systems based on operational and security goals established within your corporate policy. See Work with VMware vSphere Policy Templates and VMware vSphere Advanced Properties.

**Data Center Control**

Taking a step beyond assessment and compliance, the Forescout platform can send non-affecting notifications via email or SIEM messages, and gradients up to and including a heavy-handed port group move or suspension of virtual machines. When looking at the progression of inform/remediate/restrict, the options in the low- to middle-levels of risk are usually where most customers find a good balance.

Sending informational *take action* messages to virtual systems administrators should be a part of your business operating procedure. This should involve reviewing orphaned guests for deletion and/or archival. Remediation is common among user systems and should be used in some cases to assist with automating tasks that would otherwise be cumbersome to add on to a system administrator. Finally, instead of doing a port group move, restrict by applying a Security Group using the Hybrid Cloud Module: VMware NSX Plugin. This provides extra security similar to ACLs on physical networking equipment, with little impact on the system and services that are necessary for business operations. See Review Admission Events.
Additional VMware Documentation

You should be familiar with virtualization concepts and the VMware environment in particular when working with this plugin. Installation, configuration, and general guides can be found at: https://www.vmware.com/support/pubs/

About this Plugin

The Forescout VMware vSphere Plugin can communicate directly with a VMware ESXi server or with VMware vCenter Server® in a VMware environment to retrieve information on virtual machines hosted on an ESXi host or those managed by a particular vCenter instance and to apply actions on them. The plugin lets you configure multiple vCenter and ESXi instances.

The plugin provides policy templates, inventory detections, as well as host properties and actions that are relevant to virtual endpoints and environments.

Concepts, Components, Considerations

This section provides a basic overview of the Forescout and vSphere platforms that are involved in integration and typical deployment architectures.

The two simplest deployments of CounterACT Appliances in a vSphere environment are:

- One-to-one mapping of CounterACT Appliances to vSphere segments
- Mapping to VMware vCenter or ESXi servers

In either case, the recommended model assigns one CounterACT Appliance to each VMware server, given the potential for virtual machine growth to exceed the capacity of the connecting CounterACT Appliance. The CounterACT Appliance manages the IP addresses associated with that VMware server. This design scales easily. For example, as more VMware servers are introduced, additional CounterACT Appliances are added or defined as connecting Appliances to match endpoint volume.

One CounterACT Appliance can connect to multiple VMware servers. This type of deployment model is applicable in smaller VMware environment where the total number of virtual machines across all VMware servers would never exceed the endpoint capacity of the CounterACT Appliance. Given the potential for enterprise virtualization growth within today’s dynamic data center environments, Forescout recommends extreme caution when implementing the single CounterACT Appliance to many VMware server deployment model.
What to Do

This section describes the steps you should take to set up your system when integrating with VMware environments:

1. Verify that system requirements are met. See Requirements.
2. Review the Concepts, Components, Considerations.
3. Define Forescout Users in the VMware Environment.
4. Configure the Plugin.
5. Work with VMware vSphere Policy Templates.
6. Use the VMware vSphere Plugin to manage virtual devices.

Requirements

This section describes system requirements, including:

- Forescout Requirements
- Networking Requirements
- Supported Vendor Requirements

Forescout Requirements

The plugin requires the following Forescout releases and other components:

- Forescout version 8.1.2.
- Hybrid Cloud Module version 2.0.1, with the VMware vSphere component running.
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the Forescout Flexx Licensing How-to Guide for more information about managing Flexx licenses.

Networking Requirements

If the Forescout platform and the VMware vCenter server are not in the same location, the following ports must be open on enterprise firewalls to support communication between them:

- 443/TCP

Supported Vendor Requirements

- VMware vSphere® version 5.5, 6.0, 6.5, and 6.7
- The following VMware licenses:
  - VMware vSphere® Enterprise Plus Edition™
  - VMware vCenter® Server (standard)
About Support for Dual Stack Environments

Forescout version 8.1 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, communication from the vSphere Plugin to a vCenter Server or ESXi host only supports IPv4. IPv6 communication is not supported by the vSphere Plugin.

Define Forescout Users in the VMware Environment

The plugin communicates with ESXi or vCenter servers to retrieve information on virtual machines, and to apply actions to them. Before you configure and test this connection in the Forescout platform, define a user or group of users with the required permissions in the VMware environment. The plugin uses these credentials to log in to VMware servers. Define these users as follows:

- Define a vSphere user role that includes the permissions required by the Forescout platform.
- Define users and assign this role to them.

Details on configuring roles and users can be found in the vSphere Security Guide. Specific steps required to create a user for the Forescout platform are provided below.

Define a vSphere Role

This section describes how to define a vSphere user role that includes the permissions required by the Forescout platform in the VMware environment.

To define a user role for Forescout users in VMware:

1. Log in to vSphere as an administrator.
2. In the Administration area of the vSphere Client console, select Roles.


4. Enter a name for the new role, and enable the following privileges required by the Forescout platform:
   - Virtual Machine.Interaction.VMware Tools install (VMware Tools™ Install)
   - Virtual Machine.Interaction.Power off
   - Virtual Machine.Interaction.Power on
   - Virtual Machine.Interaction.Reset
   - Virtual Machine.Interaction.Suspend
   - Virtual Machine.Interaction.Device connection
   - Virtual Machine.Configuration.Modify device settings
   - Network.Assign network
5. Select OK to save the role.

Define Users with a Forescout Role

This section describes how to define users with a Forescout role in the VMware environment.

To define users with a Forescout role:

1. In the Inventory area of the vSphere Client console, select VMs and Templates.

   A directory window lists the datastore objects of the vSphere environment.

2. In the left pane, select the vCenter or ESXi server that you plan to configure in the Forescout platform.
3. In the right pane, select the Permissions tab. Then right-click in the Permissions pane and select **Add Permissions**.

![Assign Permissions](image)

4. Assign the role you defined for Forescout users to a new or existing user.

5. Record the login credentials of users that are assigned the Forescout role. (You enter these credentials in the Forescout platform when you configure the plugin.)

6. Repeat for additional users and roles until users are defined that allow the Forescout platform to query all servers in the VMware environment that you want to configure. See [Define a vSphere Role](#) for details.

---

### Define Users with Read-Only Permissions

This section describes how to define users with read-only permissions. With read-only permissions, users can discover VMs, but cannot perform actions.

**To define users with read-only permissions:**

1. Select **Edit Role** and create a role with no privileges.
2. Select **Assign Permissions** and assign the role to a user.

3. Configure the user in the Forescout VMware Plugin.
Configure the Plugin

This section describes the steps required to configure the VMware vSphere Plugin.

- **Define Target ESXi Host or vCenter Server**
- **Add VMware Advanced Properties**
- **Error! Reference source not found.**

Define Target ESXi Host or vCenter Server

You need to map CounterACT Appliances to a VMware server. Each CounterACT device communicates with a single VMware server. If you define more than one VMware server, you can assign individual CounterACT Appliances to each VMware server.

Removing a configured VMware server stops host discovery and property learning for virtual machines hosted by this server, but any actions remain enabled.

To define the ESXi host or vCenter server:

1. In the Console, select **Options** from the **Tools** menu.
2. In the left pane, select **VMware vSphere**. The VMware vSphere pane opens to the VMware Server tab.

