



CounterACT® VMware vSphere® Plugin

Configuration Guide

Version 2.0.1

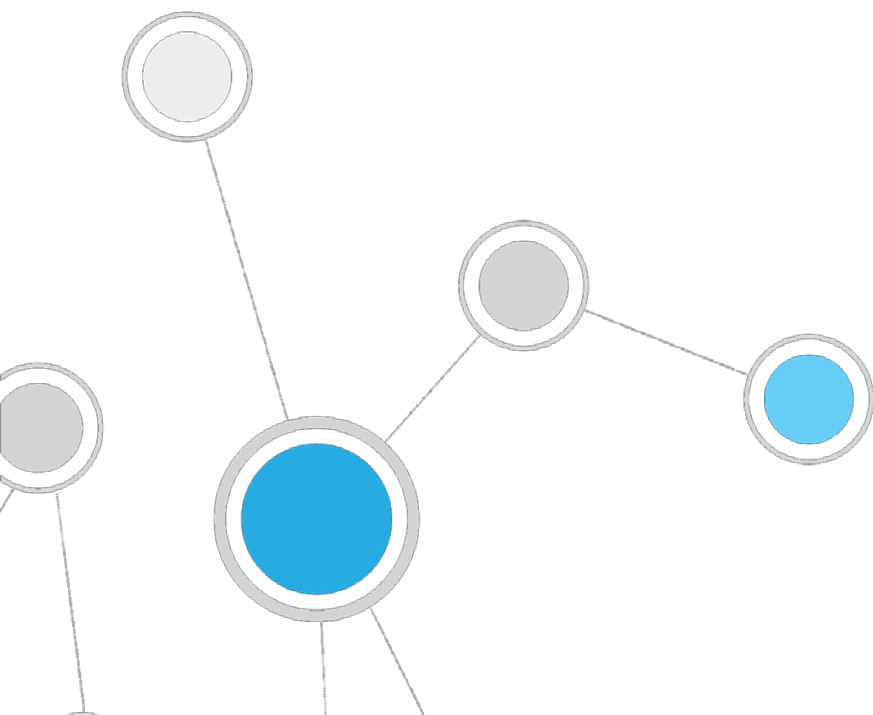


Table of Contents

About VMware vSphere® Integration	4
Use Cases	4
Additional VMware Documentation.....	4
About this Plugin.....	5
What to Do.....	5
Requirements.....	5
CounterACT Requirements.....	5
Networking Requirements	5
Supported Vendor Requirements	6
Define CounterACT Users in the VMware Environment	6
Defining a vSphere Role	6
Define Users with a CounterACT Role.....	8
Install the Plugin.....	9
Configure the Plugin.....	10
Define Target ESXi Host or vCenter Server	10
Add VMware Advanced Properties.....	13
Test the VMware Connection.....	15
View the VMware vSphere Connection	15
Run VMware vSphere Policy Templates.....	16
VMware Classification Template	18
VMware ESXi Host Firewall Compliance	21
VMware ESXi Host Lockdown Compliance	22
VMware ESXi Host Log Persistent Compliance	23
VMware ESXi Host Profile Compliance	24
VMware Low Usage Virtual Machines Template.....	25
VMware Tools Compliance Template	26
VMware VM CPU Ready	28
VMware VM Disk Usage.....	29
VMware Virtual Machines by ESXi Server Template.....	30
Create Custom VMware vSphere Policies.....	32
Detecting Virtual Devices – Host Properties	33
VMware vSphere Advanced Properties.....	34
VMware Guest OS Properties	35
VMware vSphere Server Properties.....	36
VMware vSphere Virtual Machine Properties.....	37

Managing Virtual Devices – Policy Actions.....	38
Using the VMware vSphere Plugin.....	40
Access the Inventory	41
Viewing Advanced Properties	41
Reviewing Admission Events	42
Additional CounterACT Documentation	43
Documentation Portal	43
Product Updates Portal.....	44
CounterACT Console Online Help Tools.....	44

About VMware vSphere® Integration

CounterACT® integration with VMware vSphere brings the detailed visibility, control and compliance capabilities of CounterACT to virtualized environments. The capabilities offered on physical endpoints can also be achieved on virtual endpoints such as VMware ESXi™ hosts and virtual machines (VM). For example:

- Visibility into hosts and VMs with details of various properties associated with these virtual endpoints.
- Applying CounterACT policies similar to those applied to campus endpoints to virtual endpoints.
- Eliminating guest VM redundancies by identifying stale machines.

Use Cases

- **Consolidated Visibility** – CounterACT discovers virtualized endpoints such as ESXi hosts and virtual machines by using this integration with VMware vSphere. CounterACT communicates to vCenter/ESXi via vSphere API to pull in relevant information with details on various ESXi and VM properties. See the [VMware Classification Template](#).
- **Compliance and Risk Assessment** – VMware Security Hardening Guides provide prescriptive guidance for customers on how to deploy and operate VMware products in a secure manner. The CounterACT VMware vSphere plugin provides a simple way to configure advanced properties and then use them in policies to make sure the deployed hosts or VMs follow the secure guidelines. See [Run VMware vSphere Policy Templates](#) and [VMware vSphere Advanced Properties](#).
- **Real Time Asset Management** – IT service management and asset management plays an important role in incident response. It is also closely related with security and helps with automating for quick response. As a first step in asset management, it is critical to get a complete picture of all devices. The vSphere Plugin helps in this important process by providing discovery of virtual endpoints and allows CounterACT to become the sole real-time device discovery tool for both physical and virtual endpoints. See [Reviewing 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 CounterACT 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 CounterACT actions on them. The plugin allows for configuring multiple vCenter and ESXi instances.

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

What to Do

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

1. Verify that you have met system requirements. See [Requirements](#).
2. [Define CounterACT Users in the VMware Environment](#)
3. [Install the Plugin](#)
4. [Configure the Plugin](#)
5. [Run VMware vSphere Policy Templates](#)
6. Use the in-depth information reported by the plugin to manage virtual devices, see [Using the VMware vSphere Plugin](#).

Requirements

This section describes system requirements, including:

- [CounterACT Requirements](#)
- [Networking Requirements](#)
- [Supported Vendor Requirements](#)

CounterACT Requirements

The following CounterACT releases can be integrated with this plugin.

- CounterACT version 7.0.0 with Service Pack 2.3.4 or above.

Networking Requirements

In case CounterACT and 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 5.0, 5.1, 5.5, 6.0, and 6.5

The following VMware licenses are required to work with the plugin.

- VMware vSphere® Enterprise Plus Edition™
- VMware vCenter Server (standard)

Define CounterACT Users in the VMware Environment

The plugin communicates with ESXi or vCenter servers to retrieve information on virtual machines, and to apply CounterACT actions to them. Before you configure and test this connection in CounterACT, define a user or group of users with 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 CounterACT.
- Define users and assign this role to them.

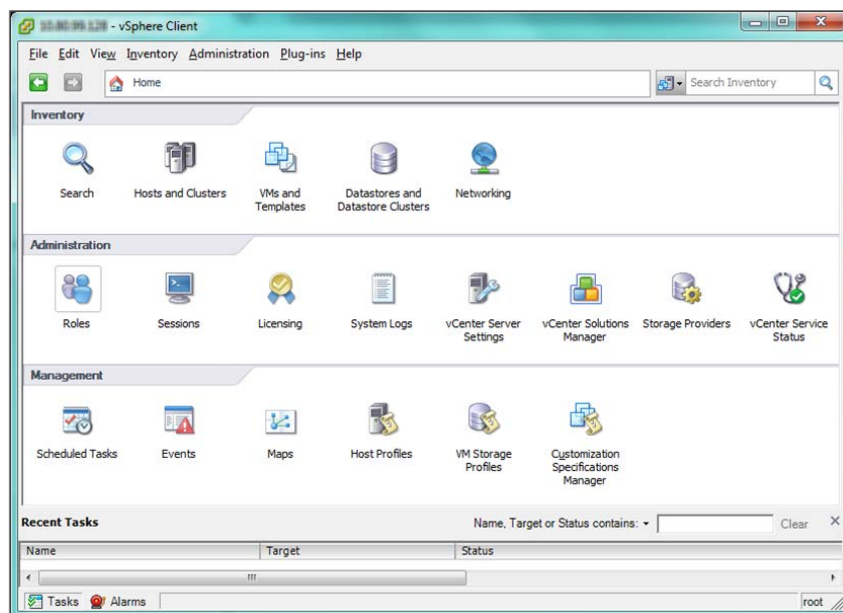
Details on configuring roles and users can be found in the [vSphere Security Guide](#). Specific steps required to create a user for CounterACT are provided below.

