# Table of Contents

**About VMware vSphere® Integration** ........................................................... 4  
Use Cases ................................................................................................... 4  
Data Center Visibility ................................................................................ 4  
Data Center Assessment & Compliance ....................................................... 5  
Data Center Control .................................................................................. 5  
Additional VMware Documentation .......................................................... 5  

**About this Plugin** ......................................................................................... 6  
What to Do .................................................................................................. 6  

**Requirements** ............................................................................................ 6  
CounterACT Requirements ............................................................................. 6  
Networking Requirements ............................................................................. 6  
Supported Vendor Requirements .................................................................... 7  
About Support for Dual Stack Environments .................................................. 7  

**Define CounterACT Users in the VMware Environment** ............................ 7  
Defining a vSphere Role ................................................................................ 7  
Define Users with a CounterACT Role .............................................................. 9  

**Configure the Plugin** .................................................................................. 10  
Define Target ESXi Host or vCenter Server .................................................... 10  
Add VMware Advanced Properties ................................................................. 13  
Verify That the Plugin Is Running ................................................................. 14  

**Test the VMware Connection** ................................................................. 15  

**View the VMware vSphere Connection** ...................................................... 15  

**Run VMware vSphere Policy Templates** .................................................. 16  
VMware Classification Template .................................................................... 17  
VMware ESXi Host Firewall Compliance ..................................................... 21  
VMware ESXi Host Lockdown Compliance ................................................... 24  
VMware ESXi Host Log Persistent Compliance .......................................... 27  
VMware ESXi Host Profile Compliance ........................................................ 31  
VMware Low Usage Virtual Machines Template ........................................... 34  
VMware Tools Compliance Template ........................................................... 38  
VMware Virtual Machines by ESXi Server Template ................................... 43  

**Create Custom VMware vSphere Policies** ................................................. 46  
Detecting Virtual Devices – Host Properties ............................................... 48  
VMware vSphere Advanced Properties ....................................................... 49
Using the VMware vSphere Plugin ................................................................. 55
   Best Practices .......................................................................................... 55
   Independent vCenter or ESXi Appliance(s) .............................................. 55
   High Redundancy vSphere Designs ......................................................... 57
Access the Asset Inventory ........................................................................ 58
View Advanced Properties ........................................................................ 59
Review Admission Events .......................................................................... 60

Hybrid Cloud Module Information ............................................................. 61

Additional CounterACT Documentation ..................................................... 62
   Documentation Downloads ...................................................................... 62
   Documentation Portal ............................................................................. 62
   CounterACT Help Tools ......................................................................... 63
About VMware vSphere® Integration

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

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

This section describes use cases supported by this module. Be sure to review the Best Practices.

Data Center Visibility

When considering data center visibility, the focus is on the properties that CounterACT can collect from the vSphere environment through integration. This can be through a simple device, operating system properties, specific security groups or tags applied to a guest.

When gathering a better understanding of VMware ESXi hosts, look first at being able to recognize an ESXi host without SPAN or nmap banner. Since the NIC vendor would be generic to the vendor of server, being able to recognize the device as a host is a great start. After that, capture properties such as:

- the connected profile and profile compliance
- product ID and licensing for CounterACT compliance state in policy
- connected vCenter server that can be used for inventory purposes

Regarding visibility of guest virtual machines, you can gather insight into what is lost through the abstraction of the virtual layer. You can also get some properties that are not readily available from physical systems by default. CounterACT can gather guest properties related to resources, state, portgroup, 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, by default, the OS captured through this integration is leveraged by the Device Profile Library Plugin in a policy utilizing primary classification conditions. See the VMware Classification Template.
**Data Center Assessment & Compliance**

When moving from visibility to assessment and compliance, some properties are already established, for example, host profile compliance and host firewall enablement. Beyond these points, your specific goals should be addressed.

When addressing VMware vSphere servers, properties to review are:

- orphaned guest virtual machines
- server software version
- SSH service running
- account lockout failure
- non-standard configurations

In regards to the guest, one could look at VMware Tools or the correlation of the system with its portgroup. To move beyond that, NSX Security Groups provide the ability to limit the exposure of systems based on operational and security goals established within your corporate policy. See [Run VMware vSphere Policy Templates](#) and [VMware vSphere Advanced Properties](#).

**Data Center Control**

Taking a step beyond assessment and compliance, CounterACT can send non-affecting notifications via email or SIEM messages, and gradients up to and including a heavy-handed portgroup move. 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. An example of this task is installing VMware Tools on a guest. Finally, instead of doing a portgroup 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 affect to 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 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. Review the Best Practices.
3. Define CounterACT Users in the VMware Environment
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 plugin requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0.
- Hybrid Cloud Module version 1.0 with the VMware vSphere component running

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)

**About Support for Dual Stack Environments**

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, **IPv6 addresses are not yet supported by this component.** The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this component.