3. Select **Add**.

4. Define the following server parameters.

<table>
<thead>
<tr>
<th>VMware Server FQDN or IP Address</th>
<th>Enter a Fully Qualified Domain Name (FQDN) or IPv4 address of the VMware server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Type</strong></td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td>- <strong>ESXi</strong> - Through the ESXi virtualization platform, you run the virtual machines, run applications, and configure the virtual machines.</td>
</tr>
<tr>
<td></td>
<td>- <strong>vCenter</strong> - Through the vCenter Server, you can leverage authentication and permission management. A vCenter Server can have its own types of events, tasks, metadata, and privileges.</td>
</tr>
</tbody>
</table>
| **Validate Server Certificate** | Select this option to validate the identity of the third-party server before establishing a connection, when the Plugin communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:

- Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance
- Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance

Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the Forescout Administration Guide. |
| **Username** | Enter the username required to log in to the server. |
| **Password** | Enter the password required to log in to the server. |
| **Verify Password** | Re-enter the password to verify it. |
| **Connecting CounterACT Device** | Select the CounterACT device to connect to this server. The specified CounterACT device is the only device that communicates with the server. When the Enterprise Manager is defined as the Connecting CounterACT Device, endpoints without an IP address detected by the plugin are not displayed in the Console Detections pane. To manage endpoints without an IP address, the Connecting CounterACT Device must be an Appliance, and not the Enterprise Manager. |
| **Comment** | (Optional) Insert text, for example, the name of the VMware vSphere server. |

5. Select **Next**.
6. Define the following advanced settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Full Poll Interval (minutes) | Specify how frequently the VMware Plugin runs a full poll of the VMware server.  
  - Minimum interval - 60 minutes  
  - Maximum Interval - 2880 seconds (48 hours)  
  - Default interval - 360 minutes |
| Delta Poll Interval (minutes)| Specify how frequently the VMware Plugin gets the Virtual Machine property updates since the last poll.  
  - Minimum interval - 1 minute  
  - Maximum interval - 30 minutes  
  - Default interval - 1 minute |
| Performance Data Poll Interval (minutes) | Specify how frequently the VMware Plugin gets the CPU, network and disk usages of the Virtual Machines.  
  - Minimum interval - 30 minutes  
  - Maximum interval - 1440 minutes (24 hours)  
  - Default interval - 60 minutes |
| Performance Measurement Period (2 - 2880 hours) | Specify a period of time in the past for which the performance metrics of the Virtual Machines are to be returned. For example, the default interval is 48 hours. This means that the past 48 hours of data are polled. |
Virtual CounterACT VMs Only  
By default, the plugin will discover for ALL VMs associated with an ESXi Host or a vCenter Server, and then resolve them to the Forescout platform at the end of each poll. When this option is selected, the plugin will only discover/resolve VMs detected as CounterACT virtual appliance (vCT) VMs. This is useful in cases where vCT VMs are on the VMware server with other non-CounterAct VMs, but only data related to vCT VMs is desired.

Enable Virtual Machine CPU Ready %  
The Virtual Machine CPU Ready % property, by default, will only be calculated and resolved for VMs detected as vCT VMs. The property can be calculated and resolved for any other VM by both selecting this option and by using this property in a policy.

Enable Virtual Machine CPU Usage %  
The Virtual Machine CPU Usage % property, by default, will only be calculated and resolved for VMs detected as vCT VMs. The property can be calculated and resolved for any other VM by both selecting this option and by using this property in a policy.

Enable Virtual Machine Disk Usage %  
The Virtual Machine Disk Usage % property, by default, will only be calculated and resolved for VMs detected as vCT VMs. The property can be calculated and resolved for any other VM by both selecting this option and by using this property in a policy.

Enable Virtual Machine Disk Highest Latency  
The Virtual Machine Disk Highest Latency property, by default, will only be calculated and resolved for VMs detected as vCT VMs. The property can be calculated and resolved for any other VM by both selecting this option and by using this property in a policy.

Enable Virtual Machine Memory Usage %  
The Virtual Machine Memory Usage % property, by default, will only be calculated and resolved for VMs detected as vCT VMs. The property can be calculated and resolved for any other VM by both selecting this option and by using this property in a policy.

This version of the vSphere Plugin was enhanced to assist troubleshooting CounterACT virtual appliance (vCT) deployments. By default, the last five properties above are always being calculated and resolved for VMs detected as CounterACT virtual appliances (vCTs). To expose these values in the Forescout platform, define specific policies for these properties and then apply these policies to the segments that cover the vCTs.

7. Select Finish.
Add VMware Advanced Properties

VMware Advanced Properties are static and dynamic properties that can be added to secure the deployments of VMs and ESXi hosts. For details, refer to the VMware vSphere Security Hardening Guide. These properties can be added at any time.

Once a property is added, it can be used within a policy to determine whether the property has the correct value or not. If the property does not have the desired value for an ESXi host or virtual machine, it is recommended to address it as the configuration is considered unsecure.

1. In the VMware vSphere pane, select the Advanced Property tab.

2. Select Add.

3. Define the following property parameters.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name of the VMware property. The valid characters are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Alphabet</td>
</tr>
<tr>
<td></td>
<td>- Numerical</td>
</tr>
<tr>
<td></td>
<td>- Underscore</td>
</tr>
<tr>
<td></td>
<td>- Punctuation: period, comma, hyphen, and space.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>(Optional) Enter a description of the property. The valid characters are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Alphabet</td>
</tr>
<tr>
<td></td>
<td>- Numerical</td>
</tr>
<tr>
<td></td>
<td>- Underscore</td>
</tr>
<tr>
<td></td>
<td>- Punctuation: period, comma, hyphen, and space.</td>
</tr>
</tbody>
</table>
**VMware Advanced Option Name**
Enter the name of the advanced property. The valid characters are:
- Alphabet
- Numerical
- Underscore
- Punctuation: period, comma, hyphen, and space.
See [VMware vSphere Advanced Properties](#).

**VMware Advanced Option Data Type**
Select a data type for the property. The supported data types are:
- Boolean
- String
- Integer

**VMware Advanced Option Type**
Select the type of virtual endpoint:
- **ESXi**
- **Virtual Machine**

4. Select **Next**.

5. Define the following advanced properties.

<table>
<thead>
<tr>
<th><strong>Display in Inventory</strong></th>
<th>Select this option if you want this dynamic property to display in the Inventory view.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Enter a description of the property.</td>
</tr>
</tbody>
</table>

6. Select **Finish**.

The properties are displayed in the Conditions dialog box and can be used in your policies. For information about adding dynamic properties, see [VMware vSphere Advanced Properties](#).

The best practice is to perform a **Test** after setting up a connection. See [Test the VMware Connection](#).
Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

7. Select **Tools > Options** and then select **Modules**.
8. Navigate to the plugin and select **Start** if the plugin is not running.

Test the VMware Connection

You can test the plugin communication with a VMware server.

To test communication:

1. In the VMware vSphere pane, select a VMware server defined in the Forescout platform.
2. Select **Test**. Using your configured settings, the Forescout platform attempts to connect to the server.
   - When you test an ESXi server, the test confirms connectivity and returns the number of virtual endpoints managed by the server.
   - When you test a vCenter server, the test confirms connectivity and returns the total number of virtual endpoints managed by the server and its managed ESXi servers. In addition, the test lists the IP address of each ESXi server managed by the vCenter server.