Defining a vSphere Role

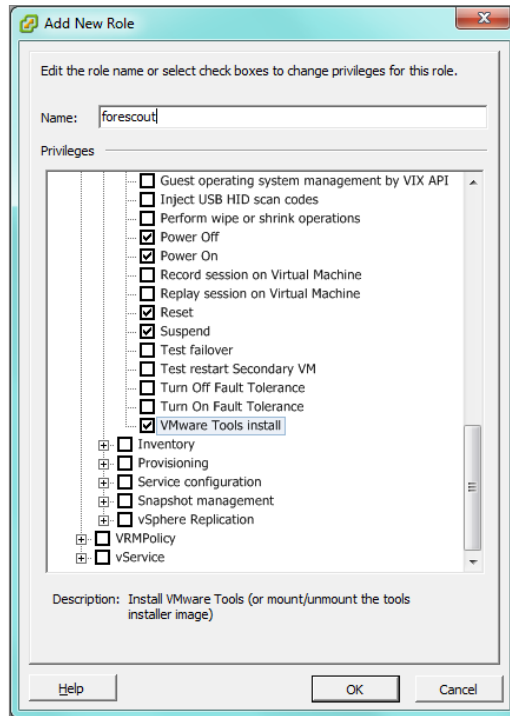
This section describes how to define a vSphere user role that includes the permissions required by CounterACT.

To define a user role for CounterACT users in the VMware environment:

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



3. In the Roles screen, select **Add Role**.
4. The Add New Role dialog opens. Enter a name for the new role, and enable the following privileges required by CounterACT:
 - VirtualMachine.Interact.ToolsInstall (VMware Tools Install)
 - VirtualMachine.Interact.PowerOff
 - VirtualMachine.Interact.PowerOn
 - VirtualMachine.Interact.Reset
 - VirtualMachine.Interact.Suspend
 - Virtual Machine.Interaction.Device Connection
 - virtual Machine.Configuration.Modify Device Settings
 - Network.Assign Network



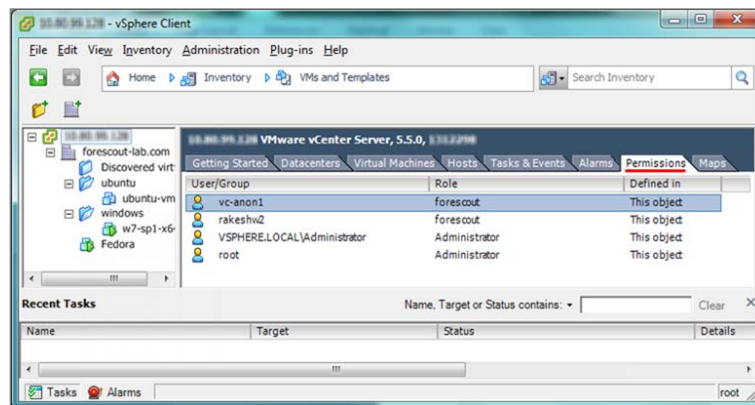
5. Select **OK** to save the role.

Define Users with a CounterACT Role

This section describes how to define users with a CounterACT role.

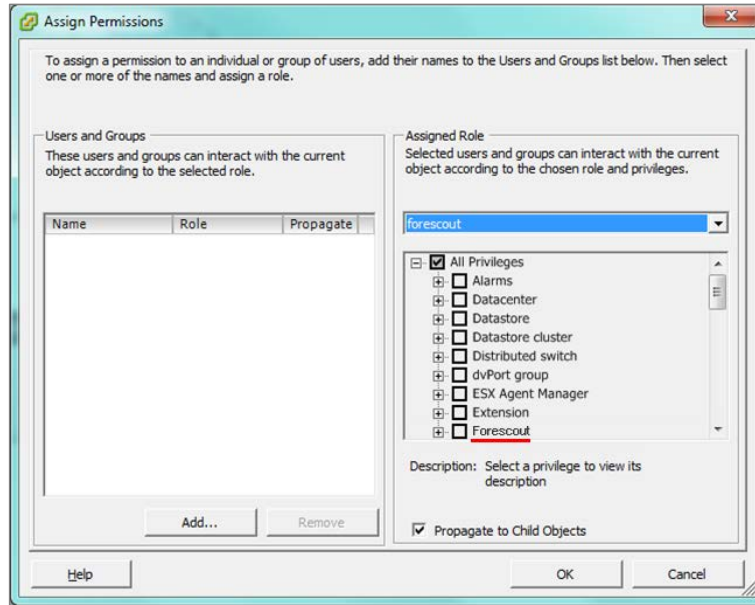
To define users with the CounterACT role in the VMware environment:

1. In the Inventory area of the vSphere Client console, select **VMs and Templates**.
2. A directory window lists the datastore objects of the vSphere environment.



3. In the left pane, select the vCenter or ESXi server that you plan on configuring in CounterACT.

4. In the right pane, select the **Permissions** tab. Right-click in the Permissions pane and then select **Add Permission**.
5. The Assign Permissions dialog opens. Assign the role you defined for CounterACT users to a new or existing user.



6. Record the login credentials of users that are assigned the CounterACT role. You enter these credentials in CounterACT when you configure the plugin.
7. Repeat steps described [Defining a vSphere Role](#) until users are defined that allow CounterACT to query all servers in the VMware environment that you want to configure in CounterACT.

Install the Plugin

This section describes how to install the plugin.

To install the plugin:

1. Navigate to the [Product Updates Portal, Base Plugins](#) page and download the plugin **.fpi** file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin **.fpi** file.
7. Select **Install**.

8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

Configure the Plugin

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

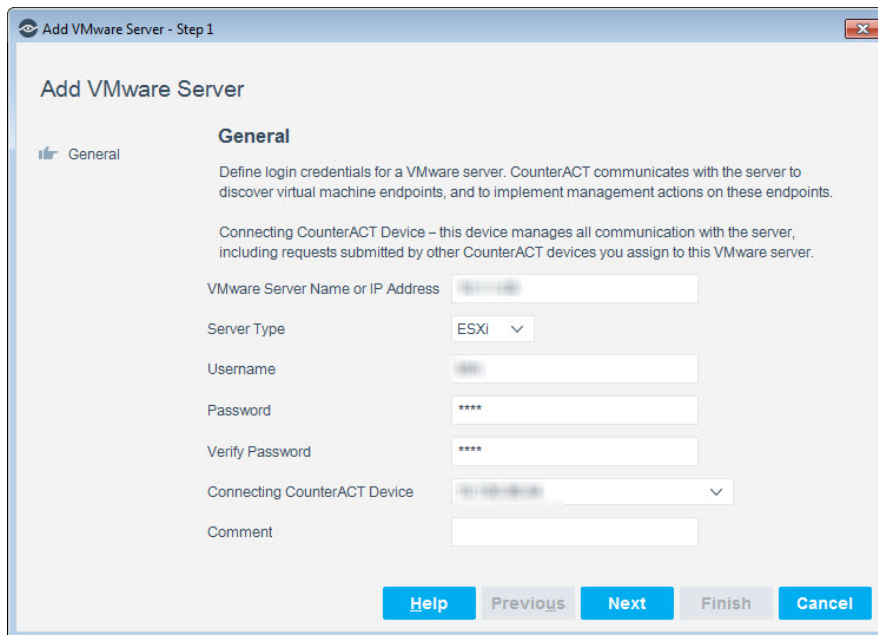
Define Target ESXi Host or vCenter Server

You will 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 will stop host discovery and property learning of virtual machines hosted by this server, but any actions will remain enabled.

