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

### About This Book

Getting Started with VCM

  - Running VCM as Administrator on the Collector [11]
  - Log In to VCM [12]
- Getting Familiar with the Portal [13]
  - General Information Bar [13]
  - Toolbar [14]
  - Sliders [15]
- Customizing VCM for your Environment [16]

Installing and Getting Started with VCM Tools

- Install the VCM Tools Only [19]
- VCM Import/Export and Content Wizard Tools [20]
  - Run the Import/Export Tool [21]
  - Run the Content Wizard to Access Additional Compliance Content [21]
- Run the Deployment Utility [21]
- Package Studio [22]
- Foundation Checker [22]

Configuring VMware Cloud Infrastructure

- Virtual Environments Configuration [23]
- Managing Agents [23]
- Managing vCenter Server Instances, Hosts, and Guest Virtual Machines [24]
- Managing Instances of vCloud Director and vApp Virtual Machines [25]
- Managing vShield Manager Instances [25]
- Configure Virtual Environments Collections [25]
- Configure Managing Agent Machines [26]
  - Collect Machines Data From the Managing Agent Machines [27]
  - Set the Trust Status for Managing Agent Machines [27]
  - Configure HTTPS Bypass Setting [28]
  - Enable Managing Agent Machines [28]
- Obtain the SSL Certificate Thumbprint [29]
- Configure vCenter Server Data Collections [30]
  - Add vCenter Server Instances [30]
  - Configure the vCenter Server Settings [31]
  - Collect vCenter Server Data [32]
  - vCenter Server Collection Results [33]
  - Configure vCenter Server Scheduled Collections [33]
- Configure vCenter Server Virtual Machine Collections [35]
  - Collect vCenter Server Virtual Machines Data [35]
  - Manage vCenter Server Virtual Machines [36]
- Configure vCloud Director Collections [37]
  - Add vCloud Director Instances [37]
  - Configure the vCloud Director Settings [38]
  - Collect vCloud Director Data [39]
  - vCloud Director Collection Results [40]
- Configure vCloud Director vApp Virtual Machines Collections [41]
  - Network Address Translation and vCloud Director vApp Discovery Rules [41]
<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Configuration Manager Administration Guide</td>
</tr>
<tr>
<td>Discover vCloud Director vApp Virtual Machines</td>
</tr>
<tr>
<td>Configure vShield Manager Collections</td>
</tr>
<tr>
<td>Configure ESX Service Console OS Collections</td>
</tr>
<tr>
<td>Configure the Collector as an Agent Proxy</td>
</tr>
<tr>
<td>Configure Virtual Machine Hosts</td>
</tr>
<tr>
<td>Copy Files to the ESX/ESXi Servers</td>
</tr>
<tr>
<td>Collect ESX Logs Data</td>
</tr>
<tr>
<td>Virtualization Collection Results</td>
</tr>
<tr>
<td>Configure the vSphere Client VCM Plug-In</td>
</tr>
<tr>
<td>Register the vSphere Client VCM Plug-In</td>
</tr>
<tr>
<td>Configuring the vSphere Client VCM Plug-In Integration Settings</td>
</tr>
<tr>
<td>Manage Machines from the vSphere Client</td>
</tr>
<tr>
<td>Troubleshooting the vSphere Client VCM Plug-In Registration</td>
</tr>
<tr>
<td>Running Compliance for the VMware Cloud Infrastructure</td>
</tr>
<tr>
<td>Create and Run Virtual Environment Compliance Templates</td>
</tr>
<tr>
<td>Create Virtual Environment Compliance Rule Groups</td>
</tr>
<tr>
<td>Create and Test Virtual Environment Compliance Rules</td>
</tr>
<tr>
<td>Create and Test Virtual Environment Compliance Filters</td>
</tr>
<tr>
<td>Preview Virtual Environment Compliance Rule Groups</td>
</tr>
<tr>
<td>Create Virtual Environment Compliance Templates</td>
</tr>
<tr>
<td>Run Virtual Environment Compliance Templates</td>
</tr>
<tr>
<td>Resolve Noncompliant Virtual Environments Template Results</td>
</tr>
<tr>
<td>Enforce Compliance Template Results Using VCM Actions</td>
</tr>
<tr>
<td>Manually Enforce Compliance Template Results</td>
</tr>
<tr>
<td>Create Virtual Environment Compliance Exceptions</td>
</tr>
<tr>
<td>Configure Alerts and Schedule Virtual Environment Compliance Runs</td>
</tr>
<tr>
<td>Create Virtual Environment Compliance Alert Rules</td>
</tr>
<tr>
<td>Create Virtual Environments Compliance Alert Configurations</td>
</tr>
<tr>
<td>Schedule Virtual Environments Compliance Template Runs</td>
</tr>
<tr>
<td>Configuring vCenter Operations Manager Integration</td>
</tr>
<tr>
<td>Configure vCenter Operations Manager Change Events</td>
</tr>
<tr>
<td>Standards Compliance for vCenter Operations Manager</td>
</tr>
<tr>
<td>Configure vCenter Operations Manager Standards Compliance</td>
</tr>
<tr>
<td>Scoring Badges for vCenter Operations Manager Standards Compliance</td>
</tr>
<tr>
<td>Auditing Security Changes in Your Environment</td>
</tr>
<tr>
<td>Configuring Windows Machines</td>
</tr>
<tr>
<td>Configure Windows Machines</td>
</tr>
<tr>
<td>Verify Available Domains</td>
</tr>
<tr>
<td>Check the Network Authority</td>
</tr>
<tr>
<td>Assign Network Authority Accounts</td>
</tr>
<tr>
<td>Discover Windows Machines</td>
</tr>
<tr>
<td>License Windows Machines</td>
</tr>
<tr>
<td>Install the VCM Windows Agent on Your Windows Machines</td>
</tr>
<tr>
<td>Locate the Enterprise Certificate</td>
</tr>
<tr>
<td>Manually Install the VCM Windows Agent</td>
</tr>
<tr>
<td>Manually Uninstall the VCM Windows Agent</td>
</tr>
<tr>
<td>Collect Windows Data</td>
</tr>
<tr>
<td>Windows Collection Results</td>
</tr>
<tr>
<td>Getting Started with Windows Custom Information</td>
</tr>
<tr>
<td>Prerequisites to Collect Windows Custom Information</td>
</tr>
<tr>
<td>Using PowerShell Scripts for WCI Collections</td>
</tr>
<tr>
<td>Windows Custom Information Change Management</td>
</tr>
<tr>
<td>Collecting Windows Custom Information</td>
</tr>
<tr>
<td>Contents</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Create Your Own WCI PowerShell Collection Script</td>
</tr>
<tr>
<td>Verify that Your Custom PowerShell Script is Valid</td>
</tr>
<tr>
<td>Install PowerShell</td>
</tr>
<tr>
<td>Collect Windows Custom Information Data</td>
</tr>
<tr>
<td>Run the Script-Based Collection Filter</td>
</tr>
<tr>
<td>View Windows Custom Information Job Status Details</td>
</tr>
<tr>
<td>Windows Custom Information Collection Results</td>
</tr>
<tr>
<td>Run Windows Custom Information Reports</td>
</tr>
<tr>
<td>Troubleshooting Custom PowerShell Scripts</td>
</tr>
</tbody>
</table>

| Configuring Linux and UNIX Machines | 121 |
| Configure Linux and UNIX Machines | 121 |
| Upgrade Requirements for UNIX/Linux Machines | 122 |
| Add UNIX/Linux Machines | 122 |
| License UNIX/Linux Machines | 123 |
| Install the Agent on UNIX/Linux Machines | 124 |
| Installation Options for Linux or UNIX csi.config | 128 |
| Manually Uninstall the UNIX/Linux Agent | 131 |
| Collect UNIX/Linux Data | 131 |
| Updates to UNIX Patch Assessment Content Affects UNIX Agent Performance | 132 |
| UNIX/Linux Collection Results | 132 |
| Configuring Oracle Instances | 133 |
| Discover Oracle Instances | 133 |
| Edit Oracle Instances | 134 |
| Collect Oracle Data | 138 |
| Oracle Collection Results | 139 |

| Configuring Mac OS X Machines | 141 |
| Configure Mac OS X Machines | 141 |
| Add Mac OS X Machines | 142 |
| License Mac OS X Machines | 143 |
| Install the Agent on Mac OS X Machines | 143 |
| Installation Options for Max OS X csi.config | 146 |
| Manually Uninstall the Mac OS X Agent | 149 |
| Collect Mac OS X Data | 149 |
| Collected Mac OS X Data Types | 150 |
| Mac OS X Collection Results | 151 |

<p>| Patching Managed Machines | 153 |
| VCM Paching for Windows Machines | 153 |
| VCM Paching for UNIX and Linux Machines | 154 |
| UNIX and Linux Patch Assessment and Deployment | 154 |
| New UNIX Patch Assessment Content | 155 |
| Getting Started with VCM Paching | 156 |
| Getting Started with VCM Paching for Windows Machines | 156 |
| Check for Updates to Bulletins | 157 |
| Collect Data from Windows Machines by Using the VCM Paching Filter Sets | 157 |
| Assess Windows Machines | 158 |
| Review VCM Paching Windows Assessment Results | 159 |
| Prerequisites for Patch Deployment | 159 |
| Default Location for UNIX/Linux Patches | 161 |
| Location for UNIX/Linux Patches | 161 |
| Default Location for UNIX/Linux Patches | 162 |
| vCenter Software Content Repository Tool | 162 |
| Deploy Patches to Windows Machines | 163 |
| Getting Started with VCM Paching for UNIX and Linux Machines | 164 |
| Check for Updates to Bulletins | 164 |</p>
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect Patch Assessment Data from UNIX and Linux Machines</td>
<td>165</td>
</tr>
<tr>
<td>Explore Assessment Results and Acquire and Store the Patches</td>
<td>166</td>
</tr>
<tr>
<td>Default Location for UNIX/Linux Patches</td>
<td>168</td>
</tr>
<tr>
<td>Deploy Patches to UNIX/Linux Machines</td>
<td>168</td>
</tr>
<tr>
<td>How the Deploy Action Works</td>
<td>169</td>
</tr>
<tr>
<td>Running VCM Patching Reports</td>
<td>170</td>
</tr>
<tr>
<td>Customize Your Environment for VCM Patching</td>
<td>170</td>
</tr>
<tr>
<td>Running and Enforcing Compliance</td>
<td>171</td>
</tr>
<tr>
<td>Getting Started with SCAP Compliance</td>
<td>171</td>
</tr>
<tr>
<td>Conduct SCAP Compliance Assessments</td>
<td>172</td>
</tr>
<tr>
<td>Provisioning Physical or Virtual Machine Operating Systems</td>
<td>175</td>
</tr>
<tr>
<td>Operating System Provisioning Components</td>
<td>175</td>
</tr>
<tr>
<td>How Operating System Provisioning Works</td>
<td>176</td>
</tr>
<tr>
<td>Configure Operating System Provisioning Servers</td>
<td>177</td>
</tr>
<tr>
<td>Add Operating System Provisioning Servers</td>
<td>178</td>
</tr>
<tr>
<td>Set the Trust Status for Operating System Provisioning Servers</td>
<td>178</td>
</tr>
<tr>
<td>Collect Operating System Distributions</td>
<td>179</td>
</tr>
<tr>
<td>Discover Provisionable Machines</td>
<td>179</td>
</tr>
<tr>
<td>Provision Machines with Operating System Distributions</td>
<td>180</td>
</tr>
<tr>
<td>Provision Windows Machines</td>
<td>180</td>
</tr>
<tr>
<td>Provision Linux Machines</td>
<td>183</td>
</tr>
<tr>
<td>Change Agent Communication</td>
<td>188</td>
</tr>
<tr>
<td>Provisioned Machines Results</td>
<td>189</td>
</tr>
<tr>
<td>Reprovision Machines</td>
<td>189</td>
</tr>
<tr>
<td>Provisioning Software on Managed Machines</td>
<td>193</td>
</tr>
<tr>
<td>Using Package Studio to Create Software Packages and Publish to Repositories</td>
<td>193</td>
</tr>
<tr>
<td>Software Repository for Windows</td>
<td>193</td>
</tr>
<tr>
<td>Package Manager for Windows</td>
<td>193</td>
</tr>
<tr>
<td>Software Provisioning Component Relationships</td>
<td>194</td>
</tr>
<tr>
<td>Install the Software Provisioning Components</td>
<td>194</td>
</tr>
<tr>
<td>Install Software Repository for Windows</td>
<td>195</td>
</tr>
<tr>
<td>Install Package Studio</td>
<td>196</td>
</tr>
<tr>
<td>Install Package Manager on Managed Machines</td>
<td>198</td>
</tr>
<tr>
<td>Using Package Studio to Create Software Packages and Publish to Repositories</td>
<td>199</td>
</tr>
<tr>
<td>Creating Packages</td>
<td>199</td>
</tr>
<tr>
<td>Using VCM Software Provisioning for Windows</td>
<td>201</td>
</tr>
<tr>
<td>Collect Package Manager Information from Machines</td>
<td>201</td>
</tr>
<tr>
<td>Collect Software Repository Data</td>
<td>202</td>
</tr>
<tr>
<td>Add Repository Sources to Package Managers</td>
<td>202</td>
</tr>
<tr>
<td>Install Packages</td>
<td>203</td>
</tr>
<tr>
<td>Related Software Provisioning Actions</td>
<td>205</td>
</tr>
<tr>
<td>Viewing Provisioning Jobs in the Job Manager</td>
<td>205</td>
</tr>
<tr>
<td>Create Compliance Rules Based on Software Provisioning Data</td>
<td>206</td>
</tr>
<tr>
<td>Create Compliance Rules Containing Software Provisioning Remediation Actions</td>
<td>207</td>
</tr>
<tr>
<td>Configuring Active Directory Environments</td>
<td>209</td>
</tr>
<tr>
<td>Configure Domain Controllers</td>
<td>209</td>
</tr>
<tr>
<td>Verify Available Domains</td>
<td>210</td>
</tr>
<tr>
<td>Check the Network Authority Account</td>
<td>210</td>
</tr>
<tr>
<td>Assign Network Authority Accounts</td>
<td>211</td>
</tr>
<tr>
<td>Discover Domain Controllers</td>
<td>211</td>
</tr>
<tr>
<td>License Domain Controllers</td>
<td>212</td>
</tr>
<tr>
<td>Install the VCM Windows Agent on Your Domain Controllers</td>
<td>213</td>
</tr>
<tr>
<td>Collect Domain Controller Data</td>
<td>214</td>
</tr>
</tbody>
</table>
About This Book

The VMware vCenter Configuration Manager Administration Guide describes the steps required to configure VCM to collect and manage data from your virtual and physical environment.

Read this document and complete the associated procedures to prepare for a successful implementation of the components.

Intended Audience

This information is written for experienced Windows or UNIX/Linux/Mac OS X system administrators who are familiar with managing network users and resources and with performing system maintenance.

To use this information effectively, you must have a basic understanding of how to configure network resources, install software, and administer operating systems. You also need to fully understand your network topology and resource naming conventions.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

VMware VCM Documentation

The vCenter Configuration Manager (VCM) documentation consists of the VCM Installation Guide, VCM Troubleshooting Guide, VCM online Help, and other associated documentation.
Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

**Online and Telephone Support**

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

**Support Offerings**

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

**VMware Professional Services**

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.
Getting Started with VCM

When you use VCM, you must understand user access and how to start VCM from any physical or virtual machine. You must also familiarize yourself with the VCM Web Console features.

This chapter includes the following topics:

- Understanding User Access 11
- Log In to VCM 12
- Getting Familiar with the Portal 13
- Customizing VCM for your Environment 16

Understanding User Access

User access determines who has access to VCM and with what roles. To manage your user access, create rules that are assigned to roles. VCM assigns the roles to each user login you create. User access is managed in the Administration User Manager node.

The user account that was used to install VCM is automatically granted access to VCM, placed in the roles of ADMIN and USER, and placed into the Admin role. This user can log in to VCM using the Admin role. The AD_Admin role allows full administration access to AD objects only.

When a user is added to the Admin role in VCM or granted access to the Administration User Manager node, that user is placed in the fixed machine roles Security Administrators and Bulk Insert Administrators Groups. They are also added to the database roles of public, ADMIN, and User in the VCM Database.

Users who will not have access to the Administration User Manager node will be assigned to public. Depending on the functions granted to a user, they might need additional or fewer privileges for their role to function properly.

VCM provides a Change Restricted role to limit users from making certain changes in your environment. With this role, users can discover, collect data from machines, assess machines, display bulletin and template details, check for updates, and view history. Users can add, edit, and delete reports, compliance rules and rule groups, and compliance and patch assessment templates. They can also install the Agent, upgrade VCM, and uninstall VCM.

When you apply the VCM Change Restricted role to a user’s VCM login, they cannot perform the following actions.
Remote command execution
Change actions against target managed machines
Change rollback
Compliance enforcement
Patch deployment
Software deployment
OS provisioning
Machine reboots

All VCM user accounts must have the following rights on the VCM Collector machine.

- Ability to log on locally to access IIS
- Read access to the System32 folder
- Write access to the CMFiles$\Exported_Reports folder to export reports
- If default permissions have been changed, read access to the C:\Program Files (x86) \VMware\VCM\WebConsole directory and all subdirectories and files

Users who add machines to VCM using a file or the Available Machines Add Machines action must have write access to CMFiles$\Discovery_Files.

Running VCM as Administrator on the Collector

By default for localhost, Internet Explorer on Windows Server 2008 R2 runs with Protected Mode enabled. If you are logged in to VCM as an Administrator, because Protected Mode is enabled, problems can occur with the SQLServer Reporting Service (SSRS) Web service interface components such as dashboards and node summaries.

**CAUTION** Although you should not access VCM on the Collector using a Web console, to restore the SSRS functionality you can run Internet Explorer as administrator or disable Protected Mode for the zone of the Collector (localhost). If you perform this action, you must take additional precautions to protect the Collector because of the increased exposure to attacks on the Collector through the Web browser, such as cross-site scripting.

Log In to VCM

Access VCM from any physical or virtual machine in your network. The level of access is determined by your VCM administrator.

**Prerequisites**

- Verify that the physical or virtual machines from which you are accessing VCM have a supported version of Internet Explorer installed. For supported platforms, see the VCM Installation Guide.
- Configure the Internet Explorer Pop-up Blocker settings to add your Collector to your list of allowed Web sites, or disable Pop-up Blocker. Click Internet Explorer and select Tools > Pop-up Blocker > Pop-up Blocker Settings and then add the path for your Collector in the allowable address field.
Procedure

1. To connect to VCM from a physical or virtual machine on your network, open Internet Explorer and type http://<name-or-IP-address-of-Collector-machine>/VCM.
2. Type your user network credentials.
3. (Optional) Select **Automatically log on using this role** to have VCM log you in.
4. Click **Log On**.

Your VCM user account can have multiple roles. If you selected the **Automatically log on using this role** option, VCM will automatically log you on as the User Role displayed on the Logon screen. To change roles, you must use the Logoff button in the top right corner of the Console. This action will return you to the Logon screen so that you can use the drop-down menu to select a different role.

**Getting Familiar with the Portal**

The VCM Web Console provides access to all VCM features to manage your environment. The Web Console uses a browser-based interface to run from any Windows machine that has access to the server on which VCM is installed. The Windows machine must be running Internet Explorer or Mozilla Firefox with the Internet Explorer tab plug-in installed.

The Web Console includes several major areas and controls.

**General Information Bar**

The general information bar displays the VCM Collector’s active SQL Server name, your VCM user name and active Role, and the following buttons.
- **Log Out**: Exits the Web Console. The Web Console closes and the VCM Logon screen appears.
- **About**: Displays information about how to contact VMware Technical Support and version information for VCM and all of its components. This information may be important when you contact VMware Technical Support.
- **Help**: Opens the online Help for the currently-active display.

**Toolbar**

The global toolbar provides you with easily-accessible options to enhance control of your environment and data.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Left Arrow" /> <img src="image" alt="Right Arrow" /></td>
<td>The left and right arrow buttons navigate to the previous or next page in the data area.</td>
</tr>
<tr>
<td><img src="image" alt="Jobs" /></td>
<td>The Jobs button opens the Jobs Running status window. This button provides access to the Collector status and allows you to stop and restart the Collector service.</td>
</tr>
<tr>
<td><img src="image" alt="Collect" /></td>
<td>The Collect button opens a wizard that allows you to define and initiate data collections.</td>
</tr>
<tr>
<td><img src="image" alt="Remote Command" /></td>
<td>The Remote Commands button allows you to invoke the Remote Commands wizard from the toolbar without having to access the node.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>The Refresh data grid view button refreshes the data grid. Press F5 on the keyboard as an alternative action.</td>
</tr>
<tr>
<td><img src="image" alt="View Row Cells" /></td>
<td>The View row cells button displays a vertically scrolling view of a single row of data, rather than the table-based data grid view in a separate window, and allows you to move between records.</td>
</tr>
<tr>
<td><img src="image" alt="Select All" /></td>
<td>The Select all displayed data rows button selects all the rows in the data grid.</td>
</tr>
<tr>
<td><img src="image" alt="Copy" /></td>
<td>The Copy button copies information from the selected rows in the data grid to the clipboard.</td>
</tr>
<tr>
<td><img src="image" alt="Copy Link to Clipboard" /></td>
<td>The Copy link to clipboard button copies the link of the content on-screen to the clipboard.</td>
</tr>
<tr>
<td><img src="image" alt="View Data Grid" /></td>
<td>The View data grid in separate window button displays the data grid in a separate window.</td>
</tr>
<tr>
<td><img src="image" alt="Export" /></td>
<td>The Export displayed data button exports data to a CSV formatted file. This file is exported to <code>\&lt;name_of_Collector_machine&gt;\CMfiles\Exported Reports</code>.</td>
</tr>
<tr>
<td><img src="image" alt="Options" /></td>
<td>The Options button opens the User Options window. These settings pertain to the User who is logged in to VCM. All VCM users can configure these settings to their individual preferences.</td>
</tr>
</tbody>
</table>
Sliders

The sliders on the left side of the Web Console include the items listed and described in the following table. The individual items that you see in VCM will vary depending on the components that you have licensed.