View the VMware vSphere Connection

The VMware vSphere pane shows all vCenter and ESXi instances that you have defined in the Forescout platform. The **Connectivity Status** column indicates the status of each VMware server.
The following Connectivity Status values are reported:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>Select Apply in the VMware vSphere configuration pane to save this server definition.</td>
</tr>
<tr>
<td>Down</td>
<td>The Forescout platform cannot connect to the server.</td>
</tr>
<tr>
<td>Up</td>
<td>The Forescout platform can connect to the server.</td>
</tr>
<tr>
<td>Managed</td>
<td>This server is managed by a vCenter server in your environment that is not defined in the Forescout platform.</td>
</tr>
<tr>
<td></td>
<td>The Forescout platform queries the ESXi server for information about endpoints managed by the ESXi server, as for a standalone ESXi.</td>
</tr>
<tr>
<td>Not Used</td>
<td>The Forescout platform learns of endpoints managed by this server when it queries the parent vCenter server. Delete this entry from the list of</td>
</tr>
<tr>
<td></td>
<td>servers.</td>
</tr>
<tr>
<td></td>
<td>The Forescout platform does not query this ESXi directly as long as its managing vCenter server is defined in the Forescout platform.</td>
</tr>
<tr>
<td>General Error</td>
<td>Other issues interfere with server interaction.</td>
</tr>
<tr>
<td>Login Error</td>
<td>The server did not recognize the login credentials defined for this server.</td>
</tr>
<tr>
<td>Plugin Error</td>
<td>The VMware Plugin is not running on the connecting CounterACT device specified for this server.</td>
</tr>
</tbody>
</table>

**Work with VMware vSphere Policy Templates**

Policy templates help you quickly create important, widely-used policies that easily control endpoints and can guide users to compliance. These policies can be viewed in the Console’s Policy Manager.

Policies use a wide range of host conditions to trigger various management and remediation actions. When the conditions of the policy are met, the actions are implemented. For example, the Forescout VMware vSphere Plugin can run a policy that checks if a virtual machine is anti-virus compliant.
Predefined actions – instructions regarding how to handle endpoints – are generally disabled by default when working with templates. You should only enable actions after testing and fine-tuning the policy.

This plugin provides the following policy templates used to detect, manage, and remediate ESXi hosts and virtual machine endpoints.

- **VMware Classification Template** – generates a policy that detects and classifies different types of VMware virtual machines and servers.
- **VMware ESXi Host Firewall Compliance** – generates a policy that checks the firewall compliance of the ESXi host.
- **VMware ESXi Host Lockdown Compliance** – generates a policy that checks whether the ESXi host is in lockdown compliance.
- **VMware ESXi Host Log Persistent Compliance** – generates a policy that checks whether the ESXi host is log persistent compliance.
- **VMware ESXi Host Profile Compliance** – generates a policy that checks if the ESXi host is configured with a host profile, and whether it is compliant.
- **VMware Low Usage Virtual Machines Template** – generates a policy that lists all virtual machines using low CPU, and network I/O usage.
- **VMware Tools Compliance Template** – generates a policy that detects and remediates virtual machines that are not running an updated version of VMware Tools.
- **VMware VM CPU Ready Template** – generates a policy that monitors performance through the VMware VM CPU Ready status by percentage.
- **VMware Disk Highest Latency Template** – generates a policy that monitors the highest latency on the VMware VM Disk.
- **VMware VM Disk Usage Template** – generates a policy that monitors the VMware VM Disk Usage as a percentage of total available disk space.
- **VMware Virtual Machines by ESXi Server Template** – generates a policy that detects virtual machines hosted by a specific ESXi server.
It is recommended that you have a basic understanding of policies before working with the templates. Refer to the Forescout Templates and Policy Management chapters of the Forescout Administration Guide.

VMware Classification Template

Use this template to identify and classify VMware servers and virtual machines.

Prerequisites

Before you run a policy based on this template, verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers.

Create a VMware Classification Policy

This section describes how to create a policy based on the VMware Classification Policy template.

To create the policy:

1. In the Console, select Policy.
3. Select **VMware vSphere** and then select **VMware Classification**.

4. Select **Next**.

5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as `My_Compliance_Policy`.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria needs to be met or not.
   - Avoid having another policy with a similar name.
Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

6. Select Next. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.

![IP Address Range dialog box]

The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.

- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box, and select Segments from the Scope pane.

- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select OK. The added range is displayed in the Scope pane.


10. Review the sub-rule conditions and actions, and then select Finish.

11. In the Policy Manager, select Apply to save the policy.

12. Select Start to execute the policy.

**How Endpoints are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.
Sub-Rules

There is no main rule in the default policy. Sub-rules of the policy evaluate the endpoint to identify whether it is a virtual machine, VMware ESXi server or VMware vCenter server. Sub-rule actions are enabled by default.

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

The default sub-rules for this policy template are:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Virtual Machine</td>
<td>This rule matches endpoints with any of the following values:</td>
</tr>
<tr>
<td></td>
<td>▪ Virtual Machine Name – Any Value</td>
</tr>
<tr>
<td></td>
<td>▪ NIC Vendor – VMWARE, INC</td>
</tr>
<tr>
<td></td>
<td>▪ Device Interfaces – Starts With: VMware Accelerated</td>
</tr>
<tr>
<td></td>
<td>The Add to Group action adds detected endpoints to the VMware virtual machines group. This action is enabled by default.</td>
</tr>
<tr>
<td>VMware ESXi Server</td>
<td>This rule matches endpoints with VMware Server Product ID list values of gsx,</td>
</tr>
<tr>
<td></td>
<td>embeddedEsx and esx.</td>
</tr>
<tr>
<td></td>
<td>The Add to Group action adds detected endpoints to the VMware ESXi Servers group.</td>
</tr>
<tr>
<td></td>
<td>This action is enabled by default.</td>
</tr>
<tr>
<td>VMware vCenter Server</td>
<td>This rule matches endpoints with VMware Server Product ID values of vpx.</td>
</tr>
<tr>
<td></td>
<td>The Add to Group action adds detected endpoints to the VMware ESXi Servers group.</td>
</tr>
<tr>
<td></td>
<td>This action is enabled by default.</td>
</tr>
</tbody>
</table>
Refer to the Forescout Administration Guide for details on the icons in the Actions column.

VMware ESXi Host Firewall Compliance

The VMware ESXi Host Firewall Compliance policy template checks the ESXi host firewall compliance.

Use this template to create a policy that checks the firewall compliance of the ESXi host.

Prerequisites

Before you run a policy based on this template, verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers.

Create a VMware ESXi Host Firewall Compliance Policy

This section describes how to create a policy based on the VMware ESXi Host Firewall Compliance policy template.

To create the policy:

1. In the Console, select Policy.
3. Select VMware vSphere and then select VMware ESXi Host Firewall Compliance.
4. Select **Next**.

5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria needs to be met or not.
   - Avoid having another policy with a similar name.
Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

6. Select Next. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.

The following options are available:
- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box, and select Segments from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select OK. The added range is displayed in the Scope pane.
9. Select Next. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See How Endpoints are Detected and Handled for details of default policy logic.
10. Review the sub-rule conditions and actions, and then select Finish.
11. In the Policy Manager, select Apply to save the policy.
12. Select Start to execute the policy.

**How Endpoints are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. Endpoints that do not match this rule are not inspected for this policy. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.
Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

By default, this template only inspects endpoints that are members of the VMware virtual machines group.

**Sub-Rules**

The sub-rules of the policy identify if the host server is security-compliant. Sub-rule actions are enabled by default.