To define the ESXi host or vCenter server:

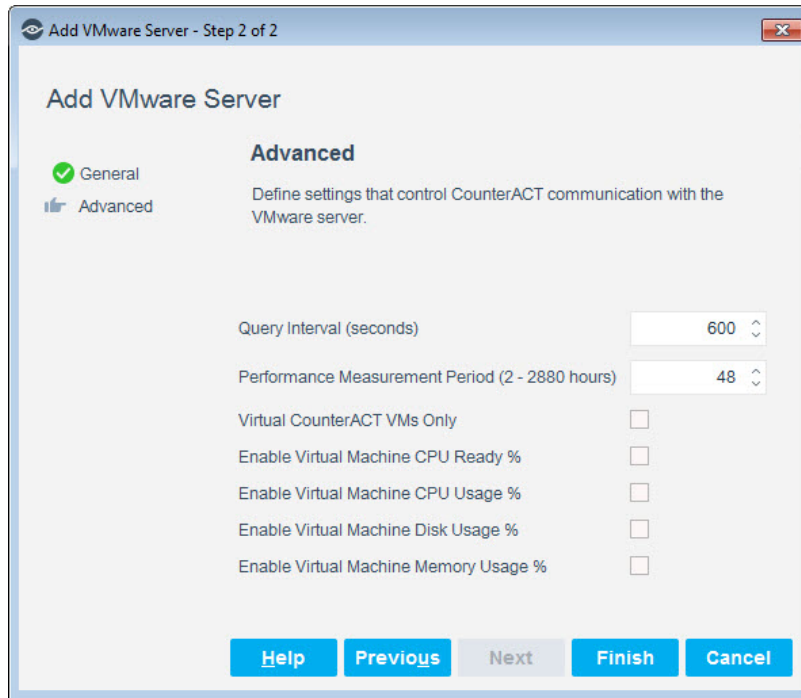
1. In the CounterACT Console, select **Options** from the **Tools** menu.
2. In the left pane, select **VMware vSphere**. The VMware vSphere pane opens to the VMware Server tab.
3. Select **Add**. The General tab opens.



4. Define Server parameters.

VMware Server Name or IP Address	Enter the hostname or IP address of the server.
Server Type	Select one: <ul style="list-style-type: none">▪ ESXi - Through the ESXi virtualization platform, you run the virtual machines, run applications, and configure the virtual machines.▪ vCenter - Through the vCenter Server, you can leverage authentication and permission management. The vCenter Server can have their own types of events, tasks, metadata, and privileges.
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.
Connecting CounterACT Device	Select a CounterACT device that will connect to this server. The CounterACT device specified in this field is the only device that communicates with the server. <ul style="list-style-type: none">- When the Enterprise Manager is defined as the Connecting CounterACT Device, endpoints without an IP address that the plugin detects 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.** The Advanced tab opens.



Query Interval (seconds)	<p>Specify how frequently the plugin should query the VMware server.</p> <p><i>To prevent CounterACT from mistakenly identifying virtual endpoints as inactive, set the Query interval to a value less than the inactivity timeouts defined in the Console.</i></p> <ol style="list-style-type: none"> 1. Select the Options icon and then select NAC in the left pane. 2. Select Time Settings and enter your settings.
Performance Measurement Period in Hours (2-2880)	<p>To measure the CPU, network and disk usage of the virtual machines, set the polling period, in hours, for the CPU, disk, and network Input/Output. The default is 48 hours.</p>
Virtual CounterACT VMs Only	<p>When this option is selected, the plugin only discovers/resolves VMs detected as virtual CounterACT (vCT) VMs associated with the polling Enterprise Manager or Appliance.</p> <p>For CounterACT 7.0.0, VMware Tools need to be manually installed on virtual CounterACT guests in order for VMware, and the VMware vSphere plugin to be aware of the IP address of the guest VM. The IP address of a virtual CounterACT device is needed for the VMware vSphere plugin to recognize the device as a virtual CounterACT VM.</p>

Enable Virtual Machine CPU Ready %	When this option is selected, the plugin pulls performance data from VMware server to calculate Virtual Machine CPU Ready % property.
Enable Virtual Machine CPU Usage %	When this option is selected, the plugin pulls performance data from VMware server to calculate Virtual Machine CPU Usage % property.
Enable Virtual Machine Disk Usage %	When this option is selected, the plugin pulls performance data from VMware server to calculate Virtual Machine Disk Usage % property.
Enable Virtual Machine Memory Usage %	When this option is selected, the plugin pulls performance data from VMware server to calculate Virtual Machine Memory Usage % property.

6. Continue to the next section.

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. They are based on the [VMware vSphere Security Hardening Guide](#). This configuration can be added anytime.

Once the property has been added, it can be used within a policy to determine whether the property has the correct desired value or not. If the property does not have the desired value for a ESXi host or VM, 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**. The Add VMware Property dialog box opens.

Add VMware Property - Step 1

Add VMware Property

VMware Property
Define dynamic property for the VMware advanced options on ESXi or Virtual Machine

Name

Description

VMware Advanced Option Name

VMware Advanced Option Data Type

VMware Advanced Option Type

Help **Previous** **Next** **Finish** **Cancel**

3. Define the property parameters.

Name	Enter the name of the VMware property. Valid characters to use are: <ul style="list-style-type: none"> ▪ Alphabet ▪ Numerical ▪ Underscore Punctuation - period, comma, hyphen and space.
Description	(Optional) Enter a description of the property. Valid characters to use are: <ul style="list-style-type: none"> ▪ Alphabet ▪ Numerical ▪ Underscore ▪ Punctuation - period, comma, hyphen and space.
VMware Advanced Option Name	Enter the name of the advanced property. Valid characters to use are: <ul style="list-style-type: none"> ▪ Alphabet ▪ Numerical ▪ Underscore Punctuation - period, comma, hyphen and space. Refer to VMware vSphere Advanced Properties .
VMware Advanced Option Data Type	Select a data type for the property. The following data types are supported: <ul style="list-style-type: none"> ▪ Boolean ▪ String ▪ Integer
VMware Advanced Option Type	Select the type of virtual endpoint: <ul style="list-style-type: none"> ▪ ESXi ▪ Virtual Machine

Add VMware Property - Step 2 of 2

Add VMware Property

☒ VMware Property
☐ VMware Advanced Property

VMware Advanced Property

Indicate if you want this dynamic property to display in Inventory view. You can also assign an optional description.

Display in inventory ☐

Description

4. Enable the dynamic property to display in the Inventory view.

Display in Inventory	Check if you want this dynamic property to display in the Inventory view.
Description	(Optional) Enter a description of the property.

5. Select **Finish**. These properties will now display in the Conditions dialog box and you can add them to your policies. For information about adding dynamic properties, see [VMware vSphere Advanced Properties](#).

Test the VMware Connection

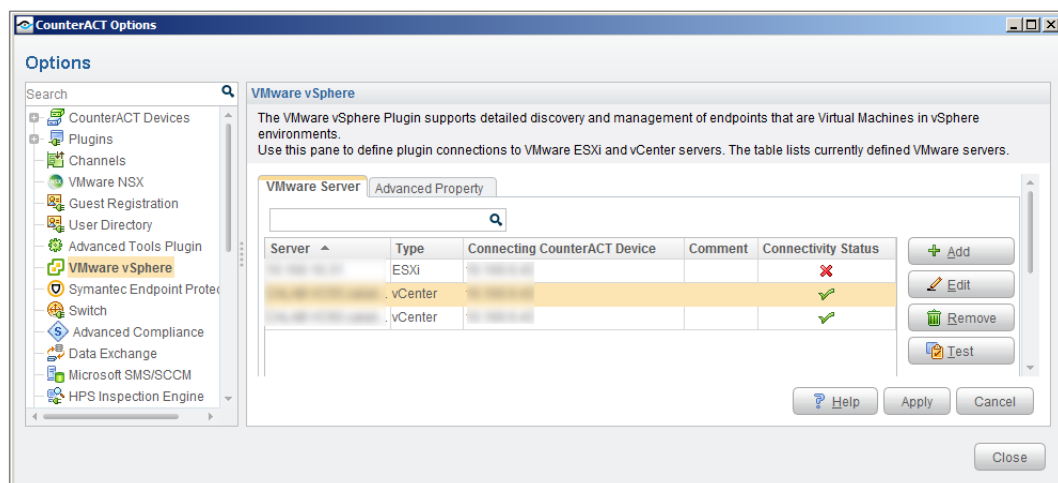
You can test the plugin communication with a VMware server.

To test communication:

1. In the VMware vSphere pane, select a VMware server defined in CounterACT.
2. Select **Test**. Using your configured settings, CounterACT 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 table in the VMware vSphere pane shows all vCenter and ESXi instances that you have defined in CounterACT. The **Connectivity Status** column indicates the status of each VMware server.



The following Connectivity Status values are reported:

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

Run VMware vSphere Policy Templates

CounterACT 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 CounterACT Console's Policy Manager.