- Active Directory and AD objects based on your role.
- Patching options are available based on your role.
- Administration is visible only to users who have Administrative rights to VCM as part of their VCM role.

For detailed instructions about any of these features, see the online Help.

<table>
<thead>
<tr>
<th>Slider</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>View, export, or print enterprise-wide, summary information.</td>
</tr>
<tr>
<td></td>
<td>Review or acknowledge current alert notifications.</td>
</tr>
<tr>
<td></td>
<td>Manage VCM discovered and non-VCM discovered hardware and software assets.</td>
</tr>
<tr>
<td></td>
<td>Review changes that occurred from one collection to the next.</td>
</tr>
<tr>
<td></td>
<td>Create, edit, or run remote commands on a VCM managed Windows or UNIX machine.</td>
</tr>
<tr>
<td></td>
<td>View information about VCM discovered domains.</td>
</tr>
<tr>
<td></td>
<td>Navigate and manage integrated service desk events.</td>
</tr>
<tr>
<td></td>
<td>Manage virtual machines.</td>
</tr>
<tr>
<td></td>
<td>View your Windows NT Domain and Active Directory related data.</td>
</tr>
<tr>
<td></td>
<td>View information for enterprise-level applications.</td>
</tr>
<tr>
<td></td>
<td>Review non-security related UNIX machine-specific information.</td>
</tr>
<tr>
<td></td>
<td>Review UNIX security data to ensure consistent security configurations across your environment.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Create and manage Compliance rule groups and templates based on AD objects or machine group data.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>View, export, or print enterprise-wide, summary information for Active Directory objects.</td>
</tr>
<tr>
<td></td>
<td>Review alert notifications for the selected AD location.</td>
</tr>
<tr>
<td></td>
<td>Review Active Directory-related changes that occurred from one collection to the next.</td>
</tr>
<tr>
<td></td>
<td>View collected information about Active Directory objects such as Users, Groups, Contacts, Computers, Printers, Shares, and Organizational Units.</td>
</tr>
<tr>
<td></td>
<td>Review Active Directory site lists, including Site Links, Site Link Bridges, Subnets, Intersite Transports, Servers, Connections and Licensing.</td>
</tr>
<tr>
<td></td>
<td>View Active Directory Group Policy Container Settings.</td>
</tr>
<tr>
<td>Slider</td>
<td>Action</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• View information about Active Directory Domains, DCs, and Trusts.</td>
</tr>
<tr>
<td></td>
<td>• Track and display access control entries and security descriptor data on all collected objects.</td>
</tr>
<tr>
<td></td>
<td>• View Active Directory Schema information.</td>
</tr>
</tbody>
</table>

| Reports         | Run out-of-the-box reports against your collected data.                |
|                 | Write your own SQL and SSRS reports using VCM’s report wizard.        |

| Patching        | Review a list of bulletins available to VCM.                          |
|                 | Create, run, or import VCM Patching templates to display the machines that require the patches described in each bulletin. |
|                 | Monitor VCM Patching jobs.                                            |
|                 | Deploy patches.                                                       |

| Administration   | Manage basic configuration options for VCM.                           |
|                  | • Establish filters to limit the data you collect from machines in your environment. |
|                  | • Review how your VCM licenses are being used.                        |
|                  | • Identify and manage your physical and virtual machines.             |
|                  | • Manage VCM Logins and Roles.                                       |
|                  | • Set options for assessment and deployment.                          |
|                  | • View the status of jobs that are currently running, scheduled to run, or completed. |
|                  | • Configure VCM to notify you of certain conditions in your environment. |

**Customizing VCM for your Environment**

Create a machine group structure that matches the organization of the machines in your environment. With these machine groups, you can manage specific machines in your environment such as all SQL Servers in a particular location. You can apply specific changes or create roles and rules for those machines independently from other machines in your environment. This approach ensures that you can restrict access to critical machines to the appropriate users with rights to VCM.

You can customize the following options for your environment:

- **Alerts**: Define the objects and types of changes that you are alerted to when they are detected in VCM. For example, you can set an alert to notify you if a registry setting changes in your environment.

- **Collection Filters and Filter Sets**: Use collection filters to specify the data to collect from the VCM managed machines. A default collection filter is provided for each data type. You can add custom collection filters that are specific to your enterprise. You can apply filters during instant collections and scheduled collections if the filters are included in a filter set. After you create collection filters, organize them into filter sets. You can create specific filter sets or filter set groups for different machine groups. You can apply filter sets during instant collections or scheduled collections.
- **Compliance Templates and Rule Groups**: Use compliance templates and rule groups to define specific settings and verify whether the machines match those criteria. VCM provides prepackaged templates and rules to check the compliance of your machines with regulatory, industry, and vendor standards. VMware provides additional compliance packages that you can import into VCM.

- **Reports**: Create and print tailored reports of information that does not appear in VCM. VCM provides prepackaged reports that you can run after you collect data from your VCM managed machines.

- **Roles and Rules**: VCM roles and access rules work together to control user access to VCM. For example, you can create a role that allows a user to view all data, but not make changes to the environment. You can create a role to run certain reports or a role that allows unlimited access to a single machine group.

  The VCM Change Restricted role limits users from making certain changes in your environment. See "Understanding User Access" on page 11.

For information to import additional compliance packages into VCM, see Import/Export and Content Wizard.
VCM Installation Manager installs several VCM components and tools on the Collector machine during the installation.

This chapter includes the following topics:

- Install the VCM Tools Only 19
- VCM Import/Export and Content Wizard Tools 20
- Run the Deployment Utility 21
- Package Studio 22
- Foundation Checker 22

Install the VCM Tools Only

You can install the VCM tools on a non-Collector Windows machine.

If you plan to install VCM on the non-Collector Windows machine later, you must uninstall the tools and then install VCM.

Prerequisites

Perform the installation requirements for each tool in the Advanced Installation selection. For example, you can install Import/Export (I/E) and Content Wizard only on a machine that is running VCM.
Procedure

1. On the non-Collector Windows machine on which you want to install the tools, insert the installation CD.

2. In Installation Manager, click **Run Installation Manager**.

   During the installation, follow the installation requirements that Installation Manager reports when Foundation Checker runs.

3. Complete the initial installation pages, and click **Next** on subsequent pages to access the Select Installation Type page.
   
   a. Clear the **VMware vCenter Configuration Manager** check box.
   
   b. Select **Tools**.
   
   c. To install a subset of tools, clear the **Tools** check box and select only the individual tools to install.

4. Click **Next**.

5. Complete the remaining instructions and click **Next**.

6. On the Installation Complete page, click **Finish**.

7. On the Installation Manager page, click **Exit**.

### VCM Import/Export and Content Wizard Tools

Use the Import/Export Tool and the Content Wizard Tool to move or update VCM business objects. These tools support the migration of any VCM Management Extension for Asset data that was added to VCM manually, but does not import or export any collected data.

The Import/Export Tool supports the following scenarios.

- Back up (export) and restore (import) business objects to the same machine.
- Back up (export) and import (if needed) business objects during a VCM upgrade.
- Export and migrate (import) business objects to additional machines in a multi-Collector environment during setup or to move custom content.
- Use the Content Wizard to download current Compliance Content from VMware and import it into an existing database.
- Using the Command Line Interface, automate the propagation of content to other machines in a multi-collector environment with a “golden machine”.
- Aid in disaster recovery by using the Command Line Interface to automate and schedule the backup of VCM content and configuration parameters.

The Command Line Interface (CLI) is a powerful extension of the Import/Export graphic user interface (GUI). In addition to supporting the scenarios noted above, the CLI allows content to be overwritten, as opposed to “rename only”, and provides for automation through scripting suitable for customizations.

**IMPORTANT** Use of the CLI should be restricted to advanced users who exercise caution when testing their scripts.

The Import/Export Tool and Content Wizard Tool were installed on your Collector machine during your VCM installation.
Run the Import/Export Tool

Use the Import/Export Tool to back up your VCM database business objects and import them into a new VCM database or into a recovered VCM database. This tool also supports the migration of any VCM Management Extension for Asset data that was manually added to VCM.

Prerequisites
Install the Import/Export Tool. See "Installing and Getting Started with VCM Tools" on page 19.

Procedure
1. On the Collector, click Start.
2. Select All Programs > VMware vCenter Configuration Manager > Tools > Import Export Tool.
3. For importing and exporting procedures, click Help > Contents and use the online help.

Run the Content Wizard to Access Additional Compliance Content

Use the Content Wizard to import additional VMware content such as VCM Compliance Content Packages. These packages are not available in VCM until you download and import them. Check the VCM Compliance Content Packages to determine if you need to import them.

Prerequisites
Install the Content Wizard. See "Installing and Getting Started with VCM Tools" on page 19.

Procedure
1. On the Collector, click Start.
2. Select All Programs > VMware vCenter Configuration Manager > Tools > Content Wizard Tool.
3. In the Content Wizard, select Get Updates from the Internet and click Next.
4. After the wizard identifies available content, click Next.
5. Select the updates to install on your Collector and click Install.
   When the installation is finished, the Event Log Results window appears.
6. On the Event Log Results window, click Save and specify a location to save the logs.
7. Click Close.
8. On the Content Wizard page, click Exit.

What to do next
View the imported data in VCM. For example, click Compliance and select Machine Group Compliance > Templates. You can now run any imported compliance template against your collected data.

Run the Deployment Utility

The Deployment Utility for UNIX/Linux and ESX/vSphere copies files to multiple target machines when you configure UNIX/Linux and ESX/vSphere machines for management in VCM.
Procedure

1. On the Collector, navigate to C:\Program Files (x86)\VMware\VCM\Tools.
2. Copy the DeployUtility-<version>.zip file from the Collector to your Windows machine.
3. Extract the files.
4. Double-click DeployUtil.exe to start the application.

What to do next

In the Deployment Utility, click Help and review the procedure for the type of machine you are configuring.

Package Studio

Use Package Studio to create software packages that can be installed by VCM. It is one component of VCM Software Provisioning that includes the Software Repository for Windows and the Package Manager.

For procedures to run the Package Studio, see the Software Provisioning Components Installation and User’s Guide.

Foundation Checker

Use the Foundation Checker tool to verify that a Windows machine designated as a VCM Collector meets all of the prerequisites necessary to install VCM.

Installation Manager uses VCM Foundation Checker to check a machine’s viability for a successful VCM deployment. Foundation Checker runs system checks that determine various conditions, settings, and requirements, and displays a results file that displays the system checks that passed, failed, or generated warnings.

If the checks run without error, you can install VCM. If the checks identify missing components or incorrect configurations, Foundation Checker instructs you where to verify the component or configuration and how to remedy the errors.

To run the Foundation Checker on a Windows machine on which you will install another instance of VCM, see the Foundation Checker User’s Guide.
VCM collects information from your instances of vCenter Server, vCloud Director, and vShield Manager so that you can then use the information to manage and maintain your virtual environment.

The collected data appears in the Console under the Virtual Environments node. The information is organized in logical groupings based on the information sources, including vCenter Server, vCloud Director, and vShield Manager.

Based on the collected virtual environments data, you can manage the objects and data at an enterprise and individual level, including running compliance rules and reports; running actions, such as changing settings and taking virtual machine snapshots; and managing the guest operating systems as fully managed VCM machines.

This chapter includes the following topics:

- Virtual Environments Configuration
- Configure Virtual Environments Collections
- Configure Managing Agent Machines
- Obtain the SSL Certificate Thumbprint
- Configure vCenter Server Data Collections
- Configure vCenter Server Virtual Machine Collections
- Configure vCloud Director Collections
- Configure vCloud Director vApp Virtual Machines Collections
- Configure vShield Manager Collections
- Configure ESX Service Console OS Collections
- Configure the vSphere Client VCM Plug-In

Virtual Environments Configuration

To manage your virtual environments, you collect vCenter Server, vCloud Director, and vShield Manager data. To collect the data, you use one or more Managing Agent machines.

After configuring your Managing Agent machines, you add and configure your vCenter Server, vCloud Director, and vShield Manager instances in VCM to use the Managing Agent for communication. For a diagram illustrating how the components are configured together, see Figure 3-1. Virtual Environments Configuration Diagram.
Managing Agents

The Managing Agent machines must have the 5.5 Agent or later installed. They must also be configured to manage the secure communication between the vCenter Server, vCloud Director, and vShield Manager instances and the Collector. Depending on the size of your Cloud Infrastructure environment, you can use your Collector as a Managing Agent or you can use another Windows machine. If your individual vCenter Server instances manage no more than 1–30 hosts and a maximum of 1000 guests, then you can use the Collector as your Managing Agent. If any of your vCenter Server instances exceed this amount, you must use a Windows machine that is not your Collector as a Managing Agent.
Managing vCenter Server Instances, Hosts, and Guest Virtual Machines

You collect data from vCenter Server instances regarding resources managed by the vCenter Server, and to identify and manage the host and guest machines. The host and guest machines are managed based on configured vCenter Server instances. From VCM, you can run vCenter Server actions such as configuring settings, turning the power on and off, or taking a snapshot. To fully manage the guest machines, install the VCM Agent on the virtual machines and manage their operating system.

Managing Instances of vCloud Director and vApp Virtual Machines

You collect data from vCloud Director instances regarding their configurations, resources managed by vCloud Director, and to identify and manage the vApp virtual machine guest operating systems. To fully manage the guest machines, you install the VCM Agent on the virtual machines and manage their operating system.

Managing vShield Manager Instances

You collect from vShield Manager instances to gather data regarding vShield App security groups. You can run reports on the collected data.

Configure Virtual Environments Collections

To manage your virtual environments, configure your Managing Agent and then implement the procedures that suit your environment.

Procedure

1. "Configure Managing Agent Machines" on page 26
   The Managing Agents are one or more physical or virtual machine running a supported Windows operating system that manages the communication between the Collector and your instances of vCenter Server, vCloud Director, and vShield Manager.

2. "Obtain the SSL Certificate Thumbprint" on page 29
   When configuring the settings for your virtual environments systems, you can use an SSL certificate thumbprint file to ensure secure communication between the Collector and your instances of vCenter Server, vCloud Director, and vShield Manager.

3. "Configure vCenter Server Data Collections" on page 30
   Collect data from your vCenter Server so that you can identify and manage your virtual environments, including ESX and ESXi hosts, and guest virtual machines.

4. "Configure vCenter Server Virtual Machine Collections" on page 35
   Configure virtual machine collections so that you can identify and manage the guest operating systems on the vCenter Server virtual machines.

5. "Configure vCloud Director Collections" on page 37
   Configure collections from your vCloud Director instances so that you can run compliance and reports, and identify your vApp virtual machines.

6. "Configure vCloud Director vApp Virtual Machines Collections" on page 41
Collect vCloud Director data so that you can identify and manage the guest operating systems of the vApp virtual machines.

7. “Configure vShield Manager Collections” on page 46
   Configure collections from your vShield Manager instances so that you can run reports on the collected data.

8. “Configure ESX Service Console OS Collections” on page 50
   The ESX Service Console OS Linux data type data and the ESX logs are collected directly from the ESX operating systems, not from vCenter Server. Configure the ESX servers so that you can collect the Linux data type and ESX log data from the ESX service console operating system.

9. “Configure the vSphere Client VCM Plug-In” on page 56
   The vSphere Client VCM Plug-In provides contextual access to VCM change, compliance, and management functions. It also provides direct access to collected vCenter Server, virtual machine host, and virtual machine guest data.

Configure Managing Agent Machines

The Managing Agents are one or more physical or virtual machine running a supported Windows operating system that manages the communication between the Collector and your instances of vCenter Server, vCloud Director, and vShield Manager.

The Managing Agent machines must have the 5.5 Agent or later installed. They must also be configured to manage the secure communication between the vCenter Server, vCloud Director, and vShield Manager instances and the Collector. Depending on the size of your Cloud Infrastructure environment, you can use your Collector as a Managing Agent or you can use another Windows machine. If your individual vCenter Server instances manage no more than 1–30 hosts and a maximum of 1000 guests, then you can use the Collector as your Managing Agent. If any of your vCenter Server instances exceed this amount, you must use a Windows machine that is not your Collector as a Managing Agent.

**CAUTION**  Do not use the Windows machines on which your vCenter Server instances are running as Managing Agent machines.

Procedure

1. “Collect Machines Data From the Managing Agent Machines” on page 27
   Collect data from your Managing Agent machines to ensure that VCM identifies the Windows machines as licensed and that the 5.5 Agent or later is installed.

2. “Set the Trust Status for Managing Agent Machines” on page 27
   You set the trusted status is on machines where you verify that the connection is legitimate. When you set the trust status, you are marking the Agent certificate as trusted.

3. “Configure HTTPS Bypass Setting” on page 28
   If your Collector is not configured to use HTTPS, you must configure the Collector to allow HTTP communication when entering sensitive parameter values.

4. “Enable Managing Agent Machines” on page 28
   Managing Agent machines must be enabled to perform the necessary communication with your instances of vCenter Server, vCloud Director, and vShield Manager.
Collect Machines Data From the Managing Agent Machines

Collect data from your Managing Agent machines to ensure that VCM identifies the Windows machines as licensed and that the 5.5 Agent or later is installed.

The Managing Agent is the Agent used to collect data from your instances of vCenter Server, vCloud Director and vShield Manager.

Prerequisites

Verify that the Windows machine that you designated as the Managing Agent is licensed and that it has the VCM Agent 5.5 or later installed. See "Configure Windows Machines" on page 87.

Procedure

1. Click Administration.
2. Select Machines Manager > Licensed Machines > Licensed Windows Machines.
3. Select the Managing Agent machines and click Collect on the VCM toolbar.
4. On the Collection Type page, select Machine Data and click OK.
5. On the Machines page, verify that the Selected list includes the Managing Agent machine and click Next.
7. Select Machines, and click Next.
8. On the Important page, resolve any conflicts and click Finish.
9. When the job finishes, verify that the Agent Version value in the data grid is 5.5 or later.

What to do next

Configure the trust status for the Managing Agents. See "Set the Trust Status for Managing Agent Machines" on page 27.

Set the Trust Status for Managing Agent Machines

You set the trusted status is on machines where you verify that the connection is legitimate. When you set the trust status, you are marking the Agent certificate as trusted.

When you transmit sensitive information, such as credentials, between the Collector and physical or virtual machines on which the Managing Agent is installed, the Agent certificate, including the Agent certificate on the Collector, must be trusted.

If you do not use this level of security, you can set the Allow sensitive parameters to be passed to agents not verified as Trusted option to Yes. To override the setting, click Administration and select Settings > General Settings > Collector.

Prerequisites

Ensure that you collected the Machines data type from the Windows machines you are using as Managing Agents. See "Collect Machines Data From the Managing Agent Machines" on page 27.
Procedure
1. Click Administration.
2. Select Certificates.
3. Select the Managing Agent machines and click Change Trust Status.
4. Add any additional machines to trust to the lower data grid.
5. Select Check to trust or uncheck to untrust the selected machines and click Next.
6. Review the number of machines affected and click Finish.

What to do next
- If your Collector is not configured to use HTTPS, set the HTTPS bypass. See "Configure HTTPS Bypass Setting" on page 28.
- Identify the Windows machines as Managing Agents. See "Enable Managing Agent Machines" on page 28.

Configure HTTPS Bypass Setting
If your Collector is not configured to use HTTPS, you must configure the Collector to allow HTTP communication when entering sensitive parameter values.

If your Collector is configured to use HTTPS, you do not need to modify this setting.

Procedure
1. Click Administration.
2. Select Settings > General Settings > Collector.
3. Select Allow HTTP communication (HTTPS bypass) when entering sensitive parameter values and click Edit Settings.
4. Select Yes and click Next.
5. Review the summary and click Finish.

What to do next
Identify the Windows machines as Managing Agents. See "Enable Managing Agent Machines" on page 28.

Enable Managing Agent Machines
Managing Agent machines must be enabled to perform the necessary communication with your instances of vCenter Server, vCloud Director, and vShield Manager.

Prerequisites
- Ensure that the Managing Agent machines are trusted machines. See "Set the Trust Status for Managing Agent Machines" on page 27.
- If your Collector is not configured to use HTTPS, set the HTTPS bypass. See "Configure HTTPS Bypass Setting" on page 28.
Procedure
1. Click Administration.
2. Select Administration > Machines Manager > Licensed Machines > Licensed Windows Machines.
3. Select the Managing Agent machines and click Change Managing Agent Status.
4. Add any additional machines to the lower data grid.
5. Select Enable - allow the selected machines to be used as managing agents and click Next.
6. Review the number of machines affected and click Finish.

What to do next
- To maintain secure communication, you need the SSL certificates from your instances of vCenter Server, vCloud Director, and vShield Manager. See "Obtain the SSL Certificate Thumbprint" on page 29.
- Configure the collections from your instances of vCenter Server, vCloud Director, and vShield Manager.
  - See "Configure vCenter Server Data Collections" on page 30.
  - See "Configure vCloud Director Collections" on page 37.
  - See "Configure vShield Manager Collections" on page 46.

Obtain the SSL Certificate Thumbprint

When configuring the settings for your virtual environments systems, you can use an SSL certificate thumbprint file to ensure secure communication between the Collector and your instances of vCenter Server, vCloud Director, and vShield Manager.

You can use this procedure to copy and save the thumbprint in advance of configuring the settings, or you can follow the process while you are using the wizard.

This procedure applies when your certificates are not properly trusted. If your certificates are configured and trusted, you must log onto the target machine to retrieve the thumbprint from the certificate store.