**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`
   - `VirtualMachine.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.

![Assign Permissions dialog](image)

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 in [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.

---

**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.

<table>
<thead>
<tr>
<th><strong>VMware Server Name or IP Address</strong></th>
<th>Enter the hostname or IP address of the 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. The vCenter Server can have their own types of events, tasks, metadata, and privileges.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Enter the username required to log in to the server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password required to log in to the server.</td>
</tr>
<tr>
<td><strong>Verify Password</strong></td>
<td>Re-enter the password.</td>
</tr>
</tbody>
</table>
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.
- 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) | Specify how frequently the plugin should query the VMware server.

- 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.

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) | 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.

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.
3. Define the property parameters.

| Name | Enter the name of the VMware property. Valid characters to use are:  
|------|-----------------------------------------------------------------------|
|      | ▪ Alphabet  
|      | ▪ Numerical  
|      | ▪ Underscore  
|      | ▪ Punctuation - period, comma, hyphen and space.                      |

| Description | (Optional) Enter a description of the property. Valid characters to use are:  
|-------------|-----------------------------------------------------------------------|
|             | ▪ 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:
- Alphabet
- Numerical
- Underscore
- Punctuation - period, comma, hyphen and space.
See [VMware vSphere Advanced Properties](#).

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

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

---

4. Make any settings 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](#).

---

**Verify That the Plugin Is Running**

After configuring the plugin, verify that it is running.

To verify:

1. Select **Tools > Options** and then select **Modules**.
2. 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 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.

![VMware vSphere pane screenshot](image)

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 <strong>Apply</strong> in the VMware vSphere configuration pane to save this server definition.</td>
</tr>
<tr>
<td>Down</td>
<td>CounterACT cannot connect to the server.</td>
</tr>
<tr>
<td>Up</td>
<td>CounterACT can connect to the server.</td>
</tr>
</tbody>
</table>
Hybrid Cloud Module: VMware vSphere® Plugin Configuration Guide

<table>
<thead>
<tr>
<th>Managed</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Used</td>
<td>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.</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>

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 Virtual Machines by ESXi Server Template - generates a policy that detects virtual machines hosted by a specific ESXi server.

 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.
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**

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 page.
– **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 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:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</th>
</tr>
</thead>
</table>
| VMware Virtual Machine   | This rule matches endpoints with any of the following values:  
  • Virtual Machine Name – Any Value  
  • NIC Vendor – VMWARE, INC  
  • Device Interfaces – Starts With: VMware Accelerated  
  The Add to Group action adds detected endpoints to the VMware virtual machines group. This action is enabled by default. |
| VMware ESXi Server       | This rule matches endpoints with VMware Server Product ID list values of gsx, embeddedEsx and esx.  
  The Add to Group action adds detected endpoints to the VMware ESXi Servers group. This action is enabled by default. |
| VMware vCenter Server    | This rule matches endpoints with VMware Server Product ID values of vpx.  
  The Add to Group action adds detected endpoints to the VMware ESXi Servers group. This action is enabled by default. |
See the CounterACT Administration 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.
3. Select VMware vSphere and then select VMware ESXi Host Firewall Compliance.
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

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 page.
- **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 appears in the Scope pane.

**9.** 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.

**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.

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.
10. 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>Firewall Disabled</td>
<td>This rule checks if the firewall on the VMware host is disabled.</td>
</tr>
</tbody>
</table>

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 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.

**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**

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 page.
– **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 appears in the Scope pane.

9. 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.

**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.

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.

10. 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>

11. Select **Finish**

12. 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 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.
3. Select VMware vSphere and then select VMware ESXi Host Log Persistent Compliance.
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**

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 page.
– **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 appears in the Scope pane.

9. 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.

### 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.

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.

10. 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.

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 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.
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

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 page.

– **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 appears in the Scope pane.

9. 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.

**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.

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

10. Select Finish
11. In the CounterACT Policy Manager, select Apply to save the policy.
12. 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.
3. Select VMware vSphere and then select VMware Low Usage Virtual Machines.
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**

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 page.
   - **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 appears in the Scope pane.

9. 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.

**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.

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. The period of the measurement can be configured using the plugin configuration or customized with the <a href="#">Set Performance Measurement Period</a> action.</td>
</tr>
</tbody>
</table>

**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 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.

**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**

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 page.
- **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 appears in the Scope pane.

9. 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.
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.

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.

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Condition Definition</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>
</tbody>
</table>
VMware Tools installed and upgrade recommended

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

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 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 endpoint is not managed correctly by the VMware server

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 is 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.

10. Select Finish

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

12. Select the Start button to execute the policy.
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.
3. Select VMware vSphere and then select VMware Virtual Machines by ESXi Server.
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.
   