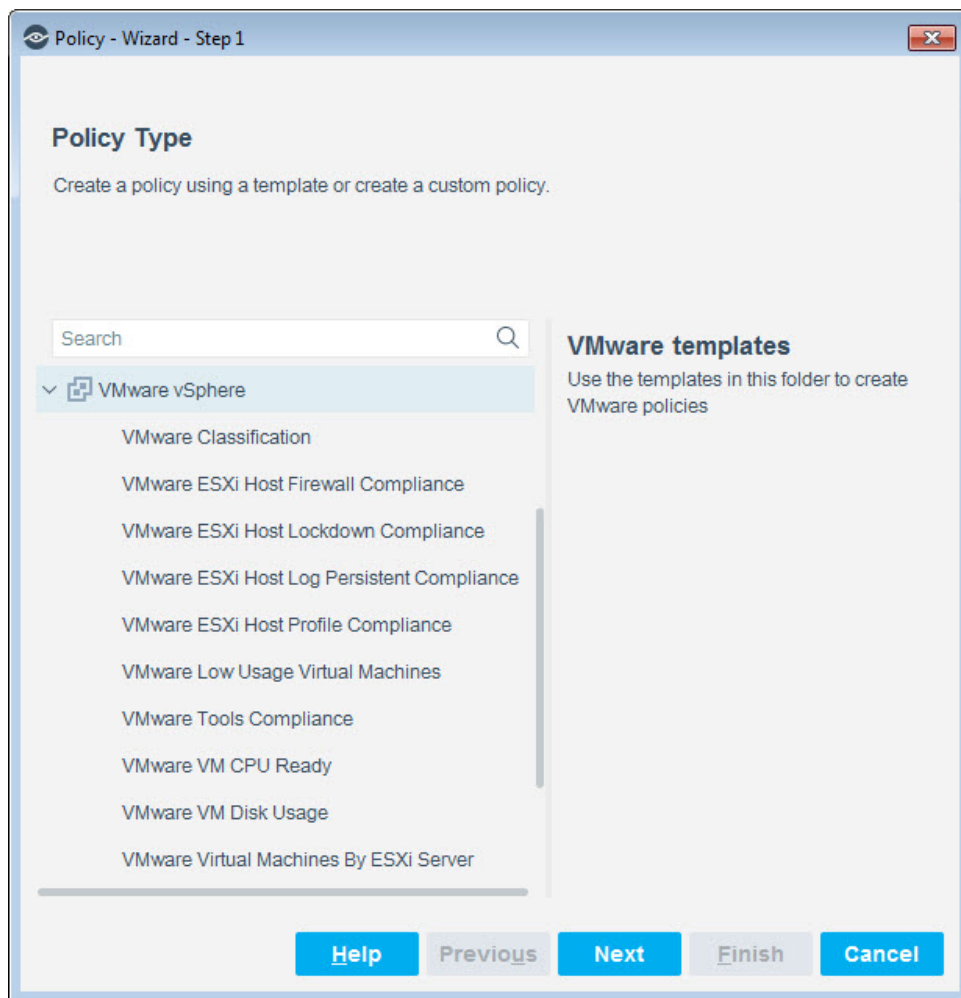
CounterACT policies use a wide range of host conditions to trigger various management and remediation actions. When the conditions of the policy are met, the actions are implemented. For example, the CounterACT VMware vSphere Plugin can run a policy that checks if a virtual machine is anti-virus compliant.


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](#) – generates a policy that monitors performance through the VMware VM CPU Ready status by percentage.
- [VMware VM Disk Usage](#) – 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 CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Manual.

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 CounterACT can communicate with one or more VMware servers.

Run the Template

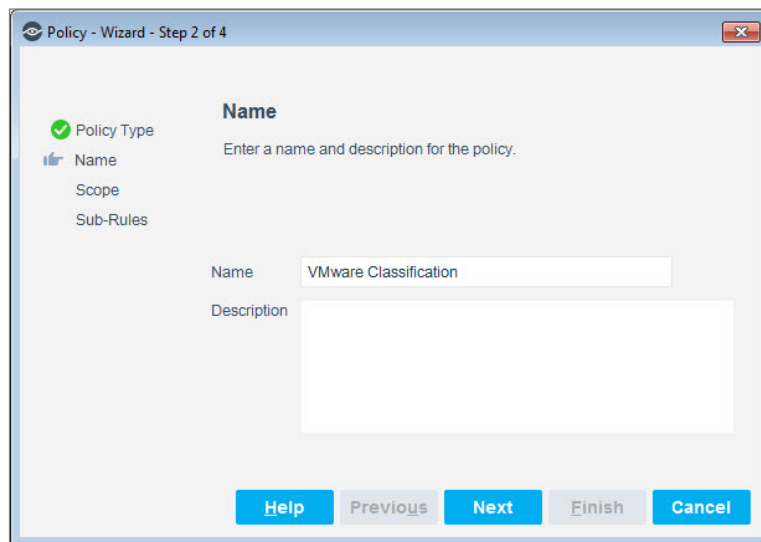
This section describes how to create a policy based on the VMware Classification Policy template.

To run the template:

1. Select the Policy tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware vSphere** and then select **VMware Classification**.
4. Select **Next**. The Name pane opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



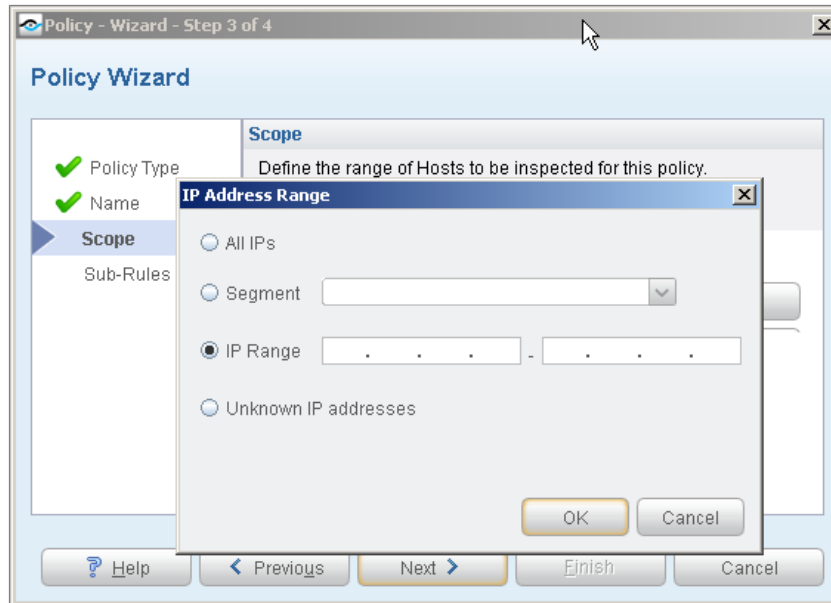
5. Define a unique name for the policy you are creating based on this template and enter a description.
 - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
 - Use a descriptive name that indicates what your policy 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.

6. Select **Next**. The Scope pane and IP address dialog box opens.

Define which Endpoints will be Inspected - Policy Scope

The Scope Pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.



7. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:
- **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
 - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope pane.
 - **IP Range**: Define a range of IP addresses. These addresses need to be within the Internal Network.
 - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**. The Sub-Rules pane opens. See [How Endpoints are Detected and Handled](#) for details of default policy logic.

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 CounterACT how to detect and handle endpoints defined in the policy scope.

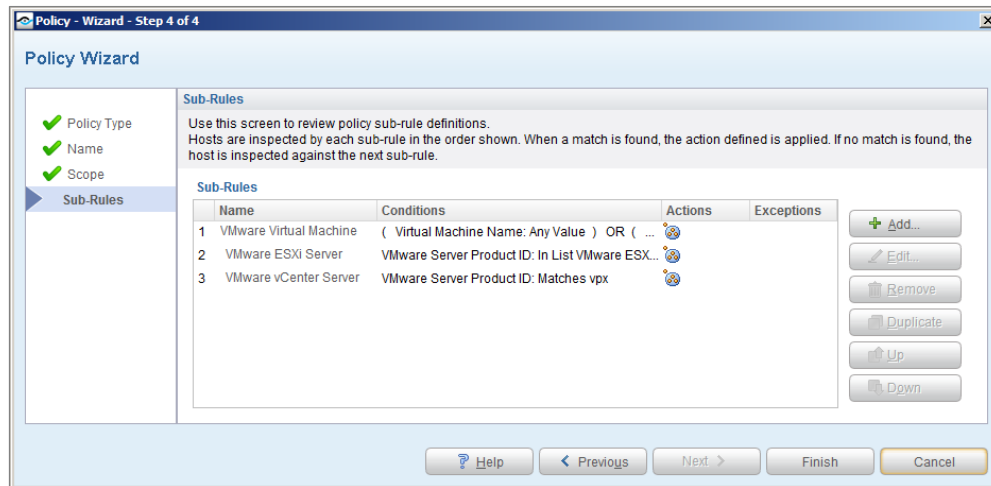
Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

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.