Prerequisites

Ensure that you have network access to the target instances of vCenter Server, vCloud Director, and vShield Manager from which you need the thumbprint string.

Procedure
1. Open Internet Explorer.
2. In the address bar, type https://<your vcenter server, vcloud director, or vshield manager instance>.
3. On the certificate error page, click Continue to this website.
4. On the address bar, click Certificate Error and select View Certificates.
5. Click the Details tab.
6. In the list, select Thumbprint.
7. Copy the thumbprint string to your clipboard or to a file so that you can access it when needed.
Configure vCenter Server Data Collections

Collect data from your vCenter Server so that you can identify and manage your virtual environments, including ESX and ESXi hosts, and guest virtual machines.

Prerequisites

- To maintain secure communication, you need the SSL certificates from your instances of vCenter Server. See "Obtain the SSL Certificate Thumbprint" on page 29.

Procedure

1. "Add vCenter Server Instances" on page 30
   Add the vCenter Server instances to VCM so that you can license and collect vCenter Server data using the Managing Agent.
2. "Configure the vCenter Server Settings" on page 31
   Configure the Managing Agent, communication, and vCenter Server access options so that VCM can collect host and guest data from the vCenter Server instances.
3. "Collect vCenter Server Data" on page 32
   Collect the vCenter Server, host, and guest data from the vCenter Server instances. The data is displayed by detailed data type and appears in the VCM Console.

The collected vCenter Server data appears in the Console in the Virtual Environments node. The collected vCenter Server data helps you identify and manage vCenter Server, host, and guest objects. See "vCenter Server Collection Results" on page 33.

Add vCenter Server Instances

Add the vCenter Server instances to VCM so that you can license and collect vCenter Server data using the Managing Agent.

In addition to adding the vCenter Server instances, and you can also add the Windows machine on which the vCenter Server is installed and manage the underlying Windows operating system.

Prerequisites

Know the names and domain information for the vCenter Server instances in your environment.

Procedure

1. Click Administration.
2. Select Machines Manager > Available Machines.
3. Click Add Machines.
4. On the Add Machines page, select Basic: Name, Domain, Type, Automatically license machines, and click Next.
5. On the Manually Add Machines - Basic page, configure these options to identify the vCenter Server instances.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine</td>
<td>Name of the vCenter Server.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the vCenter Server belongs.</td>
</tr>
<tr>
<td>Type</td>
<td>Domain type.</td>
</tr>
<tr>
<td>Machine Type</td>
<td>Select vCenter (Windows).</td>
</tr>
</tbody>
</table>

6. Click **Add**.

   The machine information is added to the list.

7. (Optional) Add other vCenter Server instances as needed.

8. When all your vCenterServer are added to the list, click **Next**.

9. On the Information page, review the summary and click **Finish**.

**What to do next**

- Configure the vCenter Server settings. See "Configure the vCenter Server Settings" on page 31.

- Manage the Windows operating systems on which vCenter Server instances are running. See "Configure Windows Machines" on page 87.

**Configure the vCenter Server Settings**

Configure the Managing Agent, communication, and vCenter Server access options so that VCM can collect host and guest data from the vCenter Server instances.

**Prerequisites**

- Collect Machines data from the Windows machine that you designated as your Managing Agent. See "Collect Machines Data From the Managing Agent Machines" on page 27.

- If you are using SSL Certificates to maintain secure communication, you must provide the certificate thumbprint from the target system when configuring the settings. See "Obtain the SSL Certificate Thumbprint" on page 29.

**Procedure**

1. Click **Administration**.

2. Select **Machines Manager** > **Licensed Machines** > **Licensed Virtual Environments**.

3. Select the vCenter Server instances and click **Configure Settings**.

4. On the Virtual Environment page, verify that the vCenter Server instances appear in the lower pane and click **Next**.

5. On the Managing Agent and Communication Settings page, configure the settings that are applied to all selected vCenter Server instances and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Agent</td>
<td>Select the Windows machine to manage communication between the Collector and the vCenter Server instances. This Windows machine must have the 5.5 Agent</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>or later installed.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port used by the VMware Infrastructure SDK on the vCenter Server instances.</td>
</tr>
<tr>
<td></td>
<td>The default value is 443.</td>
</tr>
<tr>
<td>User ID</td>
<td>Type a vCenter Server instance user name.</td>
</tr>
<tr>
<td></td>
<td>The user must have a vCenter Server administrative role or an unrestricted read only role.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password for the vCenter Server instance user ID.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Type the password again.</td>
</tr>
<tr>
<td>Ignore untrusted SSL Certificate</td>
<td>Select one of the following certificate options.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. If you selected No on the Managing Agent and Communication Settings page, you must type or paste the thumbprint string in the text box and click **Next**.

7. On the Important page, click **Finish**.

**What to do next**

Collect vCenter Server data. See "Collect vCenter Server Data" on page 32.

**Collect vCenter Server Data**

Collect the vCenter Server, host, and guest data from the vCenter Server instances. The data is displayed by detailed data type and appears in the VCM Console.

**Prerequisites**

Configure the vCenter Server settings. See "Configure the vCenter Server Settings" on page 31.

**Procedure**

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Virtual Environments**.
3. Select the vCenter Server instances and click **Collect** on the VCM toolbar.
4. On the Collection Type page, select **Machine Data** and click **OK**.
5. On the Machines page, verify that the Selected list includes all the vCenter Server instances from which you are collecting and click **Next**.
6. On the Data Types page, select the Virtualization vCenter Server data types that you want to collect from the vCenter Server instances and click **Next**.
7. On the Important page, resolve any conflicts and click **Finish**.
What to do next

- Review the collected virtualization data. Click Console and select Virtual Environments > vCenter.
- (Optional) Schedule vCenter Server collections. See "Configure vCenter Server Scheduled Collections" on page 33.

**vCenter Server Collection Results**

The collected vCenter Server data appears in the Console in the Virtual Environments node. The collected vCenter Server data helps you identify and manage vCenter Server, host, and guest objects.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>View the Virtual Environments dashboards. Click Click Console and select Dashboards &gt; Virtual Environments.</td>
</tr>
<tr>
<td></td>
<td>View the collected vCenter Server data. Click Console and select Virtual Environments &gt; vCenter to access the collected data.</td>
</tr>
<tr>
<td></td>
<td>View the change logs for the virtual environments. Click Console and select Change Management to access the collected data.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Access compliance rules that you create based on the collected vCenter Server data using the Virtual Environment Compliance node. You cannot create enforceable compliance rules for vCenter Server data.</td>
</tr>
<tr>
<td></td>
<td>The compliance rules for the virtual machines you license and on which you install the Agent are managed in the Machine Group Compliance node.</td>
</tr>
<tr>
<td>Reports</td>
<td>Run configured Virtual Environments reports, including a vCenter Summary report. Click Reports and select Machine Group Reports &gt; Virtual Environments.</td>
</tr>
<tr>
<td></td>
<td>Create reports based collected vCloud Director objects. Click Reports and select Virtual Object Reports.</td>
</tr>
<tr>
<td>Administration</td>
<td>Displays managed vCenter Server instances from which you are collecting data. Click Administration and select Machines Manager &gt; Licensed Machines &gt; Licensed Virtual Environments to view licensed vCenter Server instances.</td>
</tr>
<tr>
<td>Administration &gt;</td>
<td>Dynamic machine groups based on vCenter Server objects. These objects include instances, hosts, and guest machines, and are used to limit the displayed data.</td>
</tr>
</tbody>
</table>

**Configure vCenter Server Scheduled Collections**

Configure VCM to regularly collect vCenter Server data from your vCenter Server machine groups to ensure that you are using current results when you are viewing the data and when running reports or compliance.

This action is not required, but scheduling your collections improves your configuration management efficiency.
Procedure

1. "Create a vCenter Server Machine Group" on page 34
   Create a Windows machine group that contains your vCenter Server instances so that you can run collections on the member machines.

2. "Schedule vCenter Server Collections" on page 34
   Schedule the collection job to run against your vCenter Server machine group with the the Default filter set applied so that you regularly collect the vCenter Server and Windows data from the vCenter Server instances.

Create a vCenter Server Machine Group

Create a Windows machine group that contains your vCenter Server instances so that you can run collections on the member machines.

Procedure

1. Click Administration.

2. Select Machines Manager > Machine/Virtual Object Groups > All Windows Machines.

3. Click Add Group.

4. Type the name and description of the machine group and click Next.
   For example, type the name vCenter Server Instances.

5. Select Static and click Next.

6. Add the Windows machines that are running vCenter Server to the Selected list and click Next.

7. Click Finish.
   The group is added to the All Windows Machine list.

What to do next

Schedule the collection of the vCenter Server data types from the vCenter Server instances. See "Schedule vCenter Server Collections" on page 34.

Schedule vCenter Server Collections

Schedule the collection job to run against your vCenter Server machine group with the the Default filter set applied so that you regularly collect the vCenter Server and Windows data from the vCenter Server instances.

Prerequisites

Create a Windows machine groups that includes the machines that are running vCenter Server. See "Create a vCenter Server Machine Group" on page 34.
Procedure

1. Click Administration.
2. Select Job Manager > Scheduled.
3. Click Add.
4. Select Collection and click Next.
5. Type a job name and description and click Next. For example, vCenter Server Collections.
6. Select Default filter set and click Next.
7. Select your vCenter Server machine group and click Next. For example, vCenter Server Instances.
8. Configure when the collection job runs and click Next. For example, every four hours starting today.
9. Resolve any conflicts and click Finish. The collection job is added to your Scheduled Jobs list.

What to do next

After a scheduled run time, verify that the job ran. The information is available in Job Manager history for scheduled collections. Select the time and review the general status and success. View the machine detail status if the collection was not 100% successful.

Configure vCenter Server Virtual Machine Collections

Configure virtual machine collections so that you can identify and manage the guest operating systems on the vCenter Server virtual machines.

VCM manages virtual machines as guest machines and as Windows, Linux, or UNIX machines. To manage the virtual machines as guest machines, you collect vCenter Guests data from your vCenter Server. To manage the virtual machines based on operating system, you license, install the VCM Agent, and collect data directly from the managed machines.

You can identify the virtual machines in your environment two ways.

- Collect vCenter Guests data from you vCenter Servers and manage the virtual Windows, Linux, or UNIX machines. See "Collect vCenter Server Virtual Machines Data" on page 35.
- Manually discover Windows Machines or add Linux or UNIX machines. For Windows machines, see "Discover Windows Machines" on page 89. For Linux or UNIX machines, see "Add UNIX/Linux Machines" on page 122.

Collect vCenter Server Virtual Machines Data

Identify and license your virtual machines that are identified based on collected vCenter Guests data.

Prerequisites

Manage your vCenter Servers in VCM. See "Configure vCenter Server Data Collections" on page 30.
Procedure

1. Click Administration.
2. Select Machines Manager > Available Machines > Licensed Virtual Environments.
3. Select the vCenter Servers and click Collect on the VCM toolbar.
4. On the Collection Type page, select Machine Data and click OK.
5. On the Machines page, verify that the Selected list includes all the vCenter Servers from which you are collecting and click Next.
6. On the Data Types page select Virtualization > vCenter Guests and click Next.
7. On the Important page, resolve any conflicts and click Finish.

What to do next

License your virtual machines. See "Manage vCenter Server Virtual Machines" on page 36.

Manage vCenter Server Virtual Machines

Add and license the virtual machines identified based on a vCenter Guests collection from your vCenter Servers. If you are managing Windows virtual machines, you can also install the VCM Agent.

Using the Manage Guests wizard, you can add the virtual machines to the appropriate Available Machines data grid based on operating system, license the virtual machine based on operating system, or, for Windows machines, license and install the Agent.

Prerequisites

Collect vCenter Guests data from your vCenter Servers. See "Collect vCenter Server Virtual Machines Data" on page 35.

Procedure

1. Click Console.
2. Select Virtual Environments > vCenter > Guests > Summary.
3. Select either your Windows virtual machines or your UNIX/Linux virtual machines and click Manage Guests.
4. On the Default Domain page, configure the options and click Next.
   a. Specify the Domain in which the machines are running.
   b. Select the Domain Type.
5. On the Edit VM Guest Machine Info page, review the list and update or remove virtual machines, and click Next.
6. On the License VM Guests page, configure the options and click Next.
   a. Select License the selected machines.
   b. (Windows machines only) Select Install VCM agents for the selected Windows machines, and click Next.
7. On the Confirm Your Changes page, review the changes and click Finish.
What to do next

- For Windows operating system guest machines on which you installed the Agent, collect from the Windows virtual machines. See "Collect Windows Data" on page 97. If you did not install the Agent, see "Install the VCM Windows Agent on Your Windows Machines" on page 91.

- For UNIX/Linux operating system guest machines you must install the Agent. See "Install the Agent on UNIX/Linux Machines" on page 124.

Configure vCloud Director Collections

Configure collections from your vCloud Director instances so that you can run compliance and reports, and identify your vApp virtual machines.

Prerequisites


- To maintain secure communication, you need the SSL certificates from your instances of vCloud Director. See "Obtain the SSL Certificate Thumbprint" on page 29.

Procedure

1. "Add vCloud Director Instances" on page 37

   Add the instances of vCloud Director to VCM so that you can license and collect vCloud Director data using the Managing Agent.

2. "Configure the vCloud Director Settings" on page 38

   Configure the Managing Agent, communication, and vCloud Director access options so that VCM can collect virtual machine data from your instances of vCloud Director.

3. "Collect vCloud Director Data" on page 39

   Collect the data from the instances of vCloud Director. The data is displayed by detailed data type and appears in the VCM Console.

The collected vCloud Director data appears in the Console in the Virtual Environments node. The data helps you identify and manage vApp virtual machines. See "vCloud Director Collection Results" on page 40.

Add vCloud Director Instances

Add the instances of vCloud Director to VCM so that you can license and collect vCloud Director data using the Managing Agent.

In addition to adding the instances of vCloud Director, and you can also add the Red Hat machine on which the vCloud Director instance is installed and manage the underlying Red Hat operating system.

Prerequisites

Know the names and domain information for the instances of vCloud Director in your environment.
Procedure

1. Click Administration.
2. Select Machines Manager > Available Machines.
3. Click Add Machines.
4. On the Add Machines page, select Basic: Name, Domain, Type, Automatically license machines, and click Next.
5. On the Manually Add Machines - Basic page, configure these options to identify the instances of vCloud Director.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Name</td>
<td>Name of the vCloud Director instance.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the vCloud Director instance belongs.</td>
</tr>
<tr>
<td>Type</td>
<td>Domain type.</td>
</tr>
<tr>
<td>Machine Type</td>
<td>Select vCloud Director.</td>
</tr>
</tbody>
</table>
6. Click Add.

The machine information is added to the list.
7. (Optional) Add other instances of vCloud Director as needed.
8. When all your instances of vCloud Director are added to the list, click Next.
9. On the Information page, review the summary and click Finish.

What to do next

- Configure the vCloud Director settings. See "Configure the vCloud Director Settings" on page 38.
- Manage the Red Hat operating systems on which your vCloud Director instances are running. See "Configure Linux and UNIX Machines" on page 121.

Configure the vCloud Director Settings

Configure the Managing Agent, communication, and vCloud Director access options so that VCM can collect virtual machine data from your instances of vCloud Director.

Prerequisites

- Collect Machines data from the Windows machine that you designated as your Managing Agent. See "Collect Machines Data From the Managing Agent Machines" on page 27.
- If you are using SSL Certificates to maintain secure communication, you must provide the certificate thumbprint from the target system when configuring the settings. See "Obtain the SSL Certificate Thumbprint" on page 29.
Procedure

1. Click Administration.

2. Select Machines Manager > Licensed Machines > Licensed Virtual Environments.

3. Select the vCloud Director instances and click Configure Settings.

4. On the Virtual Environment page, verify that the vCloud Director instances appear in the lower pane and click Next.

5. On the Managing Agent and Communication Settings page, configure the settings that are applied to all selected vCloud Director instances and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Agent</td>
<td>Select the Windows machine to manage communication between the Collector and the vCloud Director instances. This Windows machine must have the 5.5 Agent or later installed. You can use the Collector as your managing agent.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port used by the API on the vCloud Director instance. The default value is 443.</td>
</tr>
<tr>
<td>User ID</td>
<td>Type a vCloud Director instance user name. The user must have a vCloud Director administrative role or an unrestricted read only role. Use a full vCloud Director administrative user, such as administrator@system.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password for the vCloud Director instance user ID.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Type the password again.</td>
</tr>
<tr>
<td>Ignore untrusted SSL Certificate</td>
<td>Select one of the following certificate options. Yes: Ignores the requirement for a valid signed certificate. No: Requires a valid signed certificate.</td>
</tr>
</tbody>
</table>

6. If you selected No on the Managing Agent and Communication Settings page, you must type or paste the thumbprint string in the text box and click Next.

7. On the Important page, click Finish.

What to do next

Collect vCloud Director data. See "Collect vCloud Director Data" on page 39.

Collect vCloud Director Data

Collect the data from the instances of vCloud Director. The data is displayed by detailed data type and appears in the VCM Console.
Prerequisites

Configure the vCloud Director settings. See "Configure the vCloud Director Settings" on page 38.

Procedure

1. Click Administration.
2. Select Machines Manager > Licensed Machines > Licensed Virtual Environments.
3. Select the vCloud Director instances and click Collect on the VCM toolbar.
4. On the Collection Type page, select Machine Data and click OK.
5. On the Machines page, verify that the Selected list includes all the vCloud Director instances from which you are collecting and click Next.
6. On the Data Types page, select the Virtualization vCloud Director data type that you want to collect from the vCloud Director instances and click Next.
7. On the Important page, resolve any conflicts and click Finish.

What to do next

Review the collected virtualization data. Click Console and select Virtual Environments > vCloud Director.

Discover the vApp virtual machines created by the vCloud Director and make them available in VCM. See "Discover vCloud Director vApp Virtual Machines" on page 43.

vCloud Director Collection Results

The collected vCloud Director data appears in the Console. The discovered virtual machines appear on Administration. After you license the virtual machines and install the Agent, you manage them based on their operating system.

The displayed data is only as current as the last time you collected data from your vCloud Director instances and from your managed machines.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>View collected vCloud Director instance data. Click Console and select Virtual Environments &gt; vCloud Director. View the change logs for the virtual environments. Click Console and select Change Management to access the collected data.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Access compliance rules that you create based on the collected vCloud Director data using the Virtual Environment Compliance node. You cannot create enforceable compliance rules for vCloud Director data. The compliance rules for the virtual machines that you license and on which you install the Agent are managed in the Machine Group Compliance node.</td>
</tr>
<tr>
<td>Reports</td>
<td>Run a configured vCloud Director report. Click Reports and select Machine Group Reports &gt; Virtual Environments &gt; vCloud Director Managed VMs. The report includes the vCloud Director Instance, Organization, Organization virtual datacenter, vApp Name, the VC Machine Name, and the related networking data. Create reports based collected vCloud Director objects. Click Reports and select Virtual Object Reports.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administration</td>
<td>Displays managed vCloud Director instances from which you are collecting data. Click Administration and select Machines Manager &gt; Licensed Machines &gt; Licensed Virtual Environments. Displays the discovered virtual machines with a machine name that is based on your configuration options in the discovery rule. For example, OrgName:vAppName:VirtualMachineName. Click Administration and select Machines Manager.</td>
</tr>
<tr>
<td></td>
<td>- If the machines are not licensed and the Agent is not installed, the machines appear in the Available Machines data grid based on the operating system.</td>
</tr>
<tr>
<td></td>
<td>- If the machines are licensed and the Agent is installed, the machines appear in the Licensed Machines data grid based on the operating system.</td>
</tr>
</tbody>
</table>

**Configure vCloud Director vApp Virtual Machines Collections**

Collect vCloud Director data so that you can identify and manage the guest operating systems of the vApp virtual machines.

To accommodate how vCloud Director manages vApps, which can include duplicate names, IP addresses, and MAC addresses, VCM collects and displays internal and external IP address information, internal machine name information, and vCenter machine name information collected directly from vCloud Director. Based on the collected data, you determine how VCM constructs a unique virtual machine name and specify which IP address to use based on the network address translation (NAT) mapping level.

To identify the vCloud Director virtual machines, you configure discovery rules that analyze data collected from the vCloud Director REST API and use the vApp virtual machine information to add new virtual machines to VCM. After installing the Agent and licensing the virtual machines, you manage the new machines based on their operating systems. The machines appear in VCM based on your configured naming convention.

**Network Address Translation and vCloud Director vApp Discovery Rules**

To configure the connection string when creating a vCloud Director virtual machines discovery rule, you must know how network address translation (NAT) is implemented in your vCloud Director instances.

The vCloud Director administrator configures the NAT mapping. How the virtual machines are configured with NAT and where VCM is in the network determines the connection string that VCM uses to communicate with the virtual machines.

vCloud Director 1.0 and 1.5 support a variety of vApp network configurations. VCM supports these scenarios.
VCM is located in the vApp with the virtual machines that it is managing.

The vApp has a direct connection to the org network.

The vApp has a direct connection to the external network.

The vApp has a one-to-one IP address NAT connection to the organization network with direct connection to the external network.

The vApp has a one-to-one IP address NAT connection to the organization network with a one one-to-one IP address NAT connection to the external network.

The vApp has a direct connection to the organization network with one IP address to one IP address NAT connection to the external network.

VCM does not support one to many IP addresses NAT mapping for vCloud Director vApp virtual machines.

To determine the connection string to use when discovering the vCloud Director virtual machines, you must know where VCM is located in the network and how NAT is implemented.