   To create a unique, descriptive policy name, specify the target ESXi server in the policy name.

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

**Define which Endpoints will be Inspected - Policy Scope**

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 page.
   - **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**. 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.

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.

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.
Hybrid Cloud Module: VMware vSphere® Plugin Configuration Guide

Main Rule

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

11. Select Finish

12. In the CounterACT Policy Manager, select Apply to save the policy.
13. 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 CounterACT Administration Guide.
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.

<table>
<thead>
<tr>
<th>Hardening Guide Properties</th>
<th>CounterACT 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 will 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>CounterACT 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.setUIOptions.enable</td>
</tr>
</tbody>
</table>
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.


<table>
<thead>
<tr>
<th>Hardening Guide Properties</th>
<th>CounterACT 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
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.

<table>
<thead>
<tr>
<th>Virtual Machine Guest Disk</th>
<th>Indicates information about the disk on which the guest runs. VMware Tools must be running on the endpoint to resolve this property.</th>
</tr>
</thead>
<tbody>
<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 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 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 State</td>
<td>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.</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>VMware ESXi Server Name</th>
<th>Indicates the hostname of the ESXi server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Host Firewall Enabled</td>
<td>Indicates whether the firewall is enabled on the ESXi server.</td>
</tr>
</tbody>
</table>
| VMware Host Lockdown Mode | Indicates the lockdown mode on the ESXi server. Options are:  
  - 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:  
  - 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 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).

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 CounterACT Administration Guide.

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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Block Virtual Machine Network Access</strong></td>
<td>This action disconnects all network adapters of a virtual machine in a VMware environment.</td>
</tr>
<tr>
<td></td>
<td>An action threshold is defined for this action in CounterACT. By default, the action can be</td>
</tr>
<tr>
<td></td>
<td>applied to no more than 1% of the endpoints managed by each Appliance.</td>
</tr>
<tr>
<td><strong>Change Virtual Machine Port Group</strong></td>
<td>This action changes the port group configured for a virtual machine in a VMware environment.</td>
</tr>
<tr>
<td></td>
<td>When changing to a port group on a virtual switch, only the port group label needs to be</td>
</tr>
<tr>
<td></td>
<td>specified. When changing to a port group on a distributed virtual switch, the switch name must</td>
</tr>
<tr>
<td></td>
<td>also be provided.</td>
</tr>
<tr>
<td></td>
<td>An action threshold is defined for this action in CounterACT. By default, the action can be</td>
</tr>
<tr>
<td></td>
<td>applied to no more than 2% of the endpoints managed by each Appliance.</td>
</tr>
<tr>
<td><strong>Install/Upgrade VMware Tools</strong></td>
<td>This action installs or upgrades VMware Tools on a virtual machine in a VMware environment.</td>
</tr>
<tr>
<td></td>
<td>Initial installation of VMware Tools may require user interaction within the guest virtual</td>
</tr>
<tr>
<td></td>
<td>machine, but upgrades are implemented automatically.</td>
</tr>
<tr>
<td><strong>Power Off Virtual Machine</strong></td>
<td>This action powers off a virtual machine in a VMware environment.</td>
</tr>
<tr>
<td></td>
<td>An action threshold is defined for this action in CounterACT. By default, the action can be</td>
</tr>
<tr>
<td></td>
<td>applied to no more than 1% of the endpoints managed by each Appliance.</td>
</tr>
<tr>
<td><strong>Power On Virtual Machine</strong></td>
<td>This action powers on a virtual machine in a VMware environment.</td>
</tr>
<tr>
<td></td>
<td>If the endpoint is in the <em>Suspended</em> state, this action restores the endpoint to the running</td>
</tr>
<tr>
<td></td>
<td>state.</td>
</tr>
<tr>
<td><strong>Reboot Virtual Machine Guest</strong></td>
<td>This action initiates reboot of the guest operating system on a virtual machine in a VMware</td>
</tr>
<tr>
<td></td>
<td>environment.</td>
</tr>
<tr>
<td></td>
<td>An action threshold is defined for this action in CounterACT. By default, the action can be</td>
</tr>
<tr>
<td></td>
<td>applied to no more than 1% of the endpoints managed by each Appliance.</td>
</tr>
<tr>
<td><strong>Reset Virtual Machine</strong></td>
<td>This action performs a hard reset of a virtual machine in a VMware environment.</td>
</tr>
<tr>
<td></td>
<td>An action threshold is defined for this action in CounterACT. By default, the action can be</td>
</tr>
<tr>
<td></td>
<td>applied to no more than 1% of the endpoints managed by each Appliance.</td>
</tr>
<tr>
<td><strong>Set Performance Measurement Period (hours)</strong></td>
<td>Set the performance measurement period in hours for the CPU, disk and network I/O usage.</td>
</tr>
<tr>
<td><strong>Shut Down Virtual Machine Guest</strong></td>
<td>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 CounterACT. By default, the action can be applied to no more than 1% of the endpoints managed by each Appliance.</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Standby Virtual Machine Guest</strong></td>
<td>This action alerts the guest operating system to prepare to be suspended. This action applies to virtual machines in a VMware environment.</td>
</tr>
<tr>
<td><strong>Suspend Virtual Machine</strong></td>
<td>This action suspends a virtual machine in a VMware environment. 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.</td>
</tr>
</tbody>
</table>

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

### Using the VMware vSphere Plugin

This section covers the best practices for using the Hybrid Module: VMware vSphere Plugin.