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Disabled</td>
<td>This rule checks if the firewall on the VMware host is disabled.</td>
</tr>
</tbody>
</table>

**VMware ESXi Host Lockdown Compliance**

The VMware ESXi Host Lockdown Compliance policy template checks whether the ESXi host lockdown mode is compliant. Hosts are compliant if VMware lockdown mode is enabled on the ESXi host.
Prerequisites

Before you run a policy based on this template, verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers.

Create a VMware ESXi Host Lockdown Compliance Policy

This section describes how to create a policy based on the VMware ESXi Host Lockdown Compliance Policy template.

To create the policy:

1. In the Console, select Policy.
3. Select VMware vSphere and then select VMware ESXi Host Lockdown Compliance.
4. Select Next.
5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria needs to be met or not.
   - Avoid having another policy with a similar name.

   Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

6. Select Next. Both the Scope pane and the IP Address Range dialog box open.

7. Use the IP Address Range dialog box to define which endpoints are inspected.

The following options are available:
   - **All IPs**: Include all IP addresses in the Internal Network.
− **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box, and select Segments from the Scope pane.

− **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select OK. The added range is displayed in the Scope pane.

9. Select Next. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See How Endpoints are Detected and Handled for details of default policy logic.

10. Review the sub-rule conditions and actions, and then select Finish.

11. In the Policy Manager, select Apply to save the policy.

12. Select Start to execute the policy.

**How Endpoints are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

By default, this template only inspects endpoints that are members of the VMware virtual machines group.

**Sub-Rules**

The sub-rules of the policy identify if the host server is security-compliant. Sub-rule actions are enabled by default.

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.
The default sub-rules for this policy template are:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lockdown Disabled</td>
<td>This rule checks if the VMware host capability to lockdown is disabled.</td>
</tr>
</tbody>
</table>

**VMware ESXi Host Log Persistent Compliance**

The VMware ESXi Host Log Persistent Compliance policy template checks if the ESXi host log persistent is compliant. Hosts are compliant if the ESXi host log is configured on a datastore or a persistent scratch location.

**Prerequisites**

Before you run a policy based on this template, verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers.

**Create a VMware ESXi Host Log Persistent Compliance Policy**

This section describes how to create a policy based on the VMware ESXi Host Log Persistent Compliance policy template.

To create the policy:

1. In the Console, select **Policy**.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware vSphere** and then select **VMware ESXi Host Log Persistent Compliance**.

4. Select **Next**.

5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as `My_Compliance_Policy`.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
− Ensure that the name indicates whether the policy criteria needs to be met or not.
− Avoid having another policy with a similar name.

Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

6. Select Next. Both the Scope pane and the IP Address Range dialog box open.

7. Use the IP Address Range dialog box to define which endpoints are inspected.

![IP Address Range dialog box](image)

The following options are available:

− **All IPs**: Include all IP addresses in the Internal Network.
− **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box, and select **Segments** from the Scope pane.
− **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select OK. The added range is displayed in the Scope pane.

9. Select Next. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See **How Endpoints are Detected and Handled** for details of default policy logic.

10. Review the sub-rule conditions and actions, and then select Finish.

11. In the Policy Manager, select Apply to save the policy.

12. Select Start to execute the policy.

**How Endpoints are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.
Endpoints that match the Main Rule are included in the policy inspection. Endpoints that do not match this rule are not inspected for this policy. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

By default, this template only inspects endpoints that are members of the VMware virtual machines group.

**Sub-Rules**

The sub-rules of the policy identify if the host server is security-compliant. Sub-rule actions are enabled by default.

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

The default sub-rules for this policy template are:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Log Not Persistent</td>
<td>This rule checks if the VMware persistent log is not configured.</td>
</tr>
</tbody>
</table>

**VMware ESXi Host Profile Compliance**

Use this template to create a policy that checks if the ESXi host profile is compliant. The VMware host profile compliance states are: compliant, non-compliant, and unknown.
Prerequisites

Before you run a policy based on this template, verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers.

Create a VMware ESXi Host Profile Compliance Policy

This section describes how to create a policy based on the VMware ESXi Host Profile Compliance policy template.

To create the policy:

1. In the Console, select Policy.
3. Select VMware and then select VMware ESXi Host Profile Compliance.
4. Select Next.
5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria needs to be met or not.
   - Avoid having another policy with a similar name.

   Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

6. Select Next. Both the Scope pane and the IP Address Range dialog box open.

7. Use the IP Address Range dialog box to define which endpoints are inspected.

   The following options are available:
   - All IPs: Include all IP addresses in the Internal Network.
   - Segment: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box, and select Segments from the Scope pane.
Unknown IP addresses: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select OK. The added range is displayed in the Scope pane.

9. Select Next. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See How Endpoints are Detected and Handled for details of default policy logic.

10. Review the sub-rule conditions and actions, and then select Finish.

11. In the Policy Manager, select Apply to save the policy.

12. Select Start to execute the policy.

How Endpoints are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. Endpoints that do not match this rule are not inspected for this policy. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

By default, this template only inspects endpoints that are members of the VMware Virtual Machines group.

Sub-Rules

Sub-rules of the policy evaluate the endpoint to identify whether it is a virtual machine, VMware ESXi server or VMware vCenter server. Sub-rule actions are enabled by default.

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.
The default sub-rules for this policy template are:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Profile Compliant</td>
<td>Checks if the server host profile compliance status is Compliant.</td>
</tr>
<tr>
<td>Host Profile Not Compliant</td>
<td>Checks if the server host profile compliance status is Non-Compliant.</td>
</tr>
<tr>
<td>Host Profile Unknown</td>
<td>Checks if the server host profile compliance status is Unknown.</td>
</tr>
</tbody>
</table>

**VMware Low Usage Virtual Machines Template**

Use this template to detect low usage and orphan virtual machines. A Virtual Machine is orphaned if the VM is found in the vCenter server but no longer exists on an ESXi host. A Virtual Machine has low usage if:

- Virtual Machine Usage CPU (one-thousandth) has a value from 0-10
- Virtual Machine Usage Disk I/O (KBps) has value from 0-20
- Virtual Machine Usage Network I/O (KBps) has value from 0-10

The VM performance is calculated as an average over a certain period of time. This performance time period can be setup during the VMware vCenter configuration using the Performance Measurement Period in Hours field.

**Prerequisites**

Before you run a policy based on this template, verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers.
Create a VMware Low Usage Virtual Machines Policy

This section describes how to create a policy based on the Low CPU and I/O Usage VMs policy template.

To create the policy:
1. In the Console, select Policy.
3. Select VMware vSphere and then select VMware Low Usage Virtual Machines.
4. Select Next.
5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria needs to be met or not.
   - Avoid having another policy with a similar name.

   *Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.*

6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.

The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is displayed in the Scope pane.
9. Select **Next**. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See [How Endpoints are Detected and Handled](#) for details of default policy logic.
10. Review the sub-rule conditions and actions, and then select **Finish**.
11. In the Policy Manager, select **Apply** to save the policy.
12. Select **Start** to execute the policy.
How Endpoints are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

By default, this template only inspects endpoints that are members of the VMware virtual machines group.

Sub-Rules

Sub-rules of the policy evaluate the endpoint to identify the orphan virtual machines and the low usage virtual machines. Sub-rule actions are enabled by default.