Table 3–1. Determining the Connection String Based on Network Configuration

<table>
<thead>
<tr>
<th>Location of VCM or the Proxy Server on the Network</th>
<th>External Network</th>
<th>Organization Network</th>
<th>Discovery Rule Connection String</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the managed vApp</td>
<td>NA</td>
<td>NA</td>
<td>Internal IP</td>
</tr>
<tr>
<td>On Org Network</td>
<td>NA</td>
<td>Direct connection.</td>
<td>None (use DNS) or Internal IP</td>
</tr>
<tr>
<td>On Org Network</td>
<td>NA</td>
<td>NAT at vApp level.</td>
<td>vApp External IP</td>
</tr>
<tr>
<td>On External Network</td>
<td>Direct Connection</td>
<td>Not connected or direct connection.</td>
<td>Internal IP</td>
</tr>
<tr>
<td>On External Network</td>
<td>Direct from Organization</td>
<td>NAT at vApp level.</td>
<td>vApp External IP</td>
</tr>
<tr>
<td>On External Network</td>
<td>NAT at Org level</td>
<td>The vApp level IP is collected from vCloud Director, but it is not used for the VCM connection.</td>
<td>Org External IP</td>
</tr>
</tbody>
</table>

After you collect the vCloud Director data, you can view the internal and external IP addresses in network information for the virtual machines.

**Best Practice**

VCM cannot use DCOM to communicate with vCloud Director vApp virtual machines across NAT mapped networks.
In a NAT mapped network environment, your best practice is to install the Agent on the vApp template machines. You must manually install the Agent with the HTTP mode enabled, but you must not collect data from these template machines. Collecting from the template machines generates machine-specific information that will cause the virtual machines created from the template to run incomplete collections.

If you discovered NAT mapped vApp virtual machines that do not have the Agent preinstalled on the templates from which they were created, you must manually install the Agent. The Agent must be installed with the HTTP protocol enabled. See “Manually Install the VCM Windows Agent” on page 93.

Discover vCloud Director vApp Virtual Machines

To begin managing the vCloud Director vApp virtual machines, create and run a VCM discovery rule. The rule runs against the collected vCloud Director data in the VCM database.

**Prerequisites**

- Collect vCloud Director data. You can run the discovery only on the collected data. See "Collect vCloud Director Data" on page 39.
- Determine how NAT is used in your vCloud Director network and where VCM is located in relationship to the network. See "Network Address Translation and vCloud Director vApp Discovery Rules" on page 41.

**Procedure**

1. Click **Administration**.
2. Select **Machines Manager > Discovery Rules**.
3. On the data grid toolbar, click **Add**.
4. On the Discovery Rules page, type a Name and Description, and click **Next**.
5. On the Discovery Method page, select **By DB Discovery** and click **Next**.
6. On the Discovery Query page, in the Discovery Query drop-down menu, select **vCloud Director Managed VMs** and click **Next**.
7. On the Discovery Query Parameters page, configure the options to use when discovering and adding the data to VCM and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Name Format</td>
<td>Select the format used to display the virtual machine name. You can select the vCenter name for the virtual machine or select a combination of names for the virtual machine that includes the vApp that contains the virtual machine, the vCloud Director organization, and the vCloud Director instance. With these formats, you can easily sort, group, and display the data in VCM. The composite name is limited to 128 characters.</td>
</tr>
<tr>
<td><strong>VCName</strong>: Name of the virtual machine in vCenter. vCloud Director creates the virtual machine and generates the name of the virtual machine, which includes the machine's host name and the 10-digit identification number of the virtual machine in vCenter. This name is unique in a single vCloud Director instance.</td>
<td></td>
</tr>
<tr>
<td><strong>vApp:VCName</strong>: Name of the vApp that contains the virtual machine and the name of the virtual machine in vCenter.</td>
<td></td>
</tr>
<tr>
<td><strong>vDC:vApp:VCName</strong>: Name of the virtual datacenter with the vApp name and...</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>the name of the virtual machine in vCenter.</td>
</tr>
<tr>
<td></td>
<td><strong>Org:vDC:vApp:VCName:</strong> Name of the vCloud Director organization with the virtual datacenter name, the name of the vApp that contains the virtual machine, and the name of the virtual machine in vCenter.</td>
</tr>
<tr>
<td></td>
<td><strong>Cloud:Org:vDC:vApp:VCName:</strong> Name of the vCloud Director instance with the name of the vCloud Director organization, the virtual datacenter name, the name of the vApp that contains the virtual machine, and the name of the virtual machine in vCenter.</td>
</tr>
<tr>
<td>Machine Name</td>
<td>Select a character to separate the elements of the vCloud Director hierarchy that you use as the machine name.</td>
</tr>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Delimiter</td>
<td>Type or select the domain in which you are managing the virtual machines.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Select the type of domain to which you are adding the virtual machines.</td>
</tr>
<tr>
<td>Domain Type</td>
<td>Select the protocol by which the Collector will communicate with the Agent.</td>
</tr>
<tr>
<td>Protocol</td>
<td>If the virtual machines in the vApp uses NAT mapping, you must select HTTP. If the virtual machines do not use NAT, you can use HTTP or DCOM.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>If you selected the HTTP protocol, you must specify the port used to communicate with the Collector.</td>
</tr>
<tr>
<td></td>
<td>Uses the HTTP Listener on the target machine. The listener is configured to listen on the designated port. Port 26542 is the default setting. Accepted port values range from 1–65535. Other applications should not use this port.</td>
</tr>
<tr>
<td>Use a proxy server</td>
<td>Select <strong>Yes</strong> if you use a proxy server for communication between the Collector and the Agents on the virtual Windows machines.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>No</strong> if you do not use a proxy server or if you are managing UNIX/Linux machines.</td>
</tr>
<tr>
<td></td>
<td>If the machines you add are Windows machines, you can select a proxy server for communication between the Collector and the Agents on managed machines that are located on the other side of a proxy server. The proxy server routes requests from the Collector to the Agents on managed machines. A proxy server can only be used with Windows HTTP agents.</td>
</tr>
<tr>
<td>Connection String</td>
<td>Select the IP address to use when communicating with the virtual machines.</td>
</tr>
<tr>
<td></td>
<td>This address can differ from the address that resolves by machine name from DNS or other name resolution systems. Use this address when VCM must contact a vApp virtual machine through a Network Address Translation (NAT) address, or when DNS available to the Collector cannot resolve the vApp virtual machines.</td>
</tr>
<tr>
<td></td>
<td>If the virtual machines that appear in the console as part of your vCloud Director collections are not added as part of your database discovery of vCloud Director data, ensure that the internal or external connection string is valid for the virtual machines. If the connection string is set to External IP, you will discover only machines with external IP addresses.</td>
</tr>
</tbody>
</table>
### Option Description

The connection string depends on the type and level at which NAT mapping is configured.

- **None (use DNS):** The Collector resolves the IP address to the virtual machine based on the configured name resolution mechanisms. For example, DNS or Hosts.

- **Internal IP:** The IP address that the virtual machine has in the vApp.

- **vApp External IP:** The IP address external to the vApp addresses of the virtual machines that are configured with NAT at the vApp level.

- **Org External IP:** The IP address external to the organization addresses of the virtual machines that are configured with NAT at the organization level or at the organization and vApp level. If NAT is implemented at the vApp and organization level, select this option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Name Filter</td>
<td>To run the query against all system resources in a vCloud Director instance, type the name of the vCloud Director instance. SQL wildcard expressions are allowed. Discovers all virtual machines managed by the vCloud Director instance.</td>
</tr>
<tr>
<td>Org Name Filter</td>
<td>To run the query against an organization in a vCloud Director instance, type the name of the organization. SQL wildcard expressions are allowed. Discovers all virtual machines in the organization.</td>
</tr>
<tr>
<td>vDC Name Filter</td>
<td>To run the query against a virtual datacenter in a vCloud Director instance, type the name of the virtual datacenter. SQL wildcard expressions are allowed. Discovers all virtual machines in the virtual datacenter.</td>
</tr>
<tr>
<td>vApp Name Filter</td>
<td>To run the query against a vApp, type the name of the vApp. SQL wildcard expressions are allowed. Discovers all virtual machines in the vApp.</td>
</tr>
<tr>
<td>VM Name Filter</td>
<td>To run the query to add a specific virtual machine, type the name of the machine. SQL wildcard expressions are allowed. Discovers the virtual machine.</td>
</tr>
<tr>
<td>Network Name Filter</td>
<td>To run the query against resources on a particular network, type the name of the network. SQL wildcard expressions are allowed. Discovers all virtual machines on the network.</td>
</tr>
<tr>
<td>IP Address Filter</td>
<td>To run the query to add virtual machines with a particular IP address, type the address. SQL wildcard expressions are allowed. Discovers all virtual machines with that IP address.</td>
</tr>
</tbody>
</table>

**Include** Select Yes to include the properties of this discovery rule to update the connection.
8. On the Important page, select the options and click Finish.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would you like to run this Discovery Rule now?</td>
<td>Select Yes.</td>
</tr>
<tr>
<td>License and Install Agent on Discovered Machines</td>
<td>If you do not use NAT mapping, select the option to install the Agent.</td>
</tr>
<tr>
<td></td>
<td>If you use NAT mapping, you must manually install the Agent on the discovered machines.</td>
</tr>
</tbody>
</table>

**What to do next**

- Review the discovery jobs to determine if your job finished. Click **Administration** and select **Job Manager > History > Other Jobs**.
- Review the collected vCloud Director vApp virtual machine data. Click **Administration** and select **Machines Manager**. In **Available Machines** and **Licensed Machines**, select the operating system type and review the list for the added virtual machines.
- If the discovered machines are listed only in the Available Machines list and the virtual machines use NAT mapping, you must manually install the Agent appropriate for the operating system. For Windows operating systems, see "Manually Install the VCM Windows Agent" on page 93. For Linux or UNIX operating systems, see "Install the Agent on UNIX/Linux Machines" on page 124.

**Configure vShield Manager Collections**

Configure collections from your vShield Manager instances so that you can run reports on the collected data.

**Prerequisites**

- To maintain secure communication, you need the SSL certificates from your instances of vShield Manager. See "Obtain the SSL Certificate Thumbprint" on page 29.

**Procedure**

1. "Add vShield Manager Instances" on page 47
   Add the instances of vShield Manager to VCM so that you can license and collect vShield Manager data using the Managing Agent.
2. "Configure the vShield Manager Settings" on page 47
   Configure the Managing Agent, communication, and vShield Manager access options so that VCM can collect group and group member data from your instances of vShield Manager.
3. "Collect vShield Manager Data" on page 49
   Collect the data from the instances of vShield Manager. The data is displayed by detailed data type and appears in the VCM Console.
The collected vShield Manager data appears in the Console in the Virtual Environments node. See "vShield Manager Collection Results" on page 49.

**Add vShield Manager Instances**

Add the instances of vShield Manager to VCM so that you can license and collect vShield Manager data using the Managing Agent.

Most vShield Manager instances are discovered, added, and licensed. Use this procedure if they are not added to VCM.

**Prerequisites**

- Ensure that the vCenter Server that each instance of vShield Manager is managing is added to VCM. See "Add vCenter Server Instances" on page 30.
- Know the names and domain information for the instances of vShield Manager in your environment.

**Procedure**

1. Click Administration.
2. Select Machines Manager > Available Machines.
3. Click Add Machines.
4. On the Add Machines page, select Basic: Name, Domain, Type, Automatically license machines, and click Next.
5. On the Manually Add Machines - Basic page, configure these options to identify the instances of vShield Manager.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine</td>
<td>Name of the instance of vShield Manager.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the instance of vShield Manager belongs.</td>
</tr>
<tr>
<td>Type</td>
<td>Domain type.</td>
</tr>
<tr>
<td>Machine Type</td>
<td>Select vShield.</td>
</tr>
</tbody>
</table>

6. Click Add.

   The machine information is added to the list.

7. (Optional) Add other instances of vShield Manager as needed.

8. When all your instances of vShield Manager are added to the list, click Next.

9. On the Information page, review the summary and click Finish.

**What to do next**

Configure the vShield Manager settings. See "Configure the vShield Manager Settings" on page 47.

**Configure the vShield Manager Settings**

Configure the Managing Agent, communication, and vShield Manager access options so that VCM can collect group and group member data from your instances of vShield Manager.
Prerequisites

- Collect Machines data from the Windows machine that you designated as your Managing Agent. See "Collect Machines Data From the Managing Agent Machines" on page 27.
- If you are using SSL Certificates to maintain secure communication, you must provide the certificate thumbprint from the target system when configuring the settings. See "Obtain the SSL Certificate Thumbprint" on page 29.

Procedure

1. Click Administration.
2. Select Machines Manager > Licensed Machines > Licensed Virtual Environments.
3. Select the instances of vShield Manager and click Configure Settings.
4. On the Virtual Environment page, verify that the vShield Manager instances appear in the lower pane and click Next.
5. On the Managing Agent and Communication Settings page, configure the settings that are applied to all selected vShield Manager instances and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Agent</td>
<td>Select the Windows machine to manage communication between the Collector and the vShield Manager instances. This Windows machine must have the 5.5 Agent or later installed. You can use the Collector as your managing agent.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port used by the API on the vShield Manager instances. The default value is 443.</td>
</tr>
<tr>
<td>User ID</td>
<td>Type a vShield Manager instance user name. The user must have a vShield Manager administrative role or an unrestricted read only role.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password for the vShield Manager instance user ID.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Type the password again.</td>
</tr>
</tbody>
</table>
| Ignore untrusted SSL Certificate | Select one of the following certificate options.  
  - Yes: Ignores the requirement for a valid signed certificate.  
  - No: Requires a valid signed certificate. |
| Select vCenter for vShield    | Select the vCenter Server instance managed by this vShield Manager instance. |
6. If you selected No on the Managing Agent and Communication Settings page, you must type or paste the thumbprint string in the text box and click Next.

7. On the Important page, click Finish.

What to do next
Collect vCloud Director data. See "Collect vShield Manager Data" on page 49.

Collect vShield Manager Data

Collect the data from the instances of vShield Manager. The data is displayed by detailed data type and appears in the VCM Console.

Prerequisites
Configure the vShield Manager settings. See "Configure the vShield Manager Settings" on page 47.

Procedure
1. Click Administration.
2. Select Machines Manager > Licensed Machines > Licensed Virtual Environments.
3. Select the vShield Manager instances and click Collect on the VCM toolbar.
4. On the Collection Type page, select Machine Data and click OK.
5. On the Machines page, verify that the Selected list includes all the vShield Manager instances from which you are collecting and click Next.
6. On the Data Types page, select the Virtualization that you want to collect from the vShield Manager instances and click Next.
7. On the Important page, resolve any conflicts and click Finish.

What to do next
Review the collected virtualization data. Click Console and select Virtual Environments > vCloud Director.

Discover the vApp virtual machines created by the vCloud Director and make them available in VCM. See "Discover vCloud Director vApp Virtual Machines" on page 43.

vShield Manager Collection Results

The collected vShield Manager data appears in the Console and is available to generate reports.

The displayed data is only as current as the last time you collected data from your vShield Manager instances.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Displays collected vShield Manager instance data.</td>
</tr>
<tr>
<td></td>
<td>Click Console and select Virtual Environments &gt; vCloud Director.</td>
</tr>
<tr>
<td>Reports</td>
<td>Create and run configured vShield Manager reports.</td>
</tr>
<tr>
<td>Administration</td>
<td>Displays managed vShield Manager instances from which you are collecting data.</td>
</tr>
<tr>
<td></td>
<td>Click Administration and select Machines Manager &gt; Licensed Machines &gt; Licensed Virtual Environments to view licensed vShield</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administration &gt;</td>
<td>Dynamic machine groups based on vShield App instances security group</td>
</tr>
<tr>
<td>Machine Groups</td>
<td>membership and are used to limit the displayed data.</td>
</tr>
</tbody>
</table>

**Configure ESX Service Console OS Collections**

The ESX Service Console OS Linux data type data and the ESX logs are collected directly from the ESX operating systems, not from vCenter Server. Configure the ESX servers so that you can collect the Linux data type and ESX log data from the ESX service console operating system.

To collect the data, VCM uses an Agent Proxy rather than a VCM Agent installed directly on the ESX and ESXi machines. To support the Agent Proxy, you must copy required files and certificates on the ESX and ESXi servers to manage the data collection from those machines.

Perform the required tasks first for ESX servers, and then for ESXi servers.

1. "Configure the Collector as an Agent Proxy" on page 50
   
   The Agent Proxy machine is a Windows machine configured to communicate with ESX and ESXi servers and to remotely collect data from those servers. The Collector automatically meets the Agent Proxy requirements. You license the Collector and then collect the Machines data type.

2. "Configure Virtual Machine Hosts" on page 51
   
   License virtual machine hosts to generate a file containing machine names and settings. You use the generated file to configure the ESX machines for management in VCM.

3. "Copy Files to the ESX/ESXi Servers" on page 53
   
   To import target machine information and copy the required files from VCM, you use the UNIX/ESX/vSphere Deployment Utility on your Agent Proxy machines.

4. "Collect ESX Logs Data" on page 55
   
   An initial collection of Virtual Environments data identifies your virtual machine hosts and their guest machines.

You have several options for reviewing and using ESX Logs data in VCM. The data used is only as current as the last collection, and the amount of time it takes for the data to display is based on the volume or complexity of the data requested. See "Virtualization Collection Results" on page 55.

**Configure the Collector as an Agent Proxy**

The Agent Proxy machine is a Windows machine configured to communicate with ESX and ESXi servers and to remotely collect data from those servers. The Collector automatically meets the Agent Proxy requirements. You license the Collector and then collect the Machines data type.

**NOTE** If you manage more than fifty host machines, you must use a separate Windows machine as your Agent Proxy. Moving the Agent Proxy activity to the separate machine optimizes performance. See "Configuring Standalone Agent Proxy Machines" in the online Help.
Procedure

1. Click Administration.

2. Select Machines Manager > Licensed Machines > Licensed Windows Machines.

3. Determine whether the Collector machine name appears in the data grid.
   If it is listed in the data grid, the machine is licensed. If it is not listed, continue with the licensing process.

4. License the Collector.
   a. Select Machines Manager > Available Machines.
   b. Select the Collector in the data grid and click License
   c. On the Machines page of the Available Machines License wizard, verify that the Collector machine name appears in the Selected list and click Next.
   d. Review the Product License Details page and click Next.
   e. Review the Important page and click Finish.
   f. Select Administration > Machines Manager > Licensed Machines > Licensed Windows Machines to verify that the Collector is now licensed.
   g. Click Refresh on the Console toolbar to update the data.

5. Run a collection for machines data to identify the Collector as an available Windows machine.
   a. Select Machines Manager > Licensed Windows Machines, select the Collector in the data grid, and click Collect on the Console toolbar.
   b. On the Collection Type page, click Machine Data and click OK.
   c. On the Machines page, verify that the Collector machine name appears in the Selected list.
   d. Click Select Data Types to collect from these machines and click Next.
   e. On the Data Types page, expand the Windows tree and select Machines.
   f. Select Use default filters and click Next.
   g. Review the Important page and click Finish.

The collection job starts. You can use the Job Manager to determine when the collection is finished.

What to do next

- When the collection is completed, verify that the Collector machine Agent Proxy State equals Current Agent. Click Administration and select Machines Manager > Agent Proxies and review the data grid.
- License and configure the target virtual machine hosts. See "Configure Virtual Machine Hosts" on page 51.

Configure Virtual Machine Hosts

License virtual machine hosts to generate a file containing machine names and settings. You use the generated file to configure the ESX machines for management in VCM.

All Virtualization data types are collected through Web Services communication except for the VM Logs, which are collected through SSH and only from ESX machines.
Prerequisites

- Verify that at least one Agent Proxy machine is configured. See "Configure the Collector as an Agent Proxy" on page 50.

Procedure

1. Click Administration.
2. Select Machines Manager > Licensed Machines > Licensed ESX/ESXi Hosts.
3. Select the ESX host and click Configure Settings.
4. Add the machines to be configured to the lower grid and click Next.

The selected machines will use the same Agent Proxy and the same SSH and Web Services settings.
5. Configure the settings on the Agent Proxy and Communication Setting page.

<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Proxy</td>
<td>The configured Agent Proxy used to manage the selected virtual machine host machines. This option is required when you are licensing host machines, but it is optional if you are modifying the settings.</td>
</tr>
</tbody>
</table>
| SSH Settings      | Select the check box to configure the settings for your ESX machines. Configure these settings so that you can collect ESX Logs data from the managed host machines.  
|                   | † **Port**: Used by VMware Web Services SDK for the ESX server on which SSH listening. The Agent Proxy communicates with the ESX server using this port. The default port (22) is set to the default value for SSH on ESX.  
|                   | † **User ID**: Used by the Agent Proxy to communicate with the ESX server through SSH. This account must have certain permissions, for example, `sudoers`, defined in the installation process. Authentication for this account uses public key cryptography that was setup during the installation process. |
| Web Services      | (Optional) Select the check box to configure the settings for your ESX and ESXi machines. Configure the settings to collect virtual environment data from a host machine.  
| Settings          | † **Port**: The port on the ESX server used by the Agent Proxy to communicate with the VMware web services interface.  
|                   | † **User ID**: The account that has access to the VMware Web services interface. If you are using ESX, this account must have Administrator access to Web services on the ESX server. This user ID may be different from the user ID for SSH communication, depending on whether you created different accounts during the ESX installation process.  
|                   | † **Password**: The password for the Web services User ID specified above. This password is encrypted in the VCM database.  
|                   | † **Confirm Password**: Retype the password.  
|                   | † **Ignore untrusted SSL Certificate**: Connection allowed even when certificates are not verified as trusted. |

6. On the Important page, record the `.xml` file name.

   The file is saved to the location configured for `CMFiles$\VMHosts_Config`. The default location is `%Program Files (x86)%\VMware\VCM\WebConsole\L1033\Files\VMHosts_Config`.

7. Click Finish.

**What to do next**

Copy the copy SSH public key file, the `csiprep.py` file, and the `csiprep.config` file to the target ESX machines. See "Copy Files to the ESX/ESXi Servers" on page 53.