10. The default sub-rules for this policy template are:

Sub-Rule Name	Condition Definition
VMware Virtual Machine	<p>This rule matches endpoints with any of the following values:</p> <ul style="list-style-type: none"> Virtual Machine Name – Any Value NIC Vendor – VMWARE, INC Device Interfaces – Starts With: VMware Accelerated <p>The Add to Group action adds detected endpoints to the VMware virtual machines group. This action is enabled by default.</p>

VMware ESXi Server	<p>This rule matches endpoints with VMware Server Product ID list values of <i>gsx</i>, <i>embeddedEsx</i> and <i>esx</i>.</p> <p>The Add to Group action adds detected endpoints to the VMware ESXi Servers group. This action is enabled by default.</p>
VMware vCenter Server	<p>This rule matches endpoints with VMware Server Product ID values of <i>vpx</i>.</p> <p>The Add to Group action adds detected endpoints to the VMware ESXi Servers group. This action is enabled by default.</p>

 See the CounterACT Console User Guide to understand the symbols listed in the Actions column.

11. Select **Finish**

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

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

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 CounterACT can communicate with one or more VMware servers.

Run the Template

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

To run the template:

1. Select the Policy tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware vSphere** and then select **VMware ESXi Host Firewall Compliance**.
4. Select **Next**. The Name pane opens. See [Name the Policy](#).
5. Select **Next**. The Scope pane and IP address dialog box opens. See [Define which Endpoints will be Inspected - Policy Scope](#).

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 [How Endpoints are Detected and Handled](#) for details of default policy logic.

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.

7. The default sub-rules for this policy template are:

Sub-Rule Name	Condition Definition
Firewall Disabled	This rule checks if the firewall on the VMware host is disabled.

8. Select **Finish**
9. In the CounterACT Policy Manager, select **Apply** to save the policy.
10. Select the **Start** button to execute the policy.

VMware ESXi Host Lockdown Compliance

The VMware ESXi Host Lockdown Compliance policy template checks whether the ESXi host is in lockdown compliance.

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

Prerequisites

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

Run the Template

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

To run the template:

1. Select the Policy tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware vSphere** and then select **VMware ESXi Host Lockdown Compliance**.
4. Select **Next**. The Name pane opens. See [Name the Policy](#).
5. Select **Next**. The Scope pane and IP address dialog box opens. See [Define which Endpoints will be Inspected - Policy Scope](#).

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 [How Endpoints are Detected and Handled](#) for details of default policy logic.

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.

7. The default sub-rules for this policy template are:

Sub-Rule Name	Condition Definition
Lockdown Disabled	This rule checks if the VMware host capability to lockdown is disabled.

8. Select **Finish**

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

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

VMware ESXi Host Log Persistent Compliance

The VMware ESXi Host Security Hardening policy template checks the if the ESXi host is log persistent compliant.

Use this template to create a policy that checks the ESXi host log persistent compliance.

Prerequisites

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

Run the Template

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

To run the template:

1. Select the Policy tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware vSphere** and then select **VMware ESXi Host Log Persistent Compliance**.
4. Select **Next**. The Name pane opens. See [Name the Policy](#).
5. Select **Next**. The Scope pane and IP address dialog box opens. See [Define which Endpoints will be Inspected - Policy Scope](#).

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 [How Endpoints are Detected and Handled](#) for details of default policy logic.

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.

7. The default sub-rules for this policy template are:

Sub-Rule Name	Condition Definition
Host Log Not Persistent	This rule checks if the VMware persistent log is not configured.

8. Select **Finish**
9. In the CounterACT Policy Manager, select **Apply** to save the policy.
10. Select the **Start** button to execute the policy.

VMware ESXi Host Profile Compliance

Use this template to create a policy that checks if the ESXi host is configured with a host profile, and whether it is compliant.

Prerequisites

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

Run the Template

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

To run the template:

1. Select the Policy tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware** and then select **VMware ESXi Host Profile Compliance**.
4. Select **Next**. The Name pane opens. See [Name the Policy](#).
5. Select **Next**. The Scope pane and IP address dialog box opens. See [Define which Endpoints will be Inspected - Policy Scope](#).
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 [How Endpoints are Detected and Handled](#) for details of default policy logic.

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.

Sub-Rule Name	Condition Definition
Host Profile Compliant	Checks if the server host profile compliance status is <i>Compliant</i> .
Host Profile Not Compliant	Checks if the server host profile compliance status is <i>Non-Compliant</i> .
Host Profile Unknown	Checks if the server host profile compliance status is <i>Unknown</i> .

7. Select **Finish**
8. In the CounterACT Policy Manager, select **Apply** to save the policy.
9. Select the **Start** button to execute the policy.

VMware Low Usage Virtual Machines Template

Use this template to create a policy that lists all virtual machines using low resources such as CPU, disk I/O and network I/O. 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 CounterACT can communicate with one or more VMware servers.

Run the Template

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

To run the template:

1. Select the Policy tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware vSphere** and then select **VMware Low Usage Virtual Machines**.
4. Select **Next**. The Name pane opens. See [Name the Policy](#).
5. Select **Next**. The Scope pane and IP address dialog box opens. See [Define which Endpoints will be Inspected - Policy Scope](#).

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 [How Endpoints are Detected and Handled](#) for details of default policy logic.

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.

7. The default sub-rules for this policy template are:

Sub-Rule Name	Condition Definition
Orphan Virtual Machines	This rule checks if the VM is an orphan machine.
Low Usage	This rule checks the CPU usage level by the one-thousandth fraction. Also checks for disk input/output and network input/output. The period of the measurement can be configured using the plugin configuration or customized with the Set Performance Measurement Period action.

8. Select **Finish**
9. In the CounterACT Policy Manager, select **Apply** to save the policy.
10. Select the **Start** button to execute the policy.

VMware Tools Compliance Template

Use this template to create a policy that detects and remediates virtual machines 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. CounterACT 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 CounterACT can communicate with one or more VMware servers.

- Verify that the *VMware Virtual Machines* group appears in the Console, Filters pane. If not, run the *VMware Classification* policy template to create this group. See [VMware Classification Template](#) for details.

Run the Template

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

To run the template:

1. Select the Policy tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware vSphere** and then select **VMware Tools Compliance**.
4. Select **Next**. The Name pane opens. See [Name the Policy](#).
5. Select **Next**. The Scope pane and IP address dialog box opens. See [Define which Endpoints will be Inspected - Policy Scope](#).
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 [How Endpoints are Detected and Handled](#) for details of default policy logic.

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.

Sub-Rule Name	Condition Definition
VMware Tools installed and up to date	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.
VMware Tools installed and upgrade recommended	<p>This rule matches endpoints with the following VMware Tools Status values:</p> <ul style="list-style-type: none">▪ VMware Tools is installed, supported, and newer than the version available on the ESXi host.▪ VMware Tools is installed, supported, but a newer version is available. <p>The Install/Upgrade VMware Tools action initiates upgrade of the VMware Tools application on detected endpoints. This action is disabled by default.</p>

VMware Tools installed but needs updating	<p>This rule matches endpoints with the following VMware Tools Status values:</p> <ul style="list-style-type: none"> 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. <p>The Install/Upgrade VMware Tools action initiates upgrade of the VMware Tools application on detected endpoints. This action is disabled by default.</p>
VMware tools installed but endpoint is not managed correctly by the VMware server	<p>This rule matches endpoints with VMware Tools Status value of VMware Tools is installed, but it is not managed by VMware.</p> <p>The Send Email action notifies administrators that detected endpoints are unmanaged. This action is disabled by default.</p>
VMware Tools is not installed	<p>This rule matches endpoints with VMware Tools Status value of VMware Tools has never been installed.</p> <p>The Install/Upgrade VMware Tools action initiates installation of the VMware Tools application on detected endpoints. This action is disabled by default.</p>

7. Select **Finish**

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

9. Select the **Start** button to execute the policy.

10. VMware VM

VMware VM CPU Ready

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 CounterACT can communicate with one or more VMware servers.

Run the Template

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

To run the template:

1. Select the Policy tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware vSphere** and then select **VMware VM CPU Ready**.
4. Select **Next**. The Name pane opens. See [Name the Policy](#).
5. Select **Next**. The Scope pane and IP address dialog box opens. See [Define which Endpoints will be Inspected - Policy Scope](#).
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 [How Endpoints are Detected and Handled](#) for details of default policy logic.