### Best Practices

This section covers common customer VMware environment scenarios and the associated Best Practice CounterACT Solution Design.

### Independent vCenter or ESXi Appliance(s)

The two simplest designs of a vSphere environment are:

- One-to-one CounterACT
- VMware vCenter or ESXi server

In either case, the model is to assign one CounterACT to each VMware server and the same CounterACT manages the IP addresses associated with that server. This design scales horizontally as more VMware servers are introduced and more CounterACT connecting endpoint management appliances are added.
Best practice configuration:

- The managing CounterACT appliances for the vCenters and the segments are on the same CounterACT appliances.

vCenter-only Configuration
vCenter and NSX Configuration

**High Redundancy vSphere Designs**

This section addresses the more common high redundancy VMware virtualization environments:

- vCenter High Availability (HA) Clustering
- vSphere Fault Tolerance (FT)
- vCenter Self-Monitoring Agent

**vCenter High Availability (HA) Clustering**

In the High Availability Clustering environment, vCenter is functioning in a hot/warm standby configuration; however, only one of the vCenter servers will have assigned servers and guests at any one time. In this case, you can assign a single vSphere Server integration to a separate CounterACT appliance that allows both the vSphere and CounterACT environments to be designed for HA. The typical model for integration is to assign one CounterACT to each vSphere server and the CounterACT connected to the active vCenter server manages the IP addresses associated with that server.

There are two options for scaling this design beyond one vCenter HA cluster:

1. As more VMware servers are introduced, scale horizontally by adding additional CounterACT appliances.
2. If there are limited CounterACT appliances, have two CounterACT appliances act as connecting appliance for both the active and standby vCenter server. Each CounterACT appliance is connected to both an active vCenter server that manages the IP addresses associated with it and the associated standby vCenter server.

The down-side to this option is that should the CounterACT appliance become unavailable, the connection to the specified vCenter environment is lost.

**vSphere Fault Tolerance (FT)**

The VMware vSphere® Fault Tolerance product allows for guest hosts of virtual machines to be seamlessly migrated from one failed vSphere host server to another that has available resources. Since the connection from CounterACT to vCenter is not affected by this feature, it does not affect the environment.

**vCenter Self-Monitoring Agent**

The VMware vCenter Self-Monitoring Agent, part of the VMware vRealize® product, allows for advanced monitoring of supported OS guest hosts (virtual machines). Since the connection from CounterACT to vCenter is not affected by this feature, it does not affect the environment.

**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 CounterACT Console. This provides activity information, accurate at the time of the poll, on cloud endpoints based on certain instances’ properties. The Asset 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

To access the Inventory:
1. Select the Inventory icon from the Console toolbar.
2. Navigate 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 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 Administration Guide* for information about how to work with the CounterACT Inventory. See *Additional CounterACT 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 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 Administration Guide* for information about how to work with the CounterACT Event properties. See *Additional CounterACT Documentation* for information on how to access the guide.

---

**Hybrid Cloud Module Information**

The VMware vSphere plugin is installed with the CounterACT Hybrid Cloud Module. The ForeScout CounterACT® Hybrid Cloud Module provides See, Control and Orchestrate functions across physical and virtual devices that are on-premises and off-premises through the following plugin integrations:

- AWS Plugin
- VMware NSX Plugin
- VMware vSphere Plugin

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

Plugins listed above are installed and rolled back with the Hybrid Cloud Module. Refer to the *ForeScout CounterACT Hybrid Cloud Module Overview Guide* for more module information, such as module requirements, upgrade and rollback instructions.
Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** - Product Updates Portal
- **Centralized Licensing Mode** - Customer Portal

*Software downloads are also available from these portals.*

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

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

**To access the Product Updates Portal:**

2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

**To access documentation on the ForeScout Customer Portal:**

2. Select Downloads or Documentation.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.
If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT 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.

CounterACT Administration Guide
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 Modules.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.

Identifying Your Licensing Mode in the Console
If your Enterprise Manager has a ForeScout CounterACT See license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select Options > Licenses to see whether you have a ForeScout CounterACT See license listed in the table.

Contact your ForeScout representative if you have any questions about identifying your licensing mode.
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.

2018-04-30 14:59