**Copy Files to the ESX/ESXi Servers**

To import target machine information and copy the required files from VCM, you use the UNIX/ESX/vSphere Deployment Utility on your Agent Proxy machines.
For ESX machines, you import target machine information from VCM and copy the SSH public key file, the csiprep.py file, and the csiprep.config file to the target ESX machines.

For ESXi machines, you import machine information and copy the necessary Web Services settings to the target machines.

**Prerequisites**

- License the ESX and ESXi machines. See "Configure Virtual Machine Hosts" on page 51.
- Locate the UNIX/ESX/vSphere Deployment Utility file in C:\Program Files (x86) \VMware\VCM\Tools\DeployUtility-<version number>. Consult the Deployment Utility online help when using the tool.

**Procedure**

1. Copy the UNIX/ESX/vSphere Deployment Utility file to the Agent Proxy machine, either a standalone Windows machine or the Collector, and unzip the file.
2. Double-click DeployUtil.exe to start the Deployment Utility.
3. Click the ESX/vSphere Configuration tab.
4. Click File > Open.
5. Browse to the location of the virtual machine hosts configuration file generated when you licensed and configured the virtual machine hosts.
   
   The default location on the Collector is \Program Files (x86) \VMware\VCM\WebConsole\L1033\Files\VMHosts_Config.
6. Select the .xml file and click Open.
   
   The machine information in the .xml file is imported into the ESX Server Settings table on the ESX/vSphere Configuration tab with the settings that you defined in VCM.
7. Select a configuration option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure ESX 3.x Servers</td>
<td>Configures the SSH certificate, the csiprep.py file, the csiprep.config file, and passes the SSH and Web Services user information to the target ESX machines.</td>
</tr>
<tr>
<td>Configure ESXi Servers</td>
<td>Passes the Web Services to the target ESX machines</td>
</tr>
</tbody>
</table>

8. (Optional) Configure the default server location.
   
   The following settings are automatically configured to the default server locations. If you need to change the paths, click the ellipsis button.
   
   - SSH Public Key file (ESX 3.x only)
   - Log Files Location
   - csiprep.py File (ESX 3.x only)
   - csiprep.config File (ESX 3.x only)

9. (Optional) Configure the VCM user name and password.
   
   To modify the settings in VCM, use the following options or manually change the values in the ESX Server Settings table. For more information about the settings, see the Deployment Utility online Help.
- Use the same user name for both SSH and Web Services collections (ESX 3.x only).
- Use the same password for all WebServices users.
- Apply the same user names and passwords to all ESX servers.

10. **Click Configure.**

    All the machines where the Configure check box is selected now have the same version of the files copied to the location specified in the Remote Path field in the table. If no path is specified, the files are copied to the /tmp directory.

**What to do next**

Collect data from the target virtual machine hosts. See "Collect ESX Logs Data" on page 55.

**Collect ESX Logs Data**

An initial collection of Virtual Environments data identifies your virtual machine hosts and their guest machines.

**Procedure**

1. On the Portal toolbar, click **Collect**.
2. Select your ESX Servers.
   
    To avoid configuration conflicts, do not select both for one action. The selected machines appear in the Selected list.
3. Click **Select Data Types to collect from these machines** and click **Next**.
4. Expand the UNIX node and select the **Machines - General** data type.
5. Expand the Virtualization node and select the **ESX Logs** data types.
6. Click **Use default filters** and click **Next**.
7. Click **Finish**.

Monitor the collection job in Job Manager. When the collection is completed, the data appears is available for reports and compliance assessments.

**What to do next**

Review the collected data in the Console, run reports, configure alerts, and use the machine groups. See "Virtualization Collection Results" on page 55.

**Virtualization Collection Results**

You have several options for reviewing and using ESX Logs data in VCM. The data used is only as current as the last collection, and the amount of time it takes for the data to display is based on the volume or complexity of the data requested.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>View ESX logs.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Console</strong> and select <strong>Virtual Environments &gt; ESX Logs</strong>.</td>
</tr>
</tbody>
</table>
Configure the vSphere Client VCM Plug-In

The vSphere Client VCM Plug-In provides contextual access to VCM change, compliance, and management functions. It also provides direct access to collected vCenter Server, virtual machine host, and virtual machine guest data.

When using the vSphere Client VCM Plug-In, the virtual machine host name in vCenter must match the virtual machine host name in VCM.

**CAUTION** Anyone accessing VCM and the vSphere Client must have a unique login. Do not share vSphere Client logins between VCM users. Do not share vSphere Client logins between VCM users and non-VCM users.

Procedure

1. "Register the vSphere Client VCM Plug-In" on page 56
   The registration process configures the URL in the VMware vSphere Client to the VCM Collector and makes the VCM Summary and VCM Actions tabs available in the vSphere Client.

2. "Configuring the vSphere Client VCM Plug-In Integration Settings" on page 57
   Configure integration settings in VCM for your vSphere Client VCM Plug-In users. The settings enable users to view the VCM reports.

3. "Manage Machines from the vSphere Client" on page 58
   vSphere Client-managed machines are available in the vSphere Client VCM Plug-In when they licensed and have the VCM Agent installed. The available actions include collecting new data and running compliance, patching, and reports for the selected machines.

Register the vSphere Client VCM Plug-In

The registration process configures the URL in the VMware vSphere Client to the VCM Collector and makes the VCM Summary and VCM Actions tabs available in the vSphere Client.

The plug-in is installed with VCM. To unregister a previous version of the plug-in, see the online Help.

**IMPORTANT** The account that you use to register the vSphere Client VCM Plug-In should be a local administrator on the vSphere instance. The account must connect to a machine that has a valid SSL certificate or must register an invalid certificate (for example, a development certificate) when that user logs into the vSphere Client.

Prerequisites

- Verify that you are using VMware vCenter 4 Server.
- Verify that the VMware vSphere Client is installed.
- Verify that the VMware Tools is installed on the virtual machines.
Procedure

1. On the VCM Collector, browse to [path]\VMware\VCM\Tools\vSphere Client VCM Plugin\bin and double-click VCVPInstaller.exe.

2. In the VCVP Plug-in Registration dialog box, configure the following options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register</td>
<td>Select the option to register the URL for the plug-in. Select Unregister only if you are discontinuing the use of the plug-in on the target vSphere Client.</td>
</tr>
<tr>
<td>Server URL</td>
<td>Type the http or https path, where &lt;server&gt; is your vSphere Client server.</td>
</tr>
<tr>
<td>Administrator User Name</td>
<td>Type the name of a user with Administrator privileges in the vSphere Client.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Type the associated password.</td>
</tr>
<tr>
<td>URL to vSphereClientVCMPlugin.xml</td>
<td>Type the http path, where &lt;VCMServer&gt; is the name or IP address for the VCM Collector. The xml file is located in \VMware\VCM\WebConsole\L1033\VCVPAnon\Xml\vSphereClientVCMPlugin.xml</td>
</tr>
</tbody>
</table>

3. Click OK.

4. Start VCM.

5. On the login screen, select the role that you are using to log into the vSphere Client VCM Plug-In.

6. Select the **Automatically log in using this role** check box.

7. Start the vSphere Client.

8. Select a Guest machine.

**What to do next**

- Confirm that you can access the **VCM Summary** and **VCM Actions** tabs.
- Configure the vSphere Client VCM Plug-In integration settings in VCM. See "Configuring the vSphere Client VCM Plug-In Integration Settings" on page 57.

**Configuring the vSphere Client VCM Plug-In Integration Settings**

Configure integration settings in VCM for your vSphere Client VCM Plug-In users. The settings enable users to view the VCM reports.

**Prerequisites**

Verify that the vSphere Client VCM Plug-In is registered. See "Register the vSphere Client VCM Plug-In" on page 56.
Procedure

1. Select Administration > Settings > Integrated Products > VMware > vSphere Client VCM Plug-In.
2. Select the setting that you want to configure and click Edit Settings.
3. On the Settings Wizard page for each setting, configure the options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine group against which the external</td>
<td>Type the name of the machine group.</td>
</tr>
<tr>
<td>reports will be run</td>
<td>The default value is All Machines.</td>
</tr>
<tr>
<td>Role to use for external report access</td>
<td>Type the name of the user role to be used to access the reports.</td>
</tr>
<tr>
<td></td>
<td>The default value is Read-Only. Users other than Admin must have the role</td>
</tr>
<tr>
<td></td>
<td>selected here in order to see reports in the vSphere Client.</td>
</tr>
<tr>
<td>User name to use for assessments</td>
<td>Type the name of the user who will be running assessments to obtain data</td>
</tr>
<tr>
<td></td>
<td>for generating reports.</td>
</tr>
</tbody>
</table>

4. Click Next.
5. Verify your settings and click Finish.

What to do next

You manage machines by running compliance, patching, and reports. See "Manage Machines from the vSphere Client" on page 58.

Manage Machines from the vSphere Client

vSphere Client-managed machines are available in the vSphere Client VCM Plug-In when they licensed and have the VCM Agent installed. The available actions include collecting new data and running compliance, patching, and reports for the selected machines.

Prerequisites

- License Windows and UNIX/Linux virtual machines. See "License Windows Machines" on page 90 and "License UNIX/Linux Machines" on page 123.
- Install the Agent on the virtual machine. See "Install the VCM Windows Agent on Your Windows Machines" on page 91 and "Install the Agent on UNIX/Linux Machines" on page 124.
- Verify that the integration settings are configured. See "Configuring the vSphere Client VCM Plug-In Integration Settings" on page 57.

Procedure

1. Start the vSphere Client.
2. Click the VCM Actions tab.

What to do next

Click help on the VCM Actions tab for more information about the actions.

Troubleshooting the vSphere Client VCM Plug-In Registration

With the vSphere Client VCM Plug-In, you can view and run certain VCM actions in the vSphere Client.
You can use troubleshooting options to identify and resolve any problems.

**Invalid Certificate on a vSphere Client**

The vSphere Client connects to the vCenter Server using the SSL certificate and displays the datacenters, hosts, and any clusters.

**Problem**

When logging into a vSphere Client for the first time, if the certificate is not valid, a security warning about the SSL certificate appears.

**Cause**

The certificate is not valid.

**Solution**

1. Select the Install this certificate and do not display any security warnings for <vCenter_Server_Instance> option.
2. Click Ignore.

**HTTPS/SSL Is Not Configured on the Collector**

If the VCM Summary and VCM Actions tabs are not displayed, the settings are improperly configured.

**Problem**

In the vSphere Client, you cannot see the VCM Summary or VCM Actions tabs.

**Cause**

If Use SSL was selected during VCM installation, the https/SSL is not properly configured on the Collector.

**Solution**

1. Open the .xml file specified during the registration.
2. Edit the file to reflect the configured connection method, either http or https.

**vSphere Client VCM Plug-In Is Not Enabled**

If the VCM Summary and VCM Actions tabs are not displayed, the plug-in is not properly configured.

**Problem**

In the vSphere Client, you cannot see the VCM Summary or VCM Actions tabs.

**Cause**

The plug-in is not enabled in the vSphere Client.

**Solution**

1. In the vSphere Client, select Plug-ins > Manage Plug-ins.
2. In the Installed Plug-ins area, right-click the vCenter Configuration Manager Extension plug-in, and select Enable.
3. Close the Plug-in Manager.

When the tabs appear, you are ready to use the vSphere Client VCM Plug-In.
Compliance templates evaluate the virtual environment object data to determine if the objects meet the criteria in the rules. If the property values on an object do not meet the criteria, and if there is no exception defined, then the object is flagged as noncompliant. When an object is non compliant, the template results provide the details of the settings or configurations that do not match the rules. You can use this information to resolve the issue.

Compliance templates include the following components:

- **Rule Groups**: The rule groups comprise rules and filters.
- **Rules**: The rules define the optimal configuration standard.
- **Filters**: The filters limit the objects on which the template runs to only the objects that meet the filter criteria. If filters are not defined, the rules are run against all objects in the virtual objects group.
- **Exceptions**: The exceptions are optional temporary or permanent exceptions to the template results. The defined exception indicates that a specific result is compliant or noncompliant even though it does not match the requirements of the rules.

After you configure your compliance templates, you can optimize how VCM monitors the compliance of objects in your environment using alerts and scheduling regular compliance template runs on your collected virtual environment data.

This chapter includes the following topics:

- Create and Run Virtual Environment Compliance Templates 61
- Create Virtual Environment Compliance Rule Groups 62
- Create and Test Virtual Environment Compliance Rules 63
- Create and Test Virtual Environment Compliance Filters 64
- Preview Virtual Environment Compliance Rule Groups 64
- Create Virtual Environment Compliance Templates 65
- Run Virtual Environment Compliance Templates 66
- Resolve Noncompliant Virtual Environments Template Results 67
- Configure Alerts and Schedule Virtual Environment Compliance Runs 69

### Create and Run Virtual Environment Compliance Templates

Create compliance templates that evaluate your virtual environment object data to determine if the objects meet the criteria in the rules that define objects as compliant or noncompliant.
The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Prerequisites
Collect virtual environments data. See “Configure Virtual Environments Collections” on page 25.

Procedure
1. "Create Virtual Environment Compliance Rule Groups” on page 62
   Create rule groups so that you can add rules and filters.
2. "Create and Test Virtual Environment Compliance Rules” on page 63
   Create rules that define the ideal value that objects should have to be considered compliant.
3. "Create and Test Virtual Environment Compliance Filters” on page 64
   Create filters that limit the objects on which the templates run to only the objects that meet the filter criteria.
4. "Preview Virtual Environment Compliance Rule Groups” on page 64
   Preview the rule group to ensure that your combination of rules and filters are returning the expected results. Use the rules preview action, with the filters turned off and then turned on to determine if a rule group is returning the expected results.
5. "Create Virtual Environment Compliance Templates” on page 65
   Create compliance templates that include one or more rule groups configured to assess your selected object group to determine which objects are compliant and noncompliant.
6. "Run Virtual Environment Compliance Templates” on page 66
   Run templates against your collected data to determine which objects are compliant or noncompliant.
7. "Resolve Noncompliant Virtual Environments Template Results” on page 67
   The results for the compliance templates indicate whether the rule was compliant or noncompliant, and whether you can enforce noncompliant results manually or using VCM, or you can add an exception for expected noncompliant results.

Create Virtual Environment Compliance Rule Groups
Create rule groups so that you can add rules and filters.

Templates can include one or more rule groups. Rule groups comprise rules and filters.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Procedure
1. Click Compliance.
2. Select Virtual Environment Compliance > Rule Groups.
3. Click Add.
4. Type the Rule Group Name and Description in the text boxes and click OK.
   For example, Guest Tools Running and a description.

What to do next
Add a rule to the rule group. See "Create and Test Virtual Environment Compliance Rules” on page 63.
Create and Test Virtual Environment Compliance Rules

Create rules that define the ideal value that objects should have to be considered compliant.

The data types correspond to the collected virtual environments data that is displayed in the Console. To identify the values you are configuring for compliance, review the data grids so that you can locate the correct data type in the rule wizard.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Prerequisites

Create a rule group. See "Create Virtual Environment Compliance Rule Groups" on page 62.

Procedure

1. Click Compliance.
2. Select Virtual Environment Compliance > Rule Groups > rule group name > Rules.
   Guest Tools Running is the rule group in this example.
3. Click Add.
4. Type the Name and Description in the text boxes and click Next.
   For example, Tools Running.
5. Expand Virtualization, select vCenter - Guests - Summary, and click Next.
   The collected guest summary data includes whether the VMware Tools is installed and running on the guest virtual machines.
6. Select Basic and click Next.
7. Click Add and configure the rules with the ideal values.
   - In the properties drop-down menu, select Tools Running Status.
   - Select = as the rule operator.
   - Click the ellipsis button and select guestToolsRunning and click OK.
   - Click Next.
8. Select the Severity of a failure in the drop-down menu and click Next.
9. Review the changes and click Finish.
   The rule is added to the data grid.
10. Select your new rule and click Preview.
11. Select Do not apply machine filters to preview and click OK.
    When you test a rule, test first without the filter to ensure that the rule returns the expected results.
12. Review the data in the Non-compliant results window to verify that your rule is behaving as expected.

What to do next

Add a filter to the rule group. See "Create and Test Virtual Environment Compliance Filters" on page 64.
Create and Test Virtual Environment Compliance Filters

Create filters that limit the objects on which the templates run to only the objects that meet the filter criteria. If filters are not defined, the rules are run against all objects in the selected virtual objects group.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_ Dev.

Prerequisites

- Create a rule group. See "Create Virtual Environment Compliance Rule Groups" on page 62.
- Create a rule. See "Create and Test Virtual Environment Compliance Rules" on page 63.

Procedure

1. Click Compliance.
2. Select Virtual Environment Compliance > Rule Groups > rule group name > Filters.
   Guest Tools Running is the rule group in this example.
3. Click Add.
4. Type the Name and Description in the text boxes and click Next.
   For example, Not vCenter_ Dev
5. Expand Virtualization, select vCenter - Guest - Summary, and click Next.
   The collected guest summary data includes vCenter names.
6. Select Basic and click Next.
7. Click Add and configure the filter with the values to limit assessed objects or to exclude objects from assessment.
   - In the properties drop-down menu, select vCenter.
   - Select <> as the filter operator.
   - Click the ellipsis and select vCenter_ Dev and click OK.
   - Click Next.
8. Review the changes and click Finish.
   The filter is added to the data grid.
10. Review the data in the Machines window to verify that your filter is behaving as expected.

What to do next

Test your rule and filter together. See "Preview Virtual Environment Compliance Rule Groups" on page 64.

Preview Virtual Environment Compliance Rule Groups

Preview the rule group to ensure that your combination of rules and filters are returning the expected results. Use the rules preview action, with the filters turned off and then turned on to determine if a rule group is returning the expected results.
The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Prerequisites

- Create a rule group. See "Create Virtual Environment Compliance Rule Groups" on page 62.
- Create a rule. See "Create and Test Virtual Environment Compliance Rules" on page 63.
- Create compliance filters. See "Create and Test Virtual Environment Compliance Filters" on page 64.

Procedure

1. Click Compliance.
2. Select Virtual Environment Compliance > Rule Groups.
   Guest Tools Running is the rule group in this example.
3. Select your new rule group and click Preview.
4. Select Do not apply machine filters to preview and click OK.
   When you test a rule, test first without the filter to ensure that the rule returns the expected results.
5. Review the data in the Non-compliant results window to verify that your rule is behaving as expected.
6. Close the window.
7. Select your new rule group and click Preview.
8. Select Apply machine filters to preview and click OK.
9. Review the data in the Non-compliant results window to verify that your rule is behaving as expected.
   If the results are incorrect, adjust your rules and filters until they work correctly when you preview them.

What to do next

- If you have more than one rule that you must run in a particular order, set the order. The Set Order option is located on the toolbar.
- Create a template. See "Create Virtual Environment Compliance Templates" on page 65.

Create Virtual Environment Compliance Templates

Create compliance templates that include one or more rule groups configured to assess your selected object group to determine which objects are compliant and noncompliant.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.
Prerequisites
Create a rule group. See "Create and Test Virtual Environment Compliance Rules" on page 63.

Procedure
1. Click Compliance.
2. Select Virtual Environment Compliance > Templates.
3. Click Add.
4. Type the Name and Description in the text boxes and click Next.
   For example, Tools Running Not vCenter_Dev and a description.
5. Move the rule group, for this example, Guest Tools Running, to the list on the right and click Next.
6. Select Return both compliant and non-compliant and click Next.
   Returning compliant and noncompliant results will help you determine whether your template is returning the correct results.
7. Review your changes and click Finish.

What to do next
Run the template. See "Run Virtual Environment Compliance Templates" on page 66.

Run Virtual Environment Compliance Templates
Run templates against your collected data to determine which objects are compliant or noncompliant.
When a compliance template is run, the results appear in a report format and a data grid format.
The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Prerequisites
Create a template. See "Create Virtual Environment Compliance Templates" on page 65.

Procedure
1. Click Compliance.
2. Select Virtual Environment Compliance > Templates.
3. Select your template in the data grid and click Run.
   In this example, select Tools Running Not vCenter_Dev.
4. Click OK.
5. When the template run is finished, click Close.
6. Double-click the template name in the data grid.
   Unless you turned off the summary view, the Virtual Environments Compliance Results report appears. The report includes the number of objects that are compliant and the number that are noncompliant.
7. To view the results in the data grid, click View data grid.
What to do next

- If you find results that you want to temporarily make compliant or noncompliant, create an exception. See "Create Virtual Environment Compliance Exceptions" on page 68.
- Evaluate the results and resolve any issues on the noncompliant objects.

Resolve Noncompliant Virtual Environments Template Results

The results for the compliance templates indicate whether the rule was compliant or noncompliant, and whether you can enforce noncompliant results manually or using VCM, or you can add an exception for expected noncompliant results.

These procedures provide a variety of examples that apply to virtual environments compliance.

Procedure

- "Enforce Compliance Template Results Using VCM Actions" on page 67
  Resolve noncompliant results using VCM actions on the data grids to change settings when the action is not available for enforceable compliance.

- "Manually Enforce Compliance Template Results" on page 68
  Resolve noncompliant results by directly accessing the physical or virtual machine, or by accessing the object in vCenter Server, to change the noncompliant configuration setting.

- "Create Virtual Environment Compliance Exceptions" on page 68
  Rather than resolve noncompliant results, exceptions are the method you use to temporarily or permanently override the specific template results.

Enforce Compliance Template Results Using VCM Actions

Resolve noncompliant results using VCM actions on the data grids to change settings when the action is not available for enforceable compliance.

For this example, a template includes a rule that requires virtual machines to be powered on. If a virtual machine is powered off, the object is noncompliant. The compliance remediation action is to power it on.