Sub-Rules

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

Sub-Rule Name	Condition Definition
Offline	NOT Host is online
Low	Virtual Machine CPU Ready (%) 0-2
Medium	Virtual Machine CPU Ready (%) 3-5
High	Virtual Machine CPU Ready (%) 6-100
Unknown	No conditions

VMware VM Disk Usage

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 CounterACT can communicate with one or more VMware servers.

Run the Template

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

To run the template:

1. Select the Policy tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware vSphere** and then select **VMware VM CPU Ready**.
4. Select **Next**. The Name pane opens. See [Name the Policy](#).
5. Select **Next**. The Scope pane and IP address dialog box opens. See [Define which Endpoints will be Inspected - Policy Scope](#).
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 [How Endpoints are Detected and Handled](#) for details of default policy logic.

Sub-Rules

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

Sub-Rule Name	Condition Definition
Offline	NOT Host is online
Low	Virtual Machine Disk Usage (%) 0-60
Medium	Virtual Machine Disk Usage (%) 61-80
High	Virtual Machine Disk Usage (%) 81-100
Unknown	No conditions

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 CounterACT can communicate with one or more VMware servers. See [Configure the Plugin](#) for details.

Run the Template

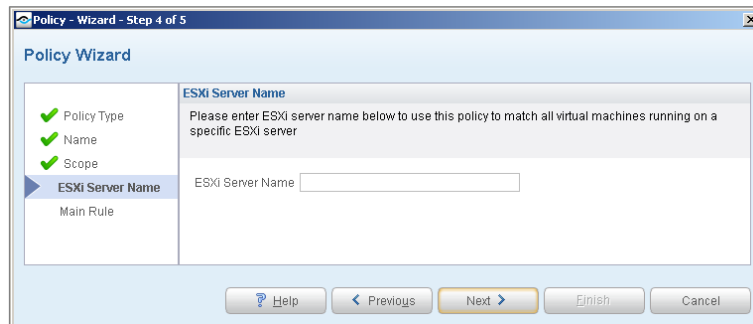
This section describes how to create a policy based on the template.

To run the template:

1. Select the Policy tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware vSphere** and then select **VMware Virtual Machines by ESXi Server**.
4. Select **Next**. The Name pane opens. See [Name the Policy](#).
5. Select **Next**. The Scope pane and IP address dialog box opens. See [Define which Endpoints will be Inspected - Policy Scope](#).
6. Select **Next**. The ESXi Server Name pane opens.

Define a Target ESXi Server

The ESXi Server Name pane lets you specify the ESXi server used by the policy to match endpoints. The policy only detects virtual machine endpoints that reside on the specified server.

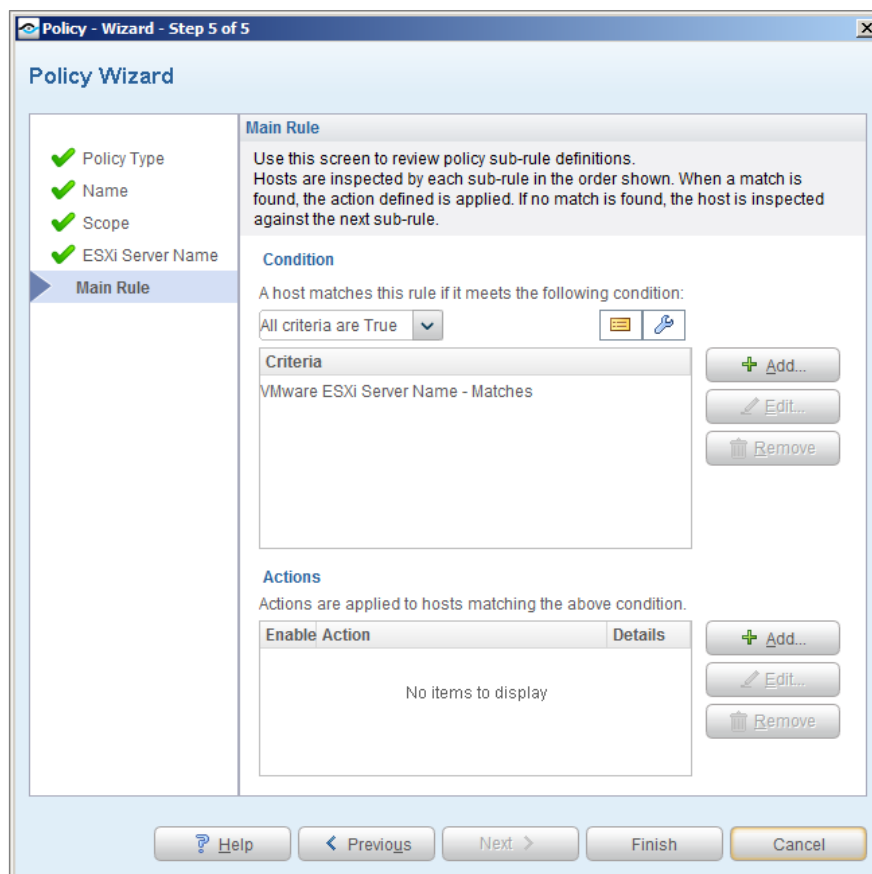


7. In the **ESXi Server Name** field, enter an individual server name of an ESXi server defined in the plugin configuration screen. See [Configure the Plugin](#).
8. Select **Next**. The Main Rule pane lists the main rule of the policy generated by the template. There are no sub-rules in the default policy.

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.



Main Rule Name	Condition Definition
VMware ESXi Server Name	<p>This rule matches endpoints with the VMware ESXi Server name.</p> <p>If the ESXi Server name matches correctly, no remediation action is applied.</p>

9. Select Finish

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

11. Select the **Start** button to execute the policy.

Create Custom VMware vSphere Policies

Custom CounterACT policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy to instruct CounterACT 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

CounterACT policy properties let you instruct CounterACT to detect hosts with specific attributes. For example, create a policy that instructs CounterACT to detect hosts running a certain operating system or with a certain application installed.

Actions

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

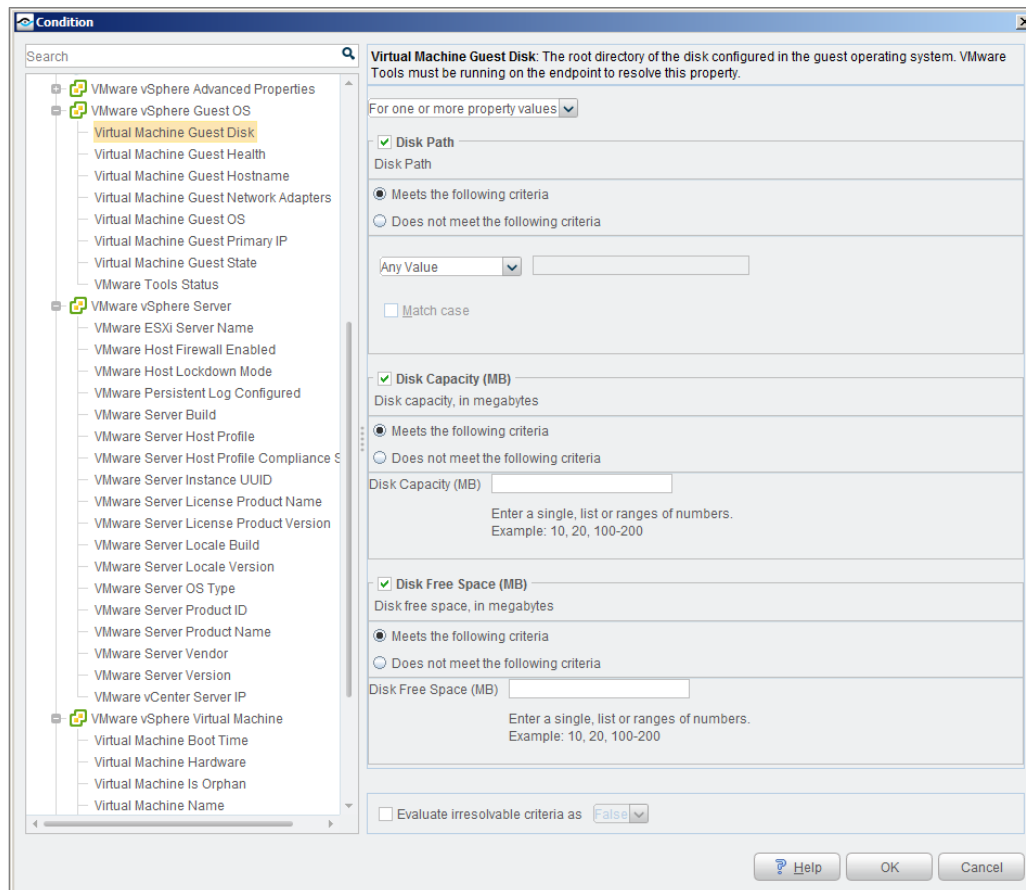
VMware vSphere Plugin Properties and Actions

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, see the *Console User Manual*.