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orphan Virtual Machines</td>
<td>This rule checks if the VM is an orphan machine.</td>
</tr>
<tr>
<td>Low Usage</td>
<td>This rule checks the CPU usage level by the one-thousandth fraction. Also checks for disk input/output and network input/output.</td>
</tr>
</tbody>
</table>
VMware Tools Compliance Template

Use this template to create a policy that detects and remediates virtual machine endpoints that are not running an updated version of VMware Tools. The policy:

- Detects virtual machines running an outdated version of VMware Tools, and remediates them by via update.
- Detects virtual machines that are not running VMware Tools, and remediates them by initiating an install of the application.
- Detects virtual machines that are running VMware Tools, but are not managed correctly by vCenter server. The Forescout platform can notify the administrator by email of such endpoints.

You can add, delete, or modify the rules, conditions, and actions of the standard policy.

Prerequisites

Before you run a policy based on this template:

- Verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers.
- Verify that the VMware Virtual Machines group is displayed in the Console, Filters pane. If not, run the VMware Classification policy template to create this group. See VMware Classification Template for details.

Create a VMware Tools Compliance Policy

This section describes how to create a policy based on the VMware Tools Compliance template.

To create the policy:

1. In the Console, select Policy.
3. Select VMware vSphere and then select VMware Tools Compliance.
4. Select **Next**.

5. Define a unique name for the policy you are creating based on this template and enter a description.
   
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as *My_Compliance_Policy*.
   
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   
   - Ensure that the name indicates whether the policy criteria needs to be met or not.
   
   - Avoid having another policy with a similar name.

   *Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.*
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

7. Use the IP Address Range dialog box to define which endpoints are inspected.

   ![IP Address Range Dialog Box]

The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is displayed in the Scope pane.

   ![Scope Configuration]

   **Scope**
   
   Define the range of Hosts to be inspected for this policy.

   **Hosts inspected by the policy**
   
   - Segment
   - No Name Assigned
   - All IPs

   **Filter by Group**
   
   - Only inspect hosts from the following groups
   - VMware Virtual Machines
   - Template Group

   **Exceptions**
   
   - Do not inspect the following
   - No items to display
9. Select **Next**. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See **How Endpoints are Detected and Handled** for details of default policy logic.

10. Review the sub-rule conditions and actions, and then select **Finish**.

11. In the Policy Manager, select **Apply** to save the policy.

12. Select **Start** to execute the policy.

**How Endpoints are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

By default, this template only inspects endpoints that are members of the VMware virtual machines group.

**Sub-Rules**

Sub-rules of the policy evaluate the endpoint to identify whether it is a virtual machine, VMware ESXi server or VMware vCenter server. Sub-rule actions are enabled by default.

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.
The default sub-rules for this policy template are:

<table>
<thead>
<tr>
<th><strong>Sub-Rule Name</strong></th>
<th><strong>Condition Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Tools installed and up to date</td>
<td>This rule matches endpoints with VMware Tools Status value of VMware Tools is installed, and the version is correct. Matching endpoints are up to date, and no remediation action is applied.</td>
</tr>
<tr>
<td>VMware Tools installed and upgrade recommended</td>
<td>This rule matches endpoints with the following VMware Tools Status values:</td>
</tr>
<tr>
<td></td>
<td>▪ VMware Tools is installed, supported, and newer than the version available on the ESXi host.</td>
</tr>
<tr>
<td></td>
<td>▪ VMware Tools is installed, supported, but a newer version is available.</td>
</tr>
<tr>
<td></td>
<td>The Install/Upgrade VMware Tools action initiates upgrade of the VMware Tools application on detected endpoints. This action is disabled by default.</td>
</tr>
</tbody>
</table>
VMware Tools installed but needs updating

This rule matches endpoints with the following VMware Tools Status values:

- VMware Tools is installed, and the version is known to be too new to work correctly with this virtual machine.
- VMware Tools is installed, but the installed version is known to have a grave bug and should be immediately upgraded.
- VMware Tools is installed, but the version is not current.
- VMware Tools is installed, but the version is too old.

The Install/Upgrade VMware Tools action initiates upgrade of the VMware Tools application on detected endpoints. This action is disabled by default.

VMware tools installed but VM is unmanaged

This rule matches endpoints with VMware Tools Status value of VMware Tools is installed, but it is not managed by VMware.

The Send Email action notifies administrators that detected endpoints are unmanaged. This action is disabled by default.

VMware Tools not installed

This rule matches endpoints with VMware Tools Status value of VMware Tools has never been installed.

The Install/Upgrade VMware Tools action initiates installation of the VMware Tools application on detected endpoints. This action is disabled by default.

VMware VM CPU Ready Template

Use this policy to monitor the VMware VM CPU Ready percentage. CPU Ready percentage values approaching 5% indicate CPU resource contention and likely VM performance issues.

CPU ready values are categorized as:

Low – 0-2%, indicating very little CPU contention
Medium – 3-5%, indicating potential performance issues due to CPU contention
High – 6-100%, indicating performance issues due to CPU contention

Prerequisites

Before you run a policy based on this template, verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers.
Create the VMware VM CPU Ready Policy

This section describes how to create a policy based on the VMware VM CPU Ready template.

To create the policy:
1. From the Console, select Policy.
3. Select VMware vSphere and then select VMware VM CPU Ready.
4. Select Next. The Name pane opens.
5. Select Next. The Scope pane and IP address dialog box opens.
6. Select Next. The Sub-Rules pane opens. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See Sub-Rules.
7. Select Finish.

Sub-Rules

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline</td>
<td>NOT Host is online</td>
</tr>
<tr>
<td>Low</td>
<td>Virtual Machine CPU Ready (%): 0-2</td>
</tr>
<tr>
<td>Medium</td>
<td>Virtual Machine CPU Ready (%): 3-5</td>
</tr>
<tr>
<td>High</td>
<td>Virtual Machine CPU Ready (%): 6-100</td>
</tr>
<tr>
<td>Unknown</td>
<td>No Conditions</td>
</tr>
</tbody>
</table>

VMware Disk Highest Latency Template

Use this policy to track the highest latency on the VMware VM Disk. The Disk Highest Latency value represents the highest reported read or write latency for all disks associated with the corresponding VMware VM.

Disk highest latency values are categorized as:
Low – 0-10
Medium – 11-50
High – 51-999999

Prerequisites

Before you run a policy based on this template, verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers.
Create a VMware Disk Highest Latency Policy

This section describes how to create a policy based on the VMware Disk Highest Latency template.

To create the policy:

1. From the Console, select Policy.
3. Select VMware vSphere and then select VMware VM Disk Highest Latency.
4. Select Next. The Name pane opens.
5. Select Next. The Scope pane and IP address dialog box opens.
6. Select Next. The Sub-Rules pane opens. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See Sub-Rules.
7. Select Finish.

Sub-Rules

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline</td>
<td>NOT Host is online</td>
</tr>
<tr>
<td>Low</td>
<td>Virtual Machine Disk Highest Latency: 0-10</td>
</tr>
<tr>
<td>Medium</td>
<td>Virtual Machine Disk Highest Latency: 11-50</td>
</tr>
<tr>
<td>High</td>
<td>Virtual Machine Disk Highest Latency: 51-999999</td>
</tr>
<tr>
<td>Unknown</td>
<td>No Conditions</td>
</tr>
</tbody>
</table>

VMware VM Disk Usage Template

Use this policy to track VMware VM Disk Usage percentage. The Disk Usage percentage aligns with the Storage or Storage Usage value for a VM as displayed in the VMware vSphere Console.

Disk usage values are categorized as:

- Low – 0-60%
- Medium – 61-80%
- High – 81-100%
Prerequisites

Before you run a policy based on this template, verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers.