Procedure

1. Click Compliance.
2. Select Virtual Environments Compliance > Templates > {template name}.
3. In the Status column, identify the rule results that are noncompliant.
4. Identify the affected physical or virtual machines or virtual objects, and determine the expected value of the property.
   For example, click and drag the Status column heading and the Rule column heading to the filter. Expand the noncompliant results and the rule related to the power state. The noncompliant object appears in the object column.
5. To resolve the noncompliant results, click Console and select Virtual Environments or the Windows tab or UNIX tab, and browse to the data grid where the action is available.
   For example, click Console and select Virtual Environments > vCenter > Guests > Summary.
6. Select the machines or objects that you identified as noncompliant and click the applicable action button on the data grid.

   For example, select the virtual machines that are powered off that should be powered on to be compliant and click Power VM On.

7. Follow the prompts to configure the options, select Run action now, and click Finish.

What to do next

Collect the appropriate data from the physical or virtual machines or objects and run compliance against the collected data. The objects should now be compliant.

Manually Enforce Compliance Template Results

Resolve noncompliant results by directly accessing the physical or virtual machine, or by accessing the object in vCenter Server, to change the noncompliant configuration setting.

Procedure

Using the allowed methods, change the noncompliant setting value on the machine or object to the required compliant value.

What to do next

Collect the appropriate data from the physical or virtual machines or objects and run compliance against the collected data. The objects should now be compliant.

Create Virtual Environment Compliance Exceptions

Rather than resolve noncompliant results, exceptions are the method you use to temporarily or permanently override the specific template results.

The exceptions are defined against the template results and indicate that a specific result is compliant or noncompliant even though it does not match the requirements of the rules.

You can add exceptions only to existing templates.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

To create an exception in this example, a virtual machine, RHEL_60_ProdDev, is approved to be excluded from the noncompliant results because you never require VMware Tools to be running on this machine.

Prerequisites

Create a template. See "Create Virtual Environment Compliance Templates" on page 65.

Procedure

1. Click Compliance.
2. Select Virtual Environment Compliance > Templates > template name.
3. Select the noncompliant result on which you are basing the exception and click Add Exception.
   
   In this example, the noncompliant result is the RHEL_60_ProdDev guest machine.
4. Type the Name, Short Description, Description, and Sponsor in the text boxes and click Next.
5. Select the template to which you are applying the exception in the drop-down menu and click Next.
   
   For this example, select Tools Running Not vCenter_Dev.
6. Select the object group to which you are applying the exception and click Next.
For this example, select All Virtual Objects.

7. Select the override options and the expiration date.
   a. Select **Override non-compliant results to compliant**.
   b. Select **No Expiration**.
   c. Click **Next**.

8. To define the exception values, modify, delete, or add to the properties, operators, and values for the selected results.
   In this example, you are specifying the RHEL_60_ProdDev as the exception.
   a. Click **Add**.
   b. In the properties drop-down menu, select **Object**.
   c. Select `=` as the rule operator.
   d. Click the ellipsis button and select **RHEL_60_ProdDev** in the property values dialog box and click **OK**.

9. Click **Finish**.

**What to do next**

- Run the template. See "Run Virtual Environment Compliance Templates" on page 66.
- Create alerts and schedule regular runs of your compliance templates. See "Configure Alerts and Schedule Virtual Environment Compliance Runs" on page 69

**Configure Alerts and Schedule Virtual Environment Compliance Runs**

To optimize how VCM monitors the compliance of objects in your environment, configure alerts and schedule regular compliance template runs on your collected virtual environment data.

**Prerequisites**

Create at least on virtual environments compliance template. See "Create and Run Virtual Environment Compliance Templates" on page 61.

**Procedure**

1.  "Create Virtual Environment Compliance Alert Rules" on page 70
   Alert rules are the conditions you define that determine when an alert is generated. Virtual environment alert rules are based on virtual environment compliance templates.

2.  "Create Virtual Environments Compliance Alert Configurations" on page 70
   Virtual environment compliance alert configurations are created for virtual objects groups to generate alerts when a virtual environment compliance template returns non-compliant results during scheduled runs of the template.

3.  "Schedule Virtual Environments Compliance Template Runs" on page 71
   Schedule a regular run of your virtual environments compliance templates to ensure that the collected data is regularly assessed for adherence to the defined compliance rules.
Create Virtual Environment Compliance Alert Rules

Alert rules are the conditions you define that determine when an alert is generated. Virtual environment alert rules are based on virtual environment compliance templates.

Prerequisites

Verify that you have virtual environment compliance templates. See "Create and Run Virtual Environment Compliance Templates" on page 61.

Procedure

1. Click Administration.
2. Select Alerts > Rules.
3. Click Add.
4. Type the alert name and description in the text boxes and click Next.
5. Select VE Compliance Results Data and click Next.
6. Select a compliance template and click Next.
7. Review the configured actions and click Finish.

What to do next

Create a virtual environments configuration that includes this rule. See "Create Virtual Environments Compliance Alert Configurations" on page 70.

Create Virtual Environments Compliance Alert Configurations

Virtual environment compliance alert configurations are created for virtual objects groups to generate alerts when a virtual environment compliance template returns non-compliant results during scheduled runs of the template.

You must have at least one unused rule to add to the alert configuration parameters.

Prerequisites

Verify that you have virtual environment alert rules. See "Create Virtual Environment Compliance Alert Rules" on page 70.

When you configure the automated responses, see the online help for configuration details.

Procedure

1. Click Administration.
2. Select Alerts > Virtual Environments Configuration.
3. In the middle pane, select the virtual objects group for which you want to generate an alert if one or more rules in the template fail.
4. Click Add.
5. Select a virtual environments compliance results alert rule and click Next.
6. Select the alert severity and click Next.
   You can select Critical, Important, Moderate, or Low.
7. Select and configure one or more automated responses that are performed when an alert is generated and click Next.
8. Review the alert configuration and click Finish.
What to do next

Schedule a job to run your virtual environments compliance templates on a timetable of your choosing. See "Schedule Virtual Environments Compliance Template Runs" on page 71.

Schedule Virtual Environments Compliance Template Runs

Schedule a regular run of your virtual environments compliance templates to ensure that the collected data is regularly assessed for adherence to the defined compliance rules.

Compliance templates are run against collected data, so you should also schedule collections for the data types and virtual objects that you are assessing.

Prerequisites

- Schedule a regular collection of the virtual environments data types for the virtual object groups against which you are running the virtual environments compliance templates.
- Create Virtual Environments Compliance Template. See "Create and Run Virtual Environment Compliance Templates" on page 61.
- Create Virtual Environments Compliance Alerts. See "Create Virtual Environment Compliance Alert Rules" on page 70.

Procedure

1. Click Administration.
2. Select Job Manager > Scheduled.
3. Click Add.
4. Select Compliance and click Next.
5. Type a name and description in the text boxes and click Next.
6. Select the virtual environment template and click Next.
7. Select the virtual objects against which to run the template assessment and click Next.
8. Configure frequency, time of day, and duration for the job and click Finish.
9. To test whether the job is producing the expected results, click Run Now on the data grid toolbar.

The job runs at the scheduled time.

What to do next

If you have a configured virtual environments compliance alert for this template and non-compliant rules were found, you can review any alerts in the Alerts node in the Console.
Configuring vCenter Operations Manager Integration

Integration of VCM with vCenter Operations Manager reports VCM configuration change events and standard compliance results in vCenter Operations Manager.

This chapter includes the following topics:

- Configure vCenter Operations Manager Change Events
- Standards Compliance for vCenter Operations Manager

Configure vCenter Operations Manager Change Events

Configure the data types to report to vCenter Operations Manager as change events and the threshold reporting level used to roll up the configuration changes. VCM records configuration changes in the change log regardless of whether you report the data in vCenter Operations Manager. From vCenter Operations Manager, you can navigate to VCM to view the details.

You can report on UNIX and Windows configuration change data and VCM initiated reboot changes. VCM reports change data to vCenter Operations Manager. vCenter Operations Manager polls VCM for configuration changes every five minutes.

For example, you can configure VCM to report a UNIX data type to vCenter Operations Manager and set the threshold reporting level to roll up a defined number of configuration changes into a single reporting icon to report the changes in the vCenter Operations Manager console.
Procedure

1. In VCM, click Administration.
2. Select Settings > Integrated Products > VMware > vCenter Operations Manager > Change Events.
3. Configure VCM to report a UNIX data type, such as UNIX Patch Assessment, to vCenter Operations Manager.
   a. Select UNIX Patch Assessment - Report to vCenter Operations Manager, and click Edit Setting.
   b. Click Yes to report the data.
   c. Click Next and click Finish.
4. Set the threshold reporting level to roll up the configuration changes in the vCenter Operations Manager console.
   a. Select UNIX Patch Assessment - Rollup Threshold, and click Edit Setting.
   b. Type the number of configuration changes for the collection to roll up to a single reporting icon to report in vCenter Operations Manager.
   c. Click Next and click Finish.

For details about the reporting settings, see the VCM online help.

Standards Compliance for vCenter Operations Manager

The integration between vCenter Operations Manager and VCM includes using the VCM compliance template results to contribute to the Risk badge score in vCenter Operations Manager.

The compliance templates are included in badge mappings that are run in VCM against objects in vCenter Server instances that are managed by both VCM and vCenter Operations Manager. These objects include virtual machines, host systems, clusters, vCenter Server instances, and data stores. The compliance mapping results determine the compliance score. vCenter Operations Manager then pulls the scores into the formulas used to calculate the Risk badge scores.

When you review the standards compliance in vCenter Operations Manager, you can navigate back to VCM to view the detailed results and identify any configuration changes that you must make to bring an object that is noncompliant back to compliance.

The correct correlation of the scores requires the following conditions:

- VCM is configured to collect data from the same vCenter Server instances that are managed by vCenter Operations Manager. See "Configure vCenter Server Data Collections" on page 30.
- You must collect the required virtualization data types from the shared vCenter Server instances. The data types are vCenter Guests, vCenter Hosts, vCenter Inventory, and vCenter Settings. See "Collect vCenter Server Data" on page 32.

Configure vCenter Operations Manager Standards Compliance

Create vCenter Operations ManagerCompliance badge scores that are based on the results of VCM compliance template mapping runs. The badge scores are values that appear in vCenter Operations Manager for vCenter Server instances, datacenters, clusters, virtual machine hosts, and virtual machines managed by your vCenter Operations Manager and VCM.
Prerequisites

- Verify that VCM is configured to collect data from the same vCenter Server instances that vCenter Operations Manager manages. See "Configure vCenter Server Data Collections" on page 30.
- Collect the required virtualization data types from the shared vCenter Server instances. The data types are vCenter Guests, vCenter Hosts, vCenter Inventory, vCenter Settings. See "Collect vCenter Server Virtual Machines Data" on page 35.
- Create compliance templates to include in the mappings. You can use Machine Group Compliance templates and Virtual Environments Compliance templates. See "Create and Run Virtual Environment Compliance Templates" on page 61.
- Review how the badge scores are calculated based on your compliance badge settings and compliance mapping options. See "Scoring Badges for vCenter Operations Manager Standards Compliance" on page 79.

Procedure

1. "Create Compliance Badge Mappings" on page 75
   Create badge mappings that contribute to the Risk badge score in vCenter Operations Manager. When you configure the mappings, you specify the templates to include, the badge to which it is assigned, and how the score is calculated.

2. "Run Compliance Badge Mappings" on page 77
   When you run the compliance badge mapping, the included templates are run against the collected data and a score is calculated based on the selected options and settings for the badge to which it is assigned.

3. "Review Mapping Scores in the Dashboard Report" on page 78
   The roll up scores appear in the Compliance Badge Rollup dashboard. Review the dashboard to ensure that the scores are calculated as expected.

4. "Schedule Compliance Badge Mapping Runs" on page 78
   Schedule the compliance badge mapping runs so that you have consistently current scores that are pulled into vCenter Operations Manager.

5. "View Compliance Badges in vCenter Operations Manager" on page 79
   The standards compliance score in VCM contributes a compliance score to the Risk badge score in vCenter Operations Manager. If the Risk score indicates distress for the object, you can view the compliance breakdown to determine which of the noncompliant templates are contributing to the score and determine what action to take to resolve the noncompliant results.

Create Compliance Badge Mappings

Create badge mappings that contribute to the Risk badge score in vCenter Operations Manager. When you configure the mappings, you specify the templates to include, the badge to which it is assigned, and how the score is calculated.
Prerequisites

- Use the Content Wizard tool to download compliance templates created by VMware, for example, the vSphere Hardening Guides and other standards. The Content Wizard is available from the Start menu on the Collector machine.

- Create compliance templates that are specific to your environment to include in the mappings. The template names should not include the '|' character. You can use Machine Group Compliance templates and Virtual Environments Compliance templates. See “Create and Run Virtual Environment Compliance Templates” on page 61.

- Review how the scores are calculated before configuring the mappings. See ”Scoring Badges for vCenter Operations Manager Standards Compliance” on page 79.

Procedure

1. Click Compliance.

2. Select vCenter Operations Manager Badge Mapping > Mappings.

3. Click Add.

4. Configure the basic settings for the mapping, select the machine group or virtual objects group context, and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Mapping name. Do not use the '</td>
</tr>
<tr>
<td>Description</td>
<td>Mapping description</td>
</tr>
<tr>
<td>Badge</td>
<td>Select the badge to which the mapping applies.</td>
</tr>
<tr>
<td></td>
<td>- Risk - Compliance: Mapped to the vCenter Operations Manager Risk badge.</td>
</tr>
<tr>
<td></td>
<td>- VCM Only: Not mapped to a vCenter Operations Manager badge.</td>
</tr>
<tr>
<td></td>
<td>This option allows you to test mapping configurations before assigning them to vCenter Operations Manager. Does not appear in vCenter Operations Manager.</td>
</tr>
<tr>
<td>Roll Up Type</td>
<td>Select the method used to calculate how the score for the templates in a mapping is determined. Scores are always between 0 and 100. A score of 0 indicates that all the rules are noncompliant. A score of 100 indicates that all the rules are compliant.</td>
</tr>
<tr>
<td></td>
<td>- Simple Percentage: Percentage of the template results that are compliant.</td>
</tr>
<tr>
<td></td>
<td>- Weighted Percentage: Percentage of the template results that are compliant where the Critical severity rule results are weighted more heavily than the Low severity rules results.</td>
</tr>
<tr>
<td></td>
<td>- Simple Rule Percentage: Percentage of compliance rules in the templates that passed as compliant. If any of the results are non-compliant, the rule is noncompliant.</td>
</tr>
<tr>
<td></td>
<td>- Weighted Rule Percentage: Percentage of the compliance rules in the templates where the Critical severity rule results are weighted more heavily than the Low severity rules results.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Select Group Context</td>
<td>Select compliance template context for which you are creating this mapping.</td>
</tr>
<tr>
<td></td>
<td>- Machine Group Compliance: Select this option to add machine group templates to the mapping. The virtual machines and host machines must also be managed as virtual objects in VCM in order for the machine object IDs to correlate to the objects in vCenter Operations Manager.</td>
</tr>
<tr>
<td></td>
<td>- Virtual Object Group Compliance: Select this option to add virtual environments templates to the mapping.</td>
</tr>
</tbody>
</table>

5. Select the Machine Group or Virtual Objects Group from which to build the mapping and click Next.

6. Select one or more templates to include in the mapping and click Next.

   The list of available templates is based on the selected machine or virtual object group. Templates used in compliance mappings should not include the `|` character.

7. Click Finish.

What to do next

Run the compliance badge mappings to determine if they are scoring as expected. See "Run Compliance Badge Mappings" on page 77.

Run Compliance Badge Mappings

When you run the compliance badge mapping, the included templates are run against the collected data and a score is calculated based on the selected options and settings for the badge to which it is assigned.

Prerequisites

- Collect the data from the machine or virtual object groups. Ensure that you collect the vCenter Guests, vCenter Hosts, vCenter Inventory, and vCenter Settings from your vCenter Server instances. See "Collect vCenter Server Data" on page 32.
- Create compliance badge mappings that include one or more templates. See "Create Compliance Badge Mappings" on page 75.

Procedure

1. Click Compliance.

2. Select vCenter Operations Manager Badge Mapping > Mappings.

3. Select a mapping and click Run.

4. Click OK.

   All templates included in the mapping are run and the score calculated. The template results are in the individual template results data grid and the score is available in the vCenter Operations Manager Compliance Rollup dashboard.

What to do next

Review the scores in the vCenter Operations Manager Compliance Rollup dashboard. See "Review Mapping Scores in the Dashboard Report" on page 78.
Review Mapping Scores in the Dashboard Report

The roll up scores appear in the Compliance Badge Rollup dashboard. Review the dashboard to ensure that the scores are calculated as expected.

The current roll up scores are also available in the Machine Group Compliance Badge Rollup Detail and Summary report.

Prerequisites

Run the Compliance Badge Mappings. See "Run Compliance Badge Mappings" on page 77.

Procedure

1. Click Console.
2. Select Dashboards > Compliance > Compliance Badge Rollup.
3. Review the scores and modify the settings as needed.

What to do next

- To ensure that the scores that are pulled into vCenter Operations Manager are always current, schedule the mappings to run at a regular time. See "Schedule Compliance Badge Mapping Runs" on page 78.
- (Optional) To change how the mappings are scored, modify the Standards Compliance Settings. Do not modify the scores unless you understand how the scores are calculated. See "Scoring Badges for vCenter Operations Manager Standards Compliance" on page 79.

Schedule Compliance Badge Mapping Runs

Schedule the compliance badge mapping runs so that you have consistently current scores that are pulled into vCenter Operations Manager.

Prerequisites

Schedule the collections for the vCenter Server instances on which you are running templates to complete the collections before you run the compliance mappings against the collected data. See "Configure vCenter Server Scheduled Collections" on page 33.

Procedure

1. Click Administration.
2. Select Job Manager > Scheduled and click Add.
3. Select vCenter Operations Manager Compliance Badge Mapping Run and click Next.
4. Type a name and description and click Next.
5. Select one mapping and click Next.
6. Use the scheduling options to schedule when the mapping runs.
   - Schedule the job to run at the frequency at which you want refreshed results to be available to pull into vCenter Operations Manager. Schedule the compliance badge mapping to run after your scheduled collection.
7. Click Finish.
What to do next

View the mapped badges in vCenter Operations Manager. See “View Compliance Badges in vCenter Operations Manager” on page 79.

View Compliance Badges in vCenter Operations Manager

The standards compliance score in VCM contributes a compliance score to the Risk badge score in vCenter Operations Manager. If the Risk score indicates distress for the object, you can view the compliance breakdown to determine which of the noncompliant templates are contributing to the score and determine what action to take to resolve the noncompliant results.

Prerequisites

Verify the following requirements.

- VCM adapter is installed.
- VCM adapter is registered.
- Internet Explorer is installed.
- You have a vCenter Operations Manager user name and password from the vCenter Operations Manager administrator.

Procedure

1. In vCenter Operations Manager, select an object in the inventory pane.
2. Click Dashboard.
3. Click Why is Risk (score)? and review the Compliance score.
4. Click the Compliance badge to view the template scores associated with the overall score.
5. On the Views tab, the score for each template appears in the Details section.
6. To view the template results in VCM, click View details in VCM for the template you are investigating.
7. If necessary, copy the URL provided in the Info dialog box into the Internet Explorer address bar.
   The template results appear in VCM.

What to do next

Resolve the noncompliant results. See “Resolve Noncompliant Virtual Environments Template Results” on page 67.

Scoring Badges for vCenter Operations Manager Standards Compliance

Badge scores are values that appear in a vCenter Operations Manager Compliance badge, and which also contribute to the dashboard values for the Risk badge.

The badge score pulled into vCenter Operations Manager is a calculated value that is based on your compliance mapping options and on the compliance badge settings configured in VCM and run against collected VCM data.

A compliance mapping is one or more compliance templates that run against a machine group or virtual object group and calculate scores based on the selected options and the defined settings. When the VCM adapter is configured in vCenter Operations Manager, the score appears as a Compliance badge for the Risk badge.
Scoring Calculation Process

The badge calculations are based on mapping options and standards compliance settings. The options and the settings interact in the following workflow:

- Scoring based on mapping options.
  - Select the compliance standard badge to which the mapping contributes a score.
  - Select the roll up type that determines the initial score calculation. If you select weighted percentages, the weight values are configured in the standards compliance settings.
- Setting detail level aggregation of scores based on the standards compliance options.
- Refining the badge scores as they appear in vCenter Operations Manager using the midpoint and magnitude settings.
- Scoring the Risk badge in vCenter Operations Manager.

Scoring Based on Mapping Options

You specify the badge name and the roll up types for each mapping you create in VCM.

Standards Compliance Badges

When you create a mapping in VCM, you select the vCenter Operations Manager badge with which it is associated.

The Compliance subbadges are aligned with the following vCenter Operations Manager badge and VCM-only roll up.

- Risk - Compliance scores are included in the Risk badge.
  The Risk badge indicates potential problems that might eventually degrade the performance of the managed environment. Risk does not necessarily imply a current problem. Risk indicates problems that might require your attention in the near future, but not immediately. The overall Risk score for an object ranges between 0 (no risk) to 100 (serious risk).
  Compliance mappings should include templates that evaluate your environment in a way that helps to identify performance issues. For example, you have an object setting that should be addressed if it is found to be noncompliant from the configuration standard, but it does not require immediate attention.
- VCM Only scores are available only in VCM.
  The VCM Only mapping scores are not pulled into vCenter Operations Manager. The scores are intended to provide mapping of multiple templates and scores only in VCM. For example, you can use this mapping to test a new mapping in VCM before you begin reporting the scores in vCenter Operations Manager.

The roll up type calculations for each badge determine the initial score.

Roll Up Types

The roll up types determine how the template results are initially scored.