Detecting Virtual Devices – Host Properties

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



The following properties are available:

- [VMware vSphere Advanced Properties \(if configured\)](#)
- [VMware Guest OS Properties](#)
- [VMware vSphere Server Properties](#)
- [VMware Virtual Machine Properties](#)
- [Additional Host Properties](#)

VMware vSphere Advanced Properties

The host dynamic advanced properties allow you the flexibility to set your customized policy with the advanced options. Two types are supported:

- 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 CounterACT VMware vSphere Plugin.

Hardening Guide Properties	CounterACT Properties
ESXi.config-persistent-logs	VMware Persistent Log Configured
ESXi.enable-normal-lockdown-mode ESXi.enable-strict-lockdown-mode	VMware Host Lockdown Mode
ESXi.firewall-enabled	VMware Host Firewall Enabled

Virtual Machine Dynamic Properties

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

<http://www.vmware.com/security/hardening-guides.html>

Hardening Guide Properties	CounterACT Properties
VM.disable-hgfs	isolation.tools.hgfsServerSet.disable
VM.disable-unexposed-features-autologon	isolation.tools.ghi.autologon.disable
VM.disable-VMtools-autoinstall	isolation.tools.autoInstall.disable
VM.restrict-host-info	tools.guestlib.enableHostInfo
VM.disable-console-gui-options	isolation.tools.setGUIOptions.enable

ESXi Host Dynamic Properties

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

<http://www.vmware.com/security/hardening-guides.html>

Hardening Guide Properties	CounterACT Properties
ESXi.set-shell-interactive-timeout	UserVars.ESXiShellInteractiveTimeOut
ESXi.set-shell-timeout	UserVars.ESXiShellTimeOut
ESXi.enable-remote-syslog	Syslog.global.logHost
ESXi.set-account-lockout	Security.AccountLockFailures
ESXi.set-account-auto-unlock-time	Security.AccountUnlockTime

See also: [To set an advanced property to display in Inventory View.](#)

VMware Guest OS Properties

Below is a list of all the static virtual machine properties found 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.

Virtual Machine Guest Disk	Indicates information about the disk on which the guest runs. VMware Tools must be running on the endpoint to resolve this property.
virtual machine Guest Health	Indicates the general health of the guest by reporting the worst alarm/configuration status of the guest. Valid values: <ul style="list-style-type: none"> Definite problem (VMware red status) Entity OK (VMware yellow status) Possible problem (VMware green status) Status unknown (VMware gray status) This value may be influenced by the Query Interval configured for the VMware server that manages the virtual machine.
Virtual Machine Guest Hostname	Indicates the hostname of the guest operating system. VMware Tools must be running on the endpoint to resolve this property.
Virtual Machine Guest Network Adapters	Indicates information about virtual network controllers defined in the guest. VMware Tools must be running on the endpoint to resolve this property.
Virtual Machine Guest OS	Indicates the operating system running on the guest.
Virtual Machine Guest Primary IP	Indicates the primary IP address of the guest operating system. VMware Tools must be running on the endpoint to resolve this property.
Virtual Machine Guest State	Indicates the most recent operation mode of the guest operating system reported to CounterACT. 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.

VMware Tools Status	Indicates whether VMware Tools is installed and running in the guest.
----------------------------	---

VMware vSphere Server Properties

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

VMware ESXi Server Name	Indicates the hostname of the ESXi server.
VMware Host Firewall Enabled	Indicates whether the firewall is enabled on the ESXi server.
VMware Host Lockdown Mode	Indicates the lockdown mode on the ESXi server. Options are <ul style="list-style-type: none"> ▪ Disabled ▪ Normal ▪ Strict
VMware Persistent Log Configured	Indicates whether the ESXi host is configured with persistent logging.
VMware Server Build	Indicates the build number of the software running on the ESXi server that hosts the virtual machine, or the vCenter server.
VMware Server Host Profile	Indicates the host profile configured on the ESXi server.
VMware Server Host Profile Compliance Status	Indicates the ESXi server host profile compliance status. Options are: <ul style="list-style-type: none"> ▪ Compliant ▪ Noncompliant ▪ Unknown
VMware Server Instance UUID	Indicates the Universally Unique Identifier (UUID) of the ESXi server that hosts the virtual machine, or the vCenter server.
VMware Server License Product Name	Indicates the product name as it appears in the license for the ESXi server that hosts the virtual machine, or the vCenter server.
VMware Server License Product Version	Indicates the product version as it appears in the license for the ESXi server that hosts the virtual machine, or the vCenter server.
VMware Server Locale Build	Indicates the locale build of the ESXi server that hosts the virtual machine, or the vCenter server.
VMware Server Locale Version	Indicates the locale version of the ESXi server that hosts the virtual machine, or the vCenter server.
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 VirtualCenter 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 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 vSphere Virtual Machine Properties

Below is a list of all the static virtual machine properties found 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**.
2. The Condition dialog box opens.
3. In the left pane, expand **VMware Virtual Machine** and then select a property.

Virtual Machine Boot Time	Indicates the date and time of the most recent reboot of the virtual machine reported to CounterACT. This value may be influenced by the Query Interval configured for the VMware server that manages the virtual machine.
Virtual Machine Hardware	Indicates the hardware configured for the virtual machine.
Virtual Machine is Orphan	Indicates whether the virtual machine is an orphan.
Virtual Machine Name	The name of the virtual machine.
Virtual Machine Peripheral Devices	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.

Virtual Machine Power State	Indicates the most recent power state for the virtual machine reported to CounterACT. This value may be influenced by the Query Interval configured for the VMware server that manages the virtual machine. This value may be influenced by the Query Interval configured for the VMware server that manages the virtual machine.
Virtual Machine Usage CPU (one thousandth)	The average virtual machine CPU usage in 1/1000 (one thousandth) fraction.
Virtual Machine Usage Disk I/O (KBps)	The Virtual machine disk input/output usage per second (KBps).
Virtual Machine Usage Network I/O (KBps)	The Virtual machine network input/output usage per second (KBps).
Virtual Machine CPU Ready (%)	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.
Virtual Machine CPU Usage (%)	The percentage of the total CPU usage for all vCPUs allocated to the VM.
Virtual Machine Disk Usage (%)	The percentage of the total disk size used by the VM on all VMware data stores associated with the VM.
Virtual Machine Memory Usage (%)	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.

Managing Virtual Devices – Policy Actions

This section describes the actions that are available when the VMware vSphere plugin is installed. The following actions are available:

- [Block Virtual Machine Network Access](#)
- [Change Virtual Machine Port Group](#)
- [Install/Upgrade VMware Tools](#)
- [Power Off Virtual Machine](#)
- [Power On Virtual Machine](#)
- [Reboot Virtual Machine Guest](#)
- [Reset Virtual Machine](#)
- [Set Performance Measurement Period](#)
- [Shut Down Virtual Machine Guest](#)
- [Standby Virtual Machine Guest](#)
- [Suspend Virtual Machine](#)

Action thresholds have been 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, see *Working with Action Thresholds* in the *Console User Manual*.

Below is a list of all the static virtual machine actions found by adding an action in the Main Rule or Sub-Rule of a policy.

To access the virtual machine actions:

1. In the Main Rule or the Sub-Rule of a policy, select **Add**.
2. Name the new rule / sub-rule and select **OK**.
3. The Policy - Sub-Rule dialog box opens.
4. Under Actions, select **Add**.
5. The Action dialog box opens. In the left pane, expand **VMware vSphere** and then select an action you want to add.