Create a VMware VM Disk Usage Policy

This section describes how to create a policy based on the VMware VM Disk Usage template.

To create the policy:

1. From the Console, select Policy.
3. Select VMware vSphere and then select VMware VM Disk Usage.
4. Select Next. The Name pane opens.
5. Select Next. Both the Scope pane and the IP Address Range dialog box open.
6. Select Next. The Sub-Rules pane opens. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See Sub-Rules.
7. Select Finish.

Sub-Rules

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline</td>
<td>NOT Host is online</td>
</tr>
<tr>
<td>Low</td>
<td>Virtual Machine Disk Usage (%): 0-60</td>
</tr>
<tr>
<td>Medium</td>
<td>Virtual Machine Disk Usage (%): 61-80</td>
</tr>
<tr>
<td>High</td>
<td>Virtual Machine Disk Usage (%): 81-100</td>
</tr>
<tr>
<td>Unknown</td>
<td>No Conditions</td>
</tr>
</tbody>
</table>
VMware Virtual Machines by ESXi Server Template

Use this template to create a policy that detects virtual machines that are hosted by a specified ESXi server. You can add, delete, or modify the rules, conditions, and actions of the standard policy.

Prerequisites

Before you run a policy based on this template, verify that you have configured the plugin so that the Forescout platform can communicate with one or more VMware servers. See Configure the Plugin for details.

Create a VMware Virtual Machines by ESXi Server Policy

This section describes how to create a policy based on the VMware Virtual Machines by ESXi Server template.

To create the policy:

1. In the Console, select Policy.
3. Select VMware vSphere and then select VMware Virtual Machines by ESXi Server.
4. Select Next.
5. Define a unique name for the policy you are creating based on this template and enter a description.
   - To create a unique, descriptive policy name, specify the target ESXi server in the policy name.

   *Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.*

6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

7. Use the IP Address Range dialog box to define which endpoints are inspected.

   The following options are available:
   - **All IPs**: Include all IP addresses in the Internal Network.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
   - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **Next** and then specify the ESXi server used by the policy to match endpoints. The policy only detects virtual machine endpoints that reside on the specified server.

9. In the **ESXi Server Name** field, enter an individual server name of an ESXi server defined in the plugin configuration screen. See [Configure the Plugin](#).

10. Select **Next**. The Main Rule pane lists the main rule of the policy generated by the template. There are no sub-rules in the default policy. For details, see [Main Rule](#).

11. Review the rule conditions and actions, and then select **Finish**.

12. In the Policy Manager, select **Apply** to save the policy.

13. Select **Start** to execute the policy.

**Main Rule**

Rules of the policy evaluate the endpoint to identify whether it is a virtual machine, VMware ESXi server or VMware vCenter server. The rule actions are enabled by default.

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.
The default rule for this policy template is:

<table>
<thead>
<tr>
<th>Main Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi Server Name</td>
<td>This rule matches endpoints with the VMware ESXi Server name. If the ESXi Server name matches correctly, no remediation action is applied.</td>
</tr>
</tbody>
</table>

Create Custom VMware vSphere Policies

Custom policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy to instruct the Forescout platform to apply a policy action to hosts that match (or do not match) conditions based on host property values. You may need to create a custom policy to deal with issues not covered in the policy templates provided by this plugin.

Properties

Policy properties let you instruct the Forescout platform to detect hosts with specific attributes. For example, create a policy that instructs the Forescout platform to detect hosts running a certain operating system or with a certain application installed.
**Actions**

Policy actions let you instruct the Forescout platform to control detected devices. For example, assign a detected device to a quarantined VLAN or send the device user or IT team an email.

**VMware vSphere Plugin Properties and Actions**

This plugin provides additional properties and actions that are useful for virtual device management. Use these properties and actions to construct customized policies for virtual device management.

For more information about creating custom policies, refer to the *Forescout Administration Guide*. See *Additional Forescout Documentation* for information on how to access this guide.

**Detect Virtual Devices – Host Properties**

This section describes the host properties that are available when the VMware vSphere Plugin is installed.

*All VMware properties can be learned through policy resolution, even if endpoints are in the Passive Learning group.*
The following properties are available:

- **VMware vSphere Advanced Properties** (if configured)
- **VMware Guest OS Properties**
- **VMware vSphere Server Properties**
- **VMware Virtual Machine Properties**

### VMware vSphere Advanced Properties

The host dynamic advanced properties let you create customized policies for:

- Virtual machines
- ESXi Hosts
The following data types are supported:

- Boolean
- String
- Integer

**Static Properties**

The static properties are pre-configured properties that come with the Forescout VMware vSphere Plugin.

<table>
<thead>
<tr>
<th>Hardening Guide Properties</th>
<th>Forescout Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi.config-persistent-logs</td>
<td>VMware Persistent Log Configured</td>
</tr>
<tr>
<td>ESXi.enable-normal-lockdown-mode</td>
<td>VMware Host Lockdown Mode</td>
</tr>
<tr>
<td>ESXi.enable-strict-lockdown-mode</td>
<td></td>
</tr>
<tr>
<td>ESXi.firewall-enabled</td>
<td>VMware Host Firewall Enabled</td>
</tr>
</tbody>
</table>

**Virtual Machine Dynamic Properties**

To create dynamic properties, you need to access the VMware vSphere 6.0 Security Hardening Guide. The following table lists some examples of Virtual Machine Dynamic properties.


<table>
<thead>
<tr>
<th>Hardening Guide Properties</th>
<th>Forescout Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.disable-hgfs</td>
<td>isolation.tools.hgfsServerSet.disable</td>
</tr>
<tr>
<td>VM.disable-unexposed-features-autologon</td>
<td>isolation.tools.ghi.autologon.disable</td>
</tr>
<tr>
<td>VM.disable-VMtools-autoinstall</td>
<td>isolation.tools.autoInstall.disable</td>
</tr>
<tr>
<td>VM.restrict-host-info</td>
<td>tools.guestlib.enableHostInfo</td>
</tr>
<tr>
<td>VM.disable-console-gui-options</td>
<td>isolation.tools.setGUIOptions.enable</td>
</tr>
</tbody>
</table>

**ESXi Host Dynamic Properties**

To create ESXi host dynamic properties, you need to access the VMware vSphere 6.0 Security Hardening Guide. The following table lists some examples of ESXi Host Dynamic properties.


<table>
<thead>
<tr>
<th>Hardening Guide Properties</th>
<th>Forescout Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi.set-shell-interactive-timeout</td>
<td>UserVars.ESXiShellInteractiveTimeOut</td>
</tr>
<tr>
<td>ESXi.set-shell-timeout</td>
<td>UserVars.ESXiShellTimeOut</td>
</tr>
<tr>
<td>ESXi.enable-remote-syslog</td>
<td>Syslog.global.logHost</td>
</tr>
<tr>
<td>ESXi.set-account-lockout</td>
<td>Security.AccountLockFailures</td>
</tr>
<tr>
<td>ESXi.set-account-auto-unlock-time</td>
<td>Security.AccountUnlockTime</td>
</tr>
</tbody>
</table>

See also: To set an advanced property to display in Inventory View.
VMware Guest OS Properties

Static virtual machine properties can be detected by adding a condition in the Main Rule or Sub-Rule of a policy. Under the Properties tree, select VMware vSphere and then select a static property.

The following table lists some examples of VMware Guest OS properties.