When you create a compliance template, each template includes one or more rules, and you assign each rule a severity level of Low, Moderate, Important, and Critical. Each rule includes one or more individual checks that return one or more results for each check. The results for the individual checks that are made on the target machine or object determine if the object is compliant or noncompliant.
For the Weighted Percentage and Weighted Rule Percentage roll up types, you can apply a weighted value. The weighting is the value by which the result or rule is multiplied to give the different severity levels more or less weight when calculating the scores. The weighting of the severity levels is configured in the Standards Compliance Settings. The default values are Low=1, Moderate=2, Important=4, and Critical=8.

Simple Percentage is the percentage of the template results that are compliant. This option does not weight the results based on severity. For example, the simple percentage score for the results is 73. This score is calculated based on 11 compliant results out of a total of 15 results.

**Table 5–1. Simple Percentage Template Results**

<table>
<thead>
<tr>
<th>Severity</th>
<th>Compliant Results</th>
<th>Noncompliant Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Important</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Moderate</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Low</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>11</td>
<td>4</td>
</tr>
</tbody>
</table>

Weighted Percentage is the percentage of the template results that are compliant where the Critical severity rule results are weighted more heavily than the Low severity rules results. For example, the weighted percentage score for the results is 46. This score is calculated based on a weighted value of 27 compliant results out of a total of 59 results.

**Table 5–2. Weighted Percentage Template Results**

<table>
<thead>
<tr>
<th>Severity</th>
<th>Weight</th>
<th>Compliant Results</th>
<th>Weighting Calculations</th>
<th>Weighted Compliant Results</th>
<th>Noncompliant Results</th>
<th>Weighting Calculations</th>
<th>Weighted Noncompliant Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>8</td>
<td>1</td>
<td>8*1=8</td>
<td>8</td>
<td>4</td>
<td>8*4=32</td>
<td>32</td>
</tr>
<tr>
<td>Important</td>
<td>4</td>
<td>2</td>
<td>4*2=8</td>
<td>8</td>
<td>0</td>
<td>4*0=0</td>
<td>0</td>
</tr>
<tr>
<td>Moderate</td>
<td>2</td>
<td>3</td>
<td>2*3=6</td>
<td>6</td>
<td>0</td>
<td>2*0=0</td>
<td>0</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
<td>5</td>
<td>1*5=5</td>
<td>5</td>
<td>0</td>
<td>1*0=0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>27</td>
<td></td>
<td>27</td>
<td>32</td>
<td></td>
<td>32</td>
</tr>
</tbody>
</table>

Simple Rule Percentage is the percentage of compliance rules in the templates that passed as compliant. If any of the results are non-compliant, the rule is non-compliant. This option does not weight the rules based on severity. For example, the simple rule percentage is 40. This score is calculated based on two compliant rules out of a total of five rules.

**Table 5–3. Simple Rule Percentage Based on Template Rules**

<table>
<thead>
<tr>
<th>Rule/Severity</th>
<th>Compliant Results</th>
<th>Non-Compliant Results</th>
<th>Simple Compliant Rule</th>
<th>Simple Noncompliant Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 1/ Critical</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Rule 2/ Important</td>
<td>5</td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Rule 3/ Important</td>
<td>15</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Rule 4/ Moderate</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Rule 5/ Low</td>
<td>0</td>
<td>9</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
You might choose scoring by rule rather than by results when some rule groups return significantly more rules than other rules in the same rule group. For example, a rule that checks user accounts returns one result per user account on an object, but a rule that checks a password policy returns only one result for an entire system.

Weighted Rule Percentage is the percentage of the compliance rules in the templates where the Critical severity rule are weighted more heavily than the Low severity rules. For example, the weighted rule percentage is 53. This score is calculated based on a weighted value of 10 compliant rules out of a total of 19 rules.

**Table 5–4. Weighted Rule Percentage Based on Template Rules**

<table>
<thead>
<tr>
<th>Rule/Severity</th>
<th>Severity Weight</th>
<th>Compliant Results</th>
<th>Non-Compliant Results</th>
<th>Simple Compliant Rule</th>
<th>Simple Noncompliant Rule</th>
<th>Weighted Compliant Rule Value</th>
<th>Weighted Non-Compliant Rule Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 1/</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule 2/</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>1</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Important</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule 3/</td>
<td>4</td>
<td>15</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Important</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule 4/</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule 5/</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

**Detail Level Score Aggregation**

After the initial scoring, the Standards Compliance Settings determine the badge scores that are calculated for the vCenter Operations Manager badges, based first on the Detail Level aggregation, and then on the midpoint and magnitude.

The level from which to roll up the badge scores that are generated for each mapping.

Use the Standards Compliance badge settings to select the level of detail at which to roll up the scores, and the midpoint and magnitude used to adjust the scores that are reported in vCenter Operations Manager.

**Table 5–5. Detail Level Score Aggregation Example Values**

<table>
<thead>
<tr>
<th>Templates in Mappings</th>
<th>Score</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mapping 1 Template 1</td>
<td>80</td>
<td>10,000</td>
</tr>
<tr>
<td>Mapping 1 Template 2</td>
<td>50</td>
<td>5</td>
</tr>
<tr>
<td>Mapping 1 Template 3</td>
<td>100</td>
<td>1</td>
</tr>
<tr>
<td>Mapping 2 Template 4</td>
<td>30</td>
<td>100</td>
</tr>
<tr>
<td>Mapping 2 Template 5</td>
<td>75</td>
<td>500</td>
</tr>
</tbody>
</table>

- **Compliance Result:** To roll up at the compliance result level means that the scores for the templates assigned to the mapping, times the number of compliance results for each score divided by the total number of compliance results.

  For example, Mapping 1 has three templates using the scores and results provided in the Scoring table. The scoring is calculated as \((80\times10,000)+(50\times5)+(100\times1)/(10,000+5+1)=80\), where 80 is the score.
- Template: To roll up at the template level means that each template's scores are averaged when rolled up to the badge level.

  For example, Mapping 1 has three templates using the scores provided in the Scoring table. The score is calculated as \((80+50+100)/3=77\), where 77 is the score.

- Mapping: To roll up at the mapping level means that the score for each mapping associated with a badge is averaged when rolled up to the badge level.

  For example, Mapping 1 and Mapping 2 are assigned to the same badge. The score is calculated as \((77+53)/2=65\), where 77 is the Mapping 1 average, 53 is the Mapping 2 average, and 65 is the average of the two mappings included in the badge.

**Midpoint and Magnitude Score Calculations**

Use midpoint and magnitude to refine how the badge scores are ultimately calculated for vCenter Operations Manager.

- Midpoint: The score that triggers the magnitude to increase or decrease the returned score.

- Magnitude: The percentage by which any score that is above or below the midpoint is calculated.

The calculation is \([\text{detail level score}-\text{midpoint}]\times[\text{difference}]\); \([\text{difference}]\times[\text{magnitude}]\times[\text{adjusted magnitude factor}]\); \([\text{detail level score}]\times[\text{adjusted magnitude factor}]\times[\text{adjusted score}]\).

Detail level scores can differ even where the midpoint and magnitude remain the same.

<table>
<thead>
<tr>
<th>Table 5–6. Static Midpoint and Magnitude Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detail Level Score</strong></td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>20</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>40</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>70</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>100</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 5–7. Different Magnitude Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detail Level Score</strong></td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>70</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>70</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### The Adjusted Score

The adjusted score is the score that is pulled by the vCenter Operations Manager VCM Adapter and appears as part of the Risk badge score.

You modify the midpoint and magnitude to give the Compliance subbadge scores a stronger or weaker influence on the Risk parent badge. For example, if the compliance mappings score is configured so that it normally scores 100 and you want any deviation to clearly degrade the score, you can set the midpoint to 99 and the magnitude to a high value. The resulting adjusted score lowers the value of the compliance score and the Risk score when any noncompliance is found.

If you do not want to apply midpoint and magnitude calculations, set the magnitude to 0.

### Scoring the in vCenter Operations Manager

The standards compliance scores are pulled from VCM into vCenter Operations Manager and added to the Risk badge score using the following calculation:

- **Risk**: $100 - \text{GeometricMean}(\text{badge}\_\text{time}\_\text{remaining}, \text{badge}\_\text{capacity}\_\text{remaining}, 100 - \text{badge}\_\text{stress}, \text{badge}\_\text{risk}\_\text{compliance})$
Auditing Security Changes in Your Environment

The VCM Auditing capability tracks all changes in the security aspects of VCM. Security-related events are written to the Windows Event Log, which is stored on the Collector, and is independent of the VCM application. The format of the event log prohibits any modifications to the recorded entries, which makes it a secure and tamper-proof auditing record of changes in security.

When you perform an action in VCM that affects security, and the auditing setting that corresponds to that change is enabled, the event is written to the event log.

**Prerequisite**

Be logged in as a user who has the Admin role assigned.

**Procedure**

1. To view the VCM Auditing settings, click **Administration**.
2. Select **Settings > General Settings > Auditing**.
3. To change an auditing setting, highlight a setting and click **Edit Setting**.

   When you change an auditing setting, the VCM Auditing data grid displays the user’s name in the Last Modified By column.

**What to do next**

For details about the Auditing settings and the Windows Event Log, see the online help.
Configuring Windows Machines

To manage your virtual and physical Windows machines, you must verify domains and accounts, discover and license those machines, install the VCM Agent, and collect Windows data from those machines. You can also collect Windows Custom Information.

This chapter includes the following topics:

- **Verify Available Domains** 88
- **Check the Network Authority** 88
- **Assign Network Authority Accounts** 89
- **Discover Windows Machines** 89
- **License Windows Machines** 90
- **Install the VCM Windows Agent on Your Windows Machines** 91
- **Collect Windows Data** 97
- **Windows Collection Results** 98
- **Getting Started with Windows Custom Information** 99

**Configure Windows Machines**

To manage Windows machines, you must configure the environmental components and machine options in VCM.

**Procedure**

1. **Verify Available Domains**
   - Allow VCM access to each domain so that the VCM Collector can interact with the Windows machines in your environment.

2. **Check the Network Authority**
   - Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

3. **Assign Network Authority Accounts**
   - Select and assign the network authority account that you identified for VCM access to the Windows machines.

4. **Discover Windows Machines**
   - In your network, identify the Windows machines that you are managing with VCM.
5. **License Windows Machines**
   To manage Windows machines, you must license them in VCM.

6. **Install the VCM Windows Agent on Your Windows Machines**
   Install the VCM Windows Agent on each Windows machine so that you can collect data and manage the virtual or physical machines.

7. **Collect Windows Data**
   Start managing the Windows machines by performing an initial collection, which adds Windows machine data to VCM.

   Continuous Windows machine management is based on the latest data you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data. See "Windows Collection Results" on page 98.

### Verify Available Domains

Allow VCM access to each domain so that the VCM Collector can interact with the Windows machines in your environment.

During installation, VCM discovered all domains to which the network authority account had access. If the Windows machines belong to a domain that is not listed, you must add that domain manually.

**Prerequisites**

Verify that you have the fully-qualified names of the domains to manage.

**Procedure**

1. Click **Administration**.
2. Select **Settings > Network Authority > Available Domains**.
3. If the domain does not appear Available Domains view, add the domain.
   a. Click **Add**.
   b. Type the domain name and select the domain type as **NetBios** or **AD**, depending on your domain.
   c. Click **OK**.
4. Verify that the domain appears in the data grid.

**What to do next**

Verify that a network authority account is available and create other necessary domain accounts. See "Check the Network Authority" on page 88.

### Check the Network Authority

Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

Although you specified an initial default network authority account when you installed VCM, you can add different administrator accounts if you do not assign the default account.

**Prerequisites**

Verify the presence of domains. See "Verify Available Domains" on page 88.
Procedure

1. Click Administration.
2. Select Settings > Network Authority > Available Accounts.
3. To add a new domain account, click Add.
4. Type the domain name, user name, and password, and click Next.
5. Click Finish to add the account.

What to do next

Assign the network authority account to the domain so that VCM can access the Windows machines in the domain. See "Assign Network Authority Accounts" on page 89.

Assign Network Authority Accounts

Select and assign the network authority account that you identified for VCM access to the Windows machines.

You can assign a single account to all domains and machine groups, or assign a unique account or multiple accounts to each domain and machine group.

In this procedure, NetBios is used as the example.

Prerequisites

Verify or add the necessary network authority account. See "Check the Network Authority" on page 88.

Procedure

1. Click Administration.
2. Select Settings > Network Authority > Assigned Accounts > By Domain > NetBios.
3. Select an assigned account.
4. Click Edit Assigned Accounts.
5. Select the account to receive authority to the domain and click Next.
6. Confirm the accounts to include in the authority list for the domain and click Finish.

What to do next

Discover the Windows machines in your environment. See "Discover Windows Machines" on page 89.

Discover Windows Machines

In your network, identify the Windows machines that you are managing with VCM.

To discover the available Windows machines, VCM uses general discovery rules to identify many Windows machines or uses specific discovery rules to identify particular Windows machines.

The time required to perform an initial discovery depends on the size and composition of your network. If all Windows machines are not available during initial discovery, such as systems that are disconnected from the network, the first discovery will not find all Windows machines. If the discovery does not identify all Windows machines, you might need to run additional discoveries after the other Windows machines become available.
**NOTE** You can use the Discovered Machines Import Tool (DMIT), which imports machines discovered by the Network Mapper (Nmap), to import many physical and virtual machines at one time into the VCM database. Download DMIT from the VMware Web site.

The following procedure is based on Active Directory.

**Prerequisites**

Assign a Network Authority Account that VCM can use for access. See “Assign Network Authority Accounts” on page 89.

**Procedure**

1. Click Administration.
2. Select Machines Manager > Discovery Rules.
3. Click Add to create a discovery rule.
4. On the Discovery Rules page, type a name and description and click Next.
5. On the Discovery Method page, select By Active Directory and click Next.
6. On the AD Domain page, specify the AD Domain, select Discover machines only from the selected domain, and click Next.
7. On the Discovery Filters page, select Discover all machines in <domain_name> Domain.
8. (Optional) Create a filter to discover Windows machines based on a limited criteria and click Next.
9. On the Important page, click Yes and click Finish.
   To avoid exceeding your license count, do not select License and Install Agent on Discovered Machines.
10. On the toolbar, click Jobs to track current discovery job status.

**What to do next**

- Verify that jobs have finished running. Click Administration and select Job Manager > History > Other Jobs > Past 24 Hours.
- Verify that the Windows machines are available. Click Administration and select Machines Manager > Available Machines.
- License the Windows machines in your environment. See "License Windows Machines" on page 90.

**License Windows Machines**

To manage Windows machines, you must license them in VCM.

The number of discovered Windows, UNIX, or Linux machines might exceed the number of your available licenses. If that happens, the number available goes negative and appears in red to indicate that you do not have enough licenses.

For servers and workstations, exceeding the limit on your license key produces warnings but does not restrict VCM operation. License key counts that are over the limit are recorded and maintained for auditing purposes. Suite license keys support unlimited licenses, provided that the suite edition includes VCM and the component that you are managing is part of the suite. If a component is not part of the suite, it counts against the nonsuite server or workstation key.
Prerequisites

Verify that the Windows machines you license are listed with a machine type of workstation or server in the Available Machines node. If the discovered or added type is not workstation or server, VCM cannot license the machines.

Procedure

1. Click Administration.
2. Select Machines Manager > Available Machines.
3. Select the Windows machines to license.
4. Click License.
5. Verify that the Windows machines to license appear in the Selected list.
   Use the arrows to move the Windows machines.
6. Click Next to view your Product License Details.
   The licensed Windows machine count increases by the number of licensed machines.
7. Click Next.
   VCM confirms that the licenses you requested will be applied to the selected Windows machines.
8. Click Finish.

What to do next

Install the VCM Windows Agent on Your Windows Machines

Install the VCM Windows Agent on each Windows machine so that you can collect data and manage the virtual or physical machines.

Before you can collect data from Windows machines, you must install the VCM Windows Agent on the licensed Windows machines in your environment to enable communication between the Collector and the target machines.

You can use VCM to install the Agent or you can install the Agent manually. When you install a VCM Collector, the VCM Windows Agent is also installed. The Collector Agent is locked and cannot be unlocked, uninstalled, or upgraded.

Standardized Windows configurations such as Federal Desktop Core Configuration (FDCC) or United States Government Configuration Baseline (USGCB) include strict security group policy settings. The Windows Firewall: Do not Allow Exceptions group policy configures Windows Firewall to block all unsolicited incoming messages, including configured exceptions. This setting overrides all configured exceptions. For VCM to communicate properly with the VCM Agent on managed machines in strict, secure environments, disable the Windows Firewall: Do not Allow Exceptions group policy on the managed machines. For more information, see support.microsoft.com.

Prerequisites

- License the Windows machines on which you install the Agent. See "License Windows Machines" on page 90.
- Verify that you know the communication protocols and ports that are used by the Collector and the Agents.
Procedure

1. Click Administration.

2. Select Machines Manager > Licensed Machines > Licensed Windows Machines.

3. In the data grid, select one or more Windows machines on which to install the Agent and click Install.

4. On the Machines page, verify that the target machines appear in the Selected list and click Next.

5. On the Install Options page, select the installation options and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share</td>
<td>Location to install the Agent. The default location is ADMIN$.</td>
</tr>
<tr>
<td>Path</td>
<td>Path for the Agent files. The default path includes CMAgent.</td>
</tr>
<tr>
<td>Install From</td>
<td>VCM Collector from which to install the Agent.</td>
</tr>
<tr>
<td>DCOM</td>
<td>Communication protocol for the Agent. The default setting is DCOM.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Secure communication protocol for the Agent. Use HTTP, which installs the HTTP Listener on the target machine and configures it to listen on the designated port.</td>
</tr>
<tr>
<td>Port</td>
<td>Designated port for the HTTP Listener.</td>
</tr>
<tr>
<td>Install using a proxy server</td>
<td>For Windows Proxies and Windows Agents only. If the target machine is separated from the Collector by a proxy server, this option instructs the installation process to check for available proxy servers.</td>
</tr>
<tr>
<td>Lock the machine after installation</td>
<td>Ensures that VCM will not uninstall the Agent or replace it with a different version.</td>
</tr>
<tr>
<td>Reinstall Agent</td>
<td>Overwrites an installed Agent.</td>
</tr>
</tbody>
</table>

6. On the Schedule page, select Run Action now and click Next.

You can schedule subsequent Agent installations to run later.

7. Review the summary information and click Finish.

What to do next

- Verify that jobs have finished running. Click Administration and select Job Manager > History > Other Jobs > Past 24 Hours.

- Collect Windows data from VCM managed machines in your environment. See "Collect Windows Data" on page 97.

Locate the Enterprise Certificate

Locate the Enterprise Certificate before you install the VCM Agent on the managed Windows machine. VCM must access the Enterprise Certificate during the Agent installation.

If your Collector is operating in a full Public Key Infrastructure (PKI), and the target machine can validate the Collector root certificate (Enterprise Certificate), the .pem file is not required.
Procedure

1. Locate the Enterprise Certificate .pem file in the Collector’s c:\Program Files (x86) \VMware\VCM\CollectorData folder.

2. If the certificate files are not in the default location, you must confirm the path to the files.
   a. Click Administration.
   b. Select Settings > General Settings > Collector.
   c. Select Root directory for all collector files.
   d. Confirm the file path in the Value column.

Manually Install the VCM Windows Agent

You can manually install the Windows Agent on the VCM managed machine by using the executable (EXE) file or the Microsoft Installer (MSI) file that is supplied with VCM.

- You use the EXE file to install the Agent in unattended, silent mode. EXE files detect an existing software version and provide the option to uninstall the existing version.

- You use the MSI file to install the Agent in unattended, silent mode. MSI files are database files. The Windows msiexec.exe executable file reads the data in the MSI file, and then installs the Agent.

  The MSI file uninstalls any existing, non-MSI Agent without sending a request. If you run the MSI installer again, the removal option is available.

  If you use a new MSI file to upgrade an MSI-installed Agent, the old Agent is uninstalled.

The VCM Enterprise Certificate is installed when you initially installed VCM. During the Agent installation process, if you select HTTP, VCM installs the Enterprise Certificate in the certificate store on the VCM managed machine.

The Collector root certificate authenticates Collector requests on the managed machine before it processes a collection or change request. The authentication process uses the Collector Certificate and established trust to the Enterprise Certificate.

Use the EXE File to Install the Agent

You can use the EXE file to manually install the VCM Windows Agent on a target machine. The directories in this procedure are default locations.

---

**CAUTION** For Vista, Windows 7, and Windows 2008 only: If you set the compatibility mode on an Agent executable file to a previous version of Windows, VCM might report the compatible operating system instead of the actual operating system. For example, on a Windows 7 machine, if you set the Agent to run in compatibility mode for Windows XP, the Agent will report that the machine is a Windows XP machine.

---

Prerequisites

Locate the Enterprise Certificate before you install the VCM Agent. See "Locate the Enterprise Certificate" on page 92.
Procedure

1. On your VCM Collector, open Windows Explorer and navigate to the Agent files directory at C:\Program Files (x86)\VMware\VCM\AgentFiles.

2. Copy the CMAgentInstall.exe file from the Collector to the target machine or a shared network location.

   The CMAgentInstall.exe file is located in the path relative to the installed software on the Collector.

3. On the target machine, use Windows Explorer and run the installation in either normal or silent mode.
   - For normal mode, run CMAgentInstall.exe.
   - For silent mode, run CMAgentInstall.exe /s INSTALLPATH=%Systemroot%\CMAgent PORT=26542 CERT=C:\<folder_without_spaces>\vcm_cert.pem.

   The %Systemroot% environment variable specifies the directory where Windows is installed, which is typically \WINNT or \WINDOWS.