Block Virtual Machine Network Access	<p>This action disconnects all network adapters of a virtual machine in a VMware environment.</p> <p>An action threshold is defined for this action in CounterACT. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.</p>
Change Virtual Machine Port Group	<p>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.</p> <p>An action threshold is defined for this action in CounterACT. By default, the action can be applied to no more than 2% of the endpoints managed by each Appliance.</p>
Install/Upgrade VMware Tools	<p>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.</p>
Power Off Virtual Machine	<p>This action powers off a virtual machine in a VMware environment.</p> <p>An action threshold is defined for this action in CounterACT. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.</p>
Power On Virtual Machine	<p>This action powers on a virtual machine in a VMware environment. If the endpoint is in the <i>Suspended</i> state, this action restores the endpoint to the running state.</p>

Reboot Virtual Machine Guest	<p>This action initiates reboot of the guest operating system on a virtual machine in a VMware environment.</p> <p>An action threshold is defined for this action in CounterACT. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.</p>
Reset Virtual Machine	<p>This action performs a hard reset of a virtual machine in a VMware environment.</p> <p>An action threshold is defined for this action in CounterACT. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.</p>
Set Performance Measurement Period (hours)	<p>Set the performance measurement period in hours for the CPU, disk and network I/O usage.</p>
Shut Down Virtual Machine Guest	<p>This action initiates a clean shutdown of the guest operating system and all its services running on a virtual machine in a VMware environment.</p> <p>An action threshold is defined for this action in CounterACT. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.</p>
Standby Virtual Machine Guest	<p>This action alerts the guest operating system to prepare to be suspended. This action applies to virtual machines in a VMware environment.</p>
Suspend Virtual Machine	<p>This action suspends a virtual machine in a VMware environment.</p> <p>An action threshold is defined for this action in CounterACT. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.</p>

- Set your parameters for the action and then select **OK**.

Using the VMware vSphere Plugin

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

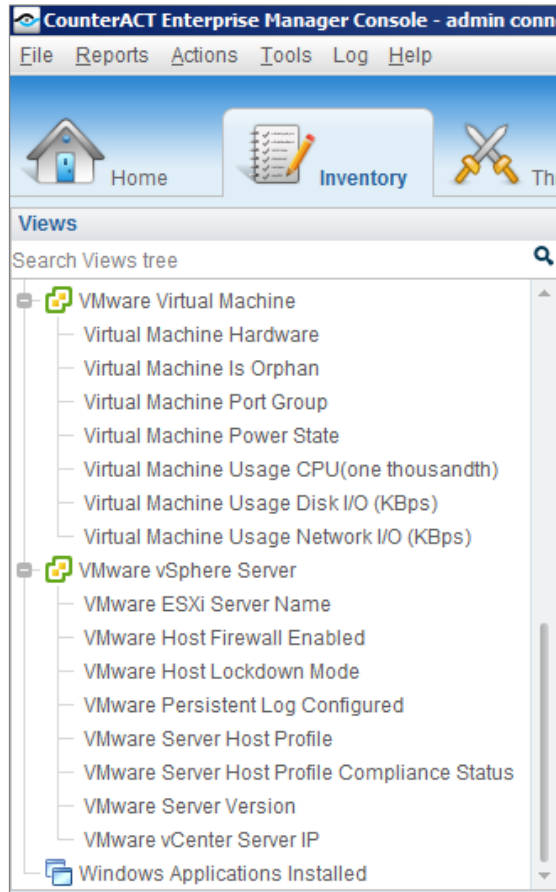
- Total number of ESXi hosts discovered
- Total number of VMs discovered
- VMs classified based on its guest OS
- VMs per ESXi host

- VMs per vSphere tag

Access the Inventory

To access the Inventory:

1. Select the Inventory icon from the Console toolbar.
2. Navigate to the Inventory entries related to this plugin.



Viewing Advanced Properties

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

To set an advanced property to display in Inventory view:

1. In the CounterACT Console, select **Options** from the **Tools** menu.
2. In the left pane, select **VMware vSphere**. The VMware vSphere pane displays.
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**.

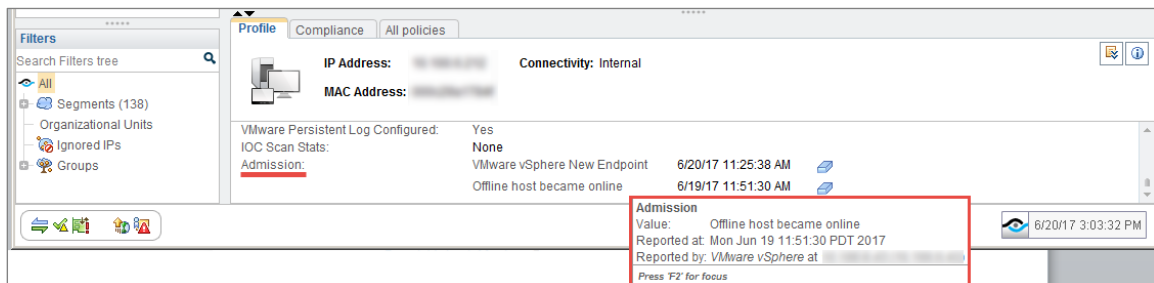
Refer to *Working at the Console>Working with Inventory Detections* in the *CounterACT Console User's Manual* or the Console, Online Help for information about how to work with the CounterACT Inventory.

Reviewing Admission Events

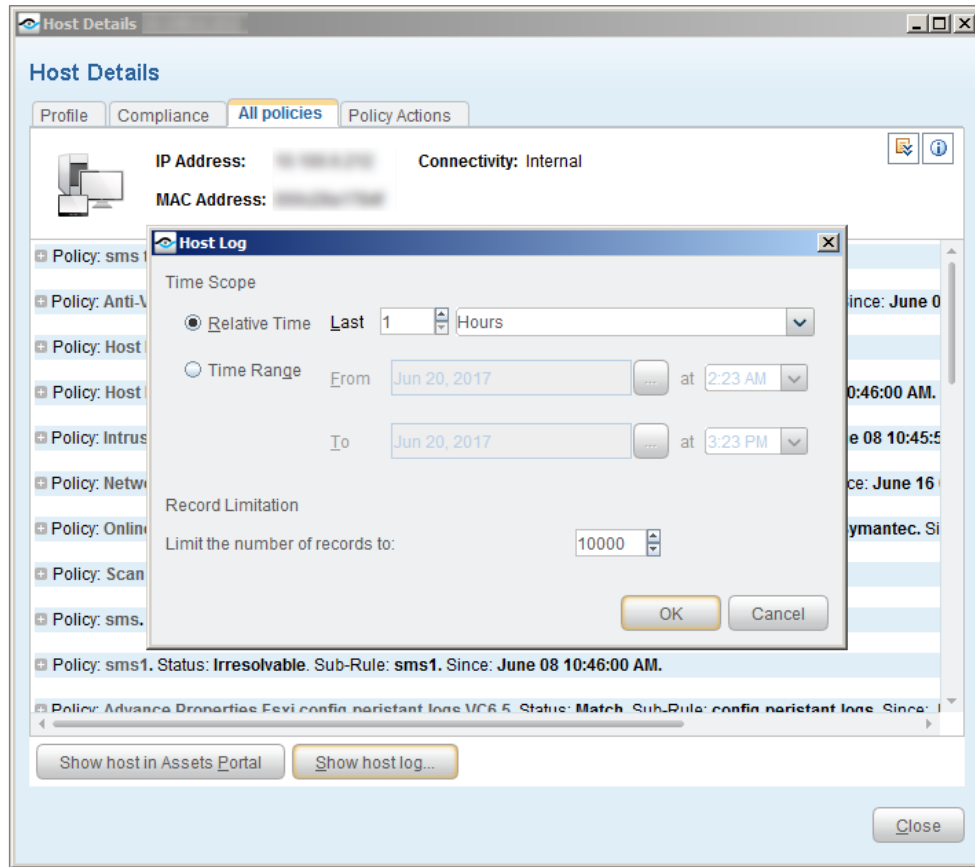
The VMware vSphere Plugin detects all new endpoints and displays them in the profile of the endpoint. This event is generated once, when the new endpoint is first detected by the plugin.

To review an admission event:

1. Login in to the CounterACT Console and select All Hosts.
2. The Detections pane opens. 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 opens in a pop-up.



4. If you require further information, double-clicking the item in the table opens the Host Details dialog box.
5. Select the All policies tab and then select Show host log. The Host Log dialog box opens.



6. Enter the parameters for running the log on and then select **OK**.
7. The Host Log is displayed with all the information. You can export or print the results.

Refer to *Working at the Working with Properties > Event Properties* in the *CounterACT Console User's Manual* or the Console, Online Help for information about how to work with the CounterACT Event properties.

Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- [Documentation Portal](#)
- [Product Updates Portal](#)
- [CounterACT Console Online Help Tools](#)

Documentation Portal

The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features, functionality and integrations.

To access the Documentation Portal:

1. Go to https://updates.forescout.com/support/files/counteract/docs_portal/.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Product Updates Portal:

1. Go to <https://updates.forescout.com/support/index.php?url=counteract>.
2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

Console User Manual

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Plugins**.
2. Select the plugin and then select **Help**.

Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Legal Notice

© 2018 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.

2018-10-07 17:00