<table>
<thead>
<tr>
<th>VMware Guest Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine Guest Disk</td>
<td>Indicates information about the disk on which the guest runs. VMware Tools must be running on the endpoint to resolve this property.</td>
</tr>
<tr>
<td>Virtual Machine Guest Health</td>
<td>Indicates the general health of the guest by reporting the worst alarm/configuration status of the guest. Valid values:</td>
</tr>
<tr>
<td></td>
<td>▪ Definite problem (VMware red status)</td>
</tr>
<tr>
<td></td>
<td>▪ Entity OK (VMware yellow status)</td>
</tr>
<tr>
<td></td>
<td>▪ Possible problem (VMware green status)</td>
</tr>
<tr>
<td></td>
<td>▪ Status unknown (VMware gray status)</td>
</tr>
<tr>
<td></td>
<td>This value may be influenced by the Query Interval configured for the VMware server that manages the virtual machine.</td>
</tr>
<tr>
<td>Virtual Machine Guest Hostname</td>
<td>Indicates the hostname of the guest operating system. VMware Tools must be running on the endpoint to resolve this property.</td>
</tr>
<tr>
<td>Virtual Machine Guest Primary IP</td>
<td>Indicates the primary IP address of the guest operating system. VMware Tools must be running on the endpoint to resolve this property.</td>
</tr>
<tr>
<td>Virtual Machine Guest Network Adapters</td>
<td>Indicates information about virtual network controllers defined in the guest. VMware Tools must be running on the endpoint to resolve this property.</td>
</tr>
<tr>
<td>Virtual Machine Guest OS</td>
<td>Indicates the operating system running on the guest.</td>
</tr>
<tr>
<td>Virtual Machine Guest State</td>
<td>Indicates the most recent operation mode of the guest operating system reported to the Forescout platform. This value may be influenced by the Query Interval configured for the VMware server that manages the virtual machine. VMware Tools must be running on the endpoint to resolve this property.</td>
</tr>
<tr>
<td>VMware Tools Status</td>
<td>Indicates whether VMware Tools is installed and running in the guest.</td>
</tr>
</tbody>
</table>

VMware vSphere Server Properties

The following table lists some examples of VMware vSphere Server properties.

<table>
<thead>
<tr>
<th>VMware vSphere Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi Server Name</td>
<td>Indicates the hostname of the ESXi server.</td>
</tr>
<tr>
<td>VMware Host Firewall Enabled</td>
<td>Indicates whether the firewall is enabled on the ESXi server.</td>
</tr>
<tr>
<td>VMware Host Lockdown Mode</td>
<td>Indicates the lockdown mode on the ESXi server. Options are</td>
</tr>
<tr>
<td></td>
<td>▪ Disabled</td>
</tr>
<tr>
<td></td>
<td>▪ Normal</td>
</tr>
<tr>
<td></td>
<td>▪ Strict</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>VMware Persistent Log Configured</strong></td>
<td>Indicates whether the ESXi host is configured with persistent logging.</td>
</tr>
<tr>
<td><strong>VMware Server Build</strong></td>
<td>Indicates the build number of the software running on the ESXi server that hosts the virtual machine, or the vCenter server.</td>
</tr>
<tr>
<td><strong>VMware Server Host Profile</strong></td>
<td>Indicates the host profile configured on the ESXi server.</td>
</tr>
<tr>
<td><strong>VMware Server Instance UUID</strong></td>
<td>Indicates the Universally Unique Identifier (UUID) of the vCenter server.</td>
</tr>
<tr>
<td><strong>VMware Server License Product Name</strong></td>
<td>Indicates the product name as it appears in the license for the ESXi server that hosts the virtual machine, or the vCenter server.</td>
</tr>
<tr>
<td><strong>VMware Server License Product Version</strong></td>
<td>Indicates the product version as it appears in the license for the ESXi server that hosts the virtual machine, or the vCenter server.</td>
</tr>
<tr>
<td><strong>VMware Server Locale Build</strong></td>
<td>Indicates the locale build of the ESXi server that hosts the virtual machine, or the vCenter server.</td>
</tr>
<tr>
<td><strong>VMware Server Locale Version</strong></td>
<td>Indicates the locale version of the ESXi server that hosts the virtual machine, or the vCenter server.</td>
</tr>
</tbody>
</table>
| **VMware Server OS Type**                  | Indicates the operating system and server architecture of the ESXi server that hosts the virtual machine, or the vCenter server. This is typically a string in the format: OS-architecture. For example:  
  - win32-x86 indicates an x86-based Windows system.  
  - linux-x86 indicates an x86-based Linux system.  
  - vmnix-x86 indicates an x86 ESX Server microkernel. |
| **VMware Server Product ID**               | Indicates the unique product line identifier for the ESXi server that hosts the virtual machine, or the vCenter server. Typical values include:  
  - gsx indicates the VMware Server product.  
  - esx indicates the ESX product.  
  - embeddedEsx indicates the ESXi product.  
  - vpx indicates the vCenter product. |
| **VMware Server Product Name**             | Indicates the short form of the product name for the ESXi server that hosts the virtual machine, or the vCenter server. This string does not contain version information. |
| **VMware Server Host Profile Compliance Status** | Indicates the ESXi server host profile compliance status. Options are:  
  - Compliant  
  - Noncompliant  
  - Unknown |
| **VMware Server Vendor**                   | Indicates the vendor of the ESXi server that hosts the virtual machine, or the vCenter server. |
| **VMware Server Version**                  | Indicates the version number of the ESXi server that hosts the virtual machine, or the vCenter server. |
VMware vCenter Server IP

Indicates the IP address of the vCenter server that manages the ESXi server that hosts the virtual machine.

## VMware Virtual Machine Properties

Static virtual machine properties can be detected by adding a condition in the Main Rule or Sub-Rule of a policy.

**To access the virtual machine properties:**

1. In the Main Rule or the Sub-Rule of a policy, select **Add**. The Condition dialog box opens.

2. In the left pane, expand **VMware Virtual Machine** and then select a property.

The following table lists some examples of VMware Virtual Machine properties.

<table>
<thead>
<tr>
<th><strong>Virtual Machine Boot Time</strong></th>
<th>Indicates the date and time of the most recent reboot of the virtual machine reported to the Forescout platform. This value may be influenced by the Query Interval configured for the VMware server that manages the virtual machine.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Machine Power State</strong></td>
<td>Indicates the most recent power state for the virtual machine reported to the Forescout platform. This value may be influenced by the Query Interval configured for the VMware server that manages the virtual machine.</td>
</tr>
<tr>
<td><strong>Virtual Machine CPU Ready (%)</strong></td>
<td>The average CPU ready % per vCPU (the percentage of time the VM was ready, but could not get scheduled to run on the physical CPU). In general, values under 5% are acceptable; while values 5% and above indicate potential performance issues due to CPU resource contention.</td>
</tr>
<tr>
<td><strong>Virtual Machine Usage CPU (one thousandth)</strong></td>
<td>The average virtual machine CPU usage in 1/1000 (one thousandth) fraction.</td>
</tr>
<tr>
<td><strong>Virtual Machine CPU Usage (%)</strong></td>
<td>The percentage of the total CPU usage for all vCPUs allocated to the VM.</td>
</tr>
<tr>
<td><strong>Virtual Machine Disk Highest Latency</strong></td>
<td>The highest read or write latency in milliseconds for all disks configured for the VM.</td>
</tr>
<tr>
<td><strong>Virtual Machine Usage Disk I/O (KBps)</strong></td>
<td>The virtual machine disk input/output usage in KBps.</td>
</tr>
<tr>
<td><strong>Virtual Machine Disk Usage (%)</strong></td>
<td>The percentage of the total disk size used by the VM on all VMware data stores associated with the VM.</td>
</tr>
<tr>
<td><strong>Virtual Machine Hardware</strong></td>
<td>Indicates the hardware configured for the virtual machine.</td>
</tr>
<tr>
<td><strong>Virtual Machine Memory Usage (%)</strong></td>
<td>The percentage of the total memory used by the VM, calculated from the amount of VMware active memory for the VM relative to the total memory configured for the VM.</td>
</tr>
<tr>
<td><strong>Virtual Machine Name</strong></td>
<td>The name of the virtual machine.</td>
</tr>
</tbody>
</table>
### Virtual Machine Usage Network I/O (KBps)

The virtual machine network input/output usage in KBps.

### Virtual Machine is Orphan

Indicates whether the virtual machine is orphaned. A virtual machine is orphaned if a VM is found in the vCenter server but no longer exists on an ESXi host.

### Virtual Machine Peripheral Devices

The storage and other peripheral devices attached to the host machine and represented in the virtual machine. This value may be influenced by the Query Interval configured for the VMware server that manages the virtual machine.

### Virtual Machine Port Group

The port group configured for the virtual machine. This value may be influenced by the Query Interval configured for the VMware server that manages the virtual machine.

### Display IPv6 Addresses

If vCenter servers have VM instances configured with IPv6 addresses, they can be displayed in the All Hosts pane. If ESXi servers have IPv6 enabled, the IPv6 addresses can be displayed in the All Hosts pane.

### Manage Virtual Devices – Policy Actions

The following actions are available when the VMware vSphere Plugin is installed.

If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl license to use these actions. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.
### Block Virtual Machine Network Access
This action disconnects all network adapters of a virtual machine in a VMware environment.
An action threshold is defined for this action in the Forescout platform. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.

### Change Virtual Machine Port Group
This action changes the port group configured for a virtual machine in a VMware environment. When changing to a port group on a virtual switch, only the port group label needs to be specified. When changing to a port group on a distributed virtual switch, the switch name must also be provided.
An action threshold is defined for this action in the Forescout platform. By default, the action can be applied to no more than 2% of the endpoints managed by each Appliance.

### Install/Upgrade VMware Tools
This action installs or upgrades VMware Tools on a virtual machine in a VMware environment. Initial installation of VMware Tools may require user interaction within the guest virtual machine, but upgrades are implemented automatically.

### Power Off Virtual Machine
This action powers off a virtual machine in a VMware environment. An action threshold is defined for this action in the Forescout platform. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.

### Power On Virtual Machine
This action powers on a virtual machine in a VMware environment. If the endpoint is in the Suspended state, this action restores the endpoint to the running state.

### Reboot Virtual Machine Guest
This action initiates reboot of the guest operating system on a virtual machine in a VMware environment.
An action threshold is defined for this action in the Forescout platform. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.

### Reset Virtual Machine
This action performs a hard reset of a virtual machine in a VMware environment.
An action threshold is defined for this action in the Forescout platform. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.

### Shut Down Virtual Machine Guest
This action initiates a clean shutdown of the guest operating system and all its services running on a virtual machine in a VMware environment.
An action threshold is defined for this action in the Forescout platform. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.

### Standby Virtual Machine Guest
This action alerts the guest operating system to prepare to be suspended. This action applies to virtual machines in a VMware environment.

### Suspend Virtual Machine
This action suspends a virtual machine in a VMware environment.
An action threshold is defined for this action in the Forescout platform. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.
Action thresholds are defined for some of these actions. These thresholds limit the percentage of endpoints managed by each Appliance to which the action can be applied simultaneously. For more information, refer to Working with Action Thresholds in the ForeScout Administration Guide.

To define the virtual machine action:

1. In the Main Rule or the Sub-Rule of a policy, select Add.
2. Name the new rule or sub-rule and select OK. The Sub-Rule dialog box opens.
3. Under Actions, select Add.
4. In the left pane of the Actions dialog box, expand VMware vSphere and then select an action.
5. Set the parameters for the action and then select OK.

Use the VMware vSphere Plugin

This section describes how to use the Hybrid Module: VMware vSphere Plugin.

Access the Asset Inventory

Once the VMware vSphere Plugin has been configured, you can view and manage the virtual devices from the Asset Inventory view in the Console. This provides activity information, accurate at the time of the poll, on cloud endpoints based on certain instances’ properties. The Asset Inventory view provides full visibility of campus endpoints data center workloads, including:

- Total number of ESXi hosts discovered
- Total number of VMs discovered
- VMs classified based on its guest OS
- VMs per ESXi host
- VMs per vSphere tag

To access the Inventory:

1. In the Console, select Inventory.
2. Go to the Inventory entries related to this plugin.
View Advanced Properties

If you do not see a specific static or dynamic VMware advanced property, you can display it by changing a setting in the VMware property itself.

To configure an advanced property to display in Inventory view:

1. In the Console, select **Options** from the **Tools** menu.
2. In the left pane, select **VMware vSphere**. The VMware vSphere pane opens.
3. Select the Advanced Property tab.
4. Select an item and then select **Edit**. The Edit VMware Property dialog box opens.
5. Select the VMware Advanced Property tab.
6. Select the **Display in Inventory** field and add an optional Description.
7. Select **OK**.
8. In the VMware vSphere pane, select **Apply**.

Refer to *Working at the Console > Working with Inventory Detections* in the *Forescout Administration Guide* for information about how to work with the Forescout Inventory. See *Additional Forescout Documentation* for information on how to access the guide.

**Review Admission Events**

The VMware vSphere Plugin detects all new endpoints and displays them in the profile of the endpoint. This event is generated once, when the endpoint is first detected by the plugin.

**To review an admission event:**

1. Log in to the Console and select **All Hosts**.
2. In the Detections pane, select a host to review the profile of the host.
3. In the Profile tab, right-click on the **Admission** field. Full information about the new endpoint is displayed.

4. If you require further information, double-click the item in the table to open the Host Details dialog box.
5. Select the All policies tab and then select **Show host log**.
6. Enter the parameters for running the log on and then select **OK**.

   The Host Log is displayed with all the information. You can export or print the results.

   Refer to the *Forescout Administration Guide* for information about how to work with Event properties. See *Additional Forescout Documentation* for information on how to access the guide.

**Hybrid Cloud Module Information**

The VMware vSphere Plugin is installed with the Forescout Hybrid Cloud Module. The Forescout Hybrid Cloud Module provides visibility and control functions across physical and virtual devices that are on-premises and off-premises through the following plugin integrations:

- AWS Plugin
- Azure Plugin
- VMware NSX Plugin
- VMware vSphere Plugin

The Hybrid Cloud Module is a Forescout Base Module. Base Modules are delivered with each Forescout release.

The plugins listed above are installed and rolled back with the Hybrid Cloud Module.

Refer to the *Forescout Hybrid Cloud Module Overview Guide* for more module information, such as module requirements, upgrade, and rollback instructions.
Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Access documentation downloads from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – Product Updates Portal
- **Flexx Licensing Mode** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select Help > About Forescout.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:


Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select Downloads.
Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive Help buttons to access information about tasks and topics quickly.

Forescout Administration Guide

- Select Forescout Help from the Help menu.

Plugin Help Files

- After installing the plugin, select Tools > Options > Modules, select the plugin, and then select Help.

Online Documentation

- Select Online Documentation from the Help menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).