   Use the following options for the installation.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMAgentInstall.exe</td>
<td>Executable file used to install the Agent.</td>
</tr>
<tr>
<td>/s</td>
<td>Indicates a silent install. When you run CMAgentInstall.exe from the command line, VMware recommends that you install the Agent in silent mode. To use the silent mode, you must unlock the Agent before you can proceed with the installation. To unlock the Agent, use the -UNLOCK option. The syntax is CMAgentInstall.exe /s INSTALLPATH=%Systemroot%\CMAgent PORT=26542 CERT=C:&lt;folder_without_spaces&gt;\vcm_cert.pem. To relock your managed machine, you must submit a lock request from the VCM Collector. To submit the lock request, click Administration and select Settings &gt; General Settings &gt; Installer. Edit the Lock Agent after it is installed? setting to lock the managed machine.</td>
</tr>
</tbody>
</table>

   | INSTALLPATH     | Location to install the Agent files.       |
   | PORT            | Port number used for HTTP Agents.          |
   |                 | The default value is 26542.                 |
   |                 | If you do not include the PORT parameter, VCM uses DCOM and does not install the communication socket listener service. The certificate is not required. |

   | CERT            | Indicates the certificate that you generated or specified on the Collector during the Collector installation. The location of the certificate file is in the fully qualified path, local to the relative to the installed software on the Collector. By default the path is C:\Program Files (x86)\VMware\VCM\CollectorData\[certificate name].pem. If you include PORT, but do not use a certificate, you must use |
The CERT=SKIP parameter to allow an HTTP Agent to operate without a valid CERT path. The CERT path cannot contain spaces, even when enclosed in quotes, so enter an 8.3 compatible path as in the preceding silent mode example.


What to do next

- To confirm that the job finished running, click Administration and select Job Manager > History > Other Jobs > Past 24 Hours.
- Collect Windows data from VCM managed machines. See "Collect Windows Data" on page 97.

Use the MSI File to Install the Agent

You can use the MSI file to manually install the VCM Windows Agent on a target machine. The directories specified in this procedure are default locations.

Prerequisites

Locate the Enterprise Certificate before you install the VCM Agent. See "Locate the Enterprise Certificate" on page 92.

Procedure

1. On your VCM Collector, open Windows Explorer and navigate to the Agent files directory at c:\Program Files (x86)\VMware\VCM\AgentFiles.
2. Copy the CMAgent[version].msi file to the target machine or a shared network location.
   The CMAgent[version].msi file is located in the path relative to the installed software on the Collector.
4. If the file does not exist, you must copy CMAgent[Version].msi to the target machine, or install it from a network share onto the target machine.
5. Copy the Enterprise Certificate .pem file to the target machine.
6. On the target machine, in Windows Explorer, run CMAgent[Version].msi using the following syntax:

   msiexec /Option <Required Parameter> [Optional Parameter]

   For example:
   msiexec.exe /qn /i "[PathToFile]\CMAgent[Version].msi" [PORTNUMBER=<available port>] [INSTALLDIR="<new path>"]

   Use the following options for the installation.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMAgent[Version].msi</td>
<td>When used with default options, this command removes any existing Windows Agent, installs the new Agent in the %SystemRoot%\CMAgent directory, and uses DCOM for</td>
</tr>
<tr>
<td>Option</td>
<td>Action</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>communication.</td>
</tr>
<tr>
<td></td>
<td>When you include an option with CMAgent[Version].msi, you must follow these conventions:</td>
</tr>
<tr>
<td></td>
<td>- Include optional parameters in any combination and order.</td>
</tr>
<tr>
<td></td>
<td>- After the required /i parameter, use uppercase letters for</td>
</tr>
<tr>
<td></td>
<td>optional parameters.</td>
</tr>
<tr>
<td></td>
<td>- Use quotation marks when a path includes spaces in the</td>
</tr>
<tr>
<td></td>
<td>source file location and the INSTALLDIR parameter.</td>
</tr>
<tr>
<td></td>
<td>To see details about the options, select Start &gt; Run &gt;</td>
</tr>
<tr>
<td></td>
<td>msiexec.</td>
</tr>
<tr>
<td></td>
<td>%Systemroot%</td>
</tr>
<tr>
<td></td>
<td>Environment variable that specifies the directory where Windows is</td>
</tr>
<tr>
<td></td>
<td>installed, which is typically \WINNT or \WINDOWS.</td>
</tr>
<tr>
<td>/qb</td>
<td>Runs the command in a basic user interface and displays the</td>
</tr>
<tr>
<td></td>
<td>progress and error messages.</td>
</tr>
<tr>
<td>/qn</td>
<td>Runs the command in quiet mode without user interaction.</td>
</tr>
<tr>
<td>/i</td>
<td>Runs the command as an installation.</td>
</tr>
<tr>
<td>/x</td>
<td>Runs the command as an uninstall process.</td>
</tr>
<tr>
<td>PORTNUMBER</td>
<td>Installs the Windows Agent on the port number specified, and uses</td>
</tr>
<tr>
<td></td>
<td>HTTP instead of DCOM. For HTTP installations where you include</td>
</tr>
<tr>
<td></td>
<td>PORTNUMBER, you must include an Enterprise Certificate by using the following syntax:</td>
</tr>
<tr>
<td></td>
<td>CERTIFICATEFILE=&quot;&lt;drive&gt;:[mypath][mycert].pem&quot;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>msiexec.exe /qn /i &quot;C:\temp\CMAgent [VersionNumber].msi&quot;</td>
</tr>
<tr>
<td></td>
<td>PORTNUMBER=2666 CERTIFICATEFILE=&quot;x:\mypath\mycert.pem&quot;</td>
</tr>
<tr>
<td></td>
<td>If you include PORTNUMBER, you must either include the path</td>
</tr>
<tr>
<td></td>
<td>to the certificate file, or supplement the CERTIFICATEFILE</td>
</tr>
<tr>
<td></td>
<td>parameter with the SKIP parameter.</td>
</tr>
<tr>
<td>INSTALLDIR</td>
<td>Location to install the Agent. Use to change the default root</td>
</tr>
<tr>
<td></td>
<td>directory specification, which is %SystemRoot%\CMAgent.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>msiexec.exe /qn /i &quot;C:\temp\CMAgent [VersionNumber].msi&quot;</td>
</tr>
<tr>
<td></td>
<td>INSTALLDIR=&quot;C:\VCM&quot;</td>
</tr>
<tr>
<td>CERTIFICATEFILE</td>
<td>Includes the Enterprise Certificate with either the path or the</td>
</tr>
<tr>
<td></td>
<td>SKIP parameter.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
</tbody>
</table>
Configuring Windows Machines

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CERTIFICATEFILE=&quot;x:[mypath][mycert].pem&quot; or CERTIFICATEFILE=&quot;SKIP&quot;</td>
</tr>
</tbody>
</table>

**What to do next**

- To confirm that the job finished running, click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Collect Windows data from VCM managed machines. See "Collect Windows Data" on page 97.

**Manually Uninstall the VCM Windows Agent**

When you no longer manage a Windows machine with VCM, you uninstall the Agent from that target machine. If you used VCM to install the Agent, you must use VCM to uninstall the Agent.

To keep historical data, do not remove the Windows machine from VCM. After you remove the Windows Agent and remove the managed Windows machine from the list of licensed machines, VCM no longer manages the Windows machine and you can no longer collect data from it.

The Windows Agent uninstall executable file exists on the VCM managed machine if you installed the Agent manually using `CMAgentInstall.exe` or `CMAgentInstall.msi`. Use this manual process to uninstall the Agent only if you used either of these commands to install the Agent.

**Procedure**

1. On the VCM managed machine, run
   
   `%SystemRoot%\CMAgent\Uninstall\Packages\CMAgentInstall\UnCMAgentInstall.exe`

   This path displays the default location. The EXE file is located in the path relative to the installed software on the Collector.

**Collect Windows Data**

Start managing the Windows machines by performing an initial collection, which adds Windows machine data to VCM.

Use the default filter set to collect a general view of the Windows machines in your environment. The first time that you use the default filter to collect data, the Windows Agent returns all of the data specified in the filter and stores the data in the VCM database. All subsequent collections will return a delta against the data previously collected.

A delta collection includes only the differences between the data on the target machine and the data stored in the VCM database. If you need a full collection, you can specify that VCM collect all data again. A full collection can take a significant amount of time depending on the number of VCM managed Windows machines from which you are collecting.

When you perform a full collection from your entire environment, run the collection during nonworking hours so that users do not notice any performance impact on managed machines. After the initial collection is finished, subsequent delta collections will most likely not impact performance.
**Prerequisites**

- Collect the Accounts and Groups data types from the primary domain controller (PDC) in each domain to increase the performance of initial collections that require a SID lookup.
- To collect data from Windows XP SP2 or Vista machines that use DCOM communication, you must enable ICMP pings in the firewall settings or disable ICMP pings in VCM.
- Verify that DCOM is enabled on the managed machine. Run `dcomcnfg` and select Enable Distributed COM on this computer.

**Procedure**

1. On the VCM toolbar, click Collect.
2. On the Collection Type page, select Machine Data and click OK.
3. On the Machines page, select the Windows machines from which to collect data and click Next.
   
   To move all visible Windows machines to the selection window, 500 at a time, use the double arrow.
4. On the Data Types page, select the Select All checkbox.
5. Select Use default filters and click Next.
6. On the Important page, resolve any conflicts and click Finish.

**What to do next**

- Verify that jobs have finished running. Click Administration and select Job Manager > History > Other Jobs > Past 24 Hours.
- Review the collection results. See "Windows Collection Results" on page 98.

**Windows Collection Results**

Continuous Windows machine management is based on the latest data that you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data.

Windows data appears in VCM and is available for several management actions, including Console dashboards and reports, Compliance views, and VCM Patching. The displayed data is only as current as the last time you collected the data.

After the initial discovery is finished, perform a weekly discovery to update the list of available Windows machines. To schedule a VCM discovery job, click Administration, select Job Manager > Scheduled, and follow the wizard.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Displays dashboards and reports based on collected data. Use the Console to view data that is relevant to day-to-day operations, troubleshooting, and analysis.</td>
</tr>
<tr>
<td></td>
<td>- To view the dashboards, click Console and select Dashboards &gt; Windows &gt; Operating Systems.</td>
</tr>
<tr>
<td></td>
<td>- To view the summary reports, click Console and select Windows &gt; Operating System &gt; Machines. You can view the data in a summary report or data grid format.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Determines if the data collected from VCM managed Windows machines meets specified compliance values, and allows you to run compliance remediation actions.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>- To run a compliance check, click <strong>Compliance</strong> and select <strong>Machine Group Compliance</strong>.</td>
</tr>
<tr>
<td></td>
<td>- To create rule groups, rules, filters, and templates, see the online help.</td>
</tr>
<tr>
<td>Reports</td>
<td>Runs preconfigured reports or you can create custom reports. VCM runs reports against the latest collected data. Depending on the data volume or complexity of the requested report, it might take time to generate the report. You can also schedule and disseminate reports.</td>
</tr>
<tr>
<td></td>
<td>- To use the reporting options, click <strong>Reports</strong> and select <strong>Machine Group Reports &gt; Windows</strong>.</td>
</tr>
<tr>
<td>Patching</td>
<td>Assesses target machines to determine if the patching status of the Windows machines is up-to-date. You can install the latest patches on target machines.</td>
</tr>
<tr>
<td></td>
<td>- To assess and patch Windows machines, click <strong>Patching</strong> and select <strong>Windows</strong>.</td>
</tr>
<tr>
<td></td>
<td>- To run assessments and patch your Windows machines, see the online help.</td>
</tr>
</tbody>
</table>

**Getting Started with Windows Custom Information**

Windows Custom Information (WCI) is data collected from VCM managed machines that is created by PowerShell scripts. WCI supplements and extends the data collected by VCM from managed Windows machines using other VCM data types.

You can create or modify WCI scripts to collect almost any data type that is accessible from VCM managed machines. VCM supports PowerShell scripting and XML output to collect Windows Custom Information.
To extend the data collected by VCM from managed Windows machines using other VCM data types, collect Windows Custom Information. Configure the prerequisites and create and validate your PowerShell script.

**Prerequisites**

- To collect Windows Custom Information from VCM managed machines, you must configure the prerequisites. See "Prerequisites to Collect Windows Custom Information" on page 100.

**Procedure**

1. "Collecting Windows Custom Information" on page 112

    To collect Windows Custom Information (WCI) using script-based filters, you create and verify your custom PowerShell scripts, install PowerShell on the VCM managed machines, and use VCM to collect the WCI data.

**Prerequisites to Collect Windows Custom Information**

To collect Windows Custom Information from VCM managed machines, you must configure the prerequisites.
Prerequisites

- Write your own PowerShell script to return data in a VCM compatible, element-normal XML format, or obtain PowerShell scripts from VMware Professional Services or another source. See "Using PowerShell Scripts for WCI Collections" on page 101.
- Understand the script signing policies if you use PowerShell 2.0. See "PowerShell Script Signing Policies" on page 105.
- Set the PowerShell execution policy on the VCM managed machine. See "Built-In PowerShell Policy Settings" on page 106.
- Understand how to write and run PowerShell scripts. See "References on PowerShell and Script Signing" on page 106.
- Verify that your PowerShell script is accessible when you paste the script content into the Script area of the collection filter on the VCM Collector.
- Confirm that the VCM Collector includes PowerShell 2.0 if the Collector is a client for WCI collections.
- Understand how VCM manages Windows Custom Information data changes. See "Windows Custom Information Change Management" on page 111.
- Confirm that PowerShell 2.0 is installed on each VCM managed machine that will be used for WCI collections. See "Install PowerShell" on page 114.
- Upgrade older VCM Agents on the VCM managed machines from which you collect Windows Custom Information, and then install the VCM 5.3 Agent or later on these machines.
- Confirm or update the Agent Thread Administration settings on the VCM Collector. The default value is set to below normal thread priority, and the Agent Data Retention default is set to a 15-day change log.

Using PowerShell Scripts for WCI Collections

Windows Custom Information (WCI) uses PowerShell as the scripting engine and the element-normal XML format as the output that is inserted into the VCM database.

WCI supports PowerShell 2.0 and works with later versions of PowerShell.

- PowerShell 2.0 is the base requirement for WCI in VCM because of its ability to set the execution policy at the process level.
- You can run WCI PowerShell collection scripts against Windows machines that have PowerShell 1.0 installed if needed, although this usage is not supported or tested. If the collection scripts do not use PowerShell 2.0 commands, your WCI filters that use the in-line method to pass a WCI script to PowerShell will operate correctly.

The WCI data type uses extensions to the VCM Windows Agent. The extensions allow the Agent to invoke PowerShell scripts. Using the script-based collection filter, VCM passes the PowerShell scripts to a VCM managed machine, and the VCM Agent parses the resulting XML output. The default WCI filter returns the PowerShell version information from the managed machines.

WCI data type extensions are flexible because they use filter parameters that the command line uses to invoke the scripting engine. The WCI extensions use a COM class name to specify the parser required for the Agent to parse the script output, and allow new types of parsers to be added at the Agent. This approach extends the support of multiple scripting engines, languages, and output formats.
Guidelines in PowerShell Scripting for WCI

When you develop custom PowerShell scripts to collect the Windows Custom Information (WCI) data type from VCM managed Windows machines, follow these guidelines.

- Make XML element names unique at the same level.
  
  For example, you can specify two child nodes that are not siblings.
- Make attributes unique at the same level.
- Use unique XML element names to generate valid VCM XML. The XML elements are code blocks that include the element's start and end tags. The element can contain other elements, text, attributes, or a combination of them.
- Use repeatable identifiers to prevent false indications of changes at the Collector. If your element labels (identifiers) are not the same for every collection of the same item, you will see false additions, changes, and deletions in the VCM change log.
- Confirm that the script returns valid XML element names and attribute names.

If the data to be returned is an element name or an attribute name that is not valid for XML, you can encode the name using the `ToCMBase64String` function. A VCM Collector job, called the inserter, is executed during each collection. The inserter recognizes the names that are encoded with this function and decodes them in the raw insertion process.

The inserter parses the resulting XML file and inserts the data into a new raw database table named `VCM_Raw` by default. The XML process transforms the raw data into data that appears in VCM.

The function is defined as follows.

```powershell
function ToCMBase64String([string]$input_string)
{
    return [string]("cmbase64-" +
    [System.Convert]::ToBase64String([System.Text.Encoding]::UNICODE.GetBytes($input_string))).replace("=","-"
    )
}
```

- Include a comment block and configurable parameter entries near the start of the script so that when you clone a WCI collection filter you can see the parameters and set them when you edit the collection filter. To view and edit the collection filters, click Administration and select Collection Filters > Filters.
- Redirect any variable declarations in the script to out-null, along with any other tasks that generate output that is not part of the XML result set. For example, you can use the following command.

  ```powershell
  [reflection.assembly]::LoadWithPartialName("Microsoft.SqlServer.Smo") > out-null
  ```
- Do not include any formatting, white space, carriage returns, or line feeds at the end of elements, nodes, or attributes.

Challenges in PowerShell Scripting for WCI

When you develop custom collection scripts, understand the challenges that you might encounter while scripting in PowerShell to collect the Windows Custom Information (WCI) data type from VCM managed Windows machines.

PowerShell scripts can use the split method of PowerShell strings, which separates the columns of the rows into separate values in arrays. For example, Windows provides the `schtasks.exe` utility to manage scheduled tasks on a local or remote computer and report on the scheduled tasks.
The split method of PowerShell strings in the $schtasks script separates the columns of the $schtasks rows into separate values in arrays.

- Column names row provides the names to use for attributes.
- Corresponding data from the scheduled task rows provides the values to use for these attributes.

The top-level name of <schtasks> is an arbitrary name that you apply to distinguish the results of this script from other results. The XML script returns the parsed data, which resembles the following structure.

```
<schtasks>
  <taskname1>
    <attribute1>Value1</attribute1>
    <attribute2>Value2</attribute2>
  </taskname1>
  <taskname2>
    <attribute1>Value1</attribute1>
    <attribute2>Value2</attribute2>
  </taskname2>
</schtasks>
```

The returned data can include the following problems with content.

- White space, such as tabs or spaces, is not allowed in returned data.
- Column names include spaces.
- Specific task entries do not include a unique and repeatable identifier.
- Values can contain XML syntax in functions, which you must enclose in CDATA.
Column Names Include Spaces

Running the `schtasks` command without any options displays a column name of Next Run Time. Because this name includes spaces, you cannot use it as an attribute name in an XML document. Running the `schtasks` command verbosely generates other column names that include spaces. Although you cannot use these invalid names as attribute names, you can preserve the names by using VCM encoding standards.

To preserve these column names in the form that `schtasks` returns and allow for XML handling, VCM encodes the column names with the `ToCMBase64String` function. To create a valid XML form of an element name or attribute name, this function uses Unicode Base64 encoding and character substitution, such as using a dash instead of an equal sign, as shown in the following example.

```powershell
function ToCMBase64String([string]$input_string)
{
    return [string]"cmbase64-" +
    [System.Convert]::ToBase64String([System.Text.Encoding]::UNICODE.GetBytes($input_string)).replace("=","-")
}
```

Using this function corrects the invalid column name data.

VCM prefaxes the string with `cmbase64-` so that the VCM inserter can decode the data and load the decoded data into the VCM database.

The valid XML appears as follows.

```xml
<cmbase64=TgBlAHgAdAAgAFIAdQBuACAAVABpAG0AZQA->
12:32:00, 5/26/2010
</cmbase64=TgBlAHgAdAAgAFIAdQBuACAAVABpAG0AZQA->
```

Invalid XML omits the encoding function as follows.

```xml
<Next Run Time>
12:32:00, 5/26/2010
</Next Run Time>
```

Task Entries Do Not Include a Unique and Repeatable Identifier

Use repeatable identifiers to prevent false indications of changes at the Collector. If your element labels (identifiers) are not the same for every collection of the same item, you will see false additions, changes, and deletions in the VCM change log.

The Windows `schtasks` command does not include a unique and repeatable identifier for specific task entries. Because unique element names are a requirement for valid VCM XML and repeatable identifiers help prevent false indications of changes at the VCM Collector, you must code the task names correctly in your script.

To create unique and repeatable element names, create a task entry name based on a hash of the data in the row. You can use this method for data that does not have a name-type attribute, where the task name exists but is not guaranteed to be unique. When the task name is user-friendly and useful, you must attempt to preserve the name and use it in the collection script.
To preserve the user-friendly name, use the task name as the element name for the task rows. When you create a collection filter that uses your script, you must select the incremental duplicate handling option so that the collection process includes an incremental entry in the list of entries where the same task name appears multiple times.

For example, in a sample test environment, many Windows machines had more than one task named GoogleUpdateTaskMachineCore. A PowerShell script can label the rows as Task1, Task2, and so on. If you delete Task1, Task2 becomes Task1, and VCM displays multiple change details for Task1, such as the command line and the next run time. This report would be incorrect because even though Task 1 would have changed place in the sequence, the task would not have changed.

The task names are labeled accordingly.

- The first task entry is labeled GoogleUpdateTaskMachineCore.
- The second task entry is labeled GoogleUpdateTaskMachineCore_1.

Because task names can contain characters that are not valid in XML element names, VCM encodes the task names with the ToCMBase64String function. If you reorder the list of tasks whose names are identical, VCM can still report extra changes. For this reason, require the VCM user interface to display the friendly task names.

Enclose Values that Can Contain XML Syntax in CDATA

When you develop your custom PowerShell scripts to collect the Windows Custom Information data type from VCM managed Windows machines, you must use CDATA to enclose values that contain XML syntax.

For example:

```powershell
function wrapInCDATA( [string]$input_string)
{
    $wrappedInCDATA | out-null
    if ( $input_string.Length -gt 0 )
    {
        $wrappedInCDATA = "<!" + "[CDATA" + "$] + "$]" + ">"
    }
    return $wrappedInCDATA
}
```

PowerShell Script Signing Policies

With PowerShell 2.0 you can set the script signing policies at the machine, user, and process levels. The process level runs a single execution of `powershell.exe`.

In VCM, Windows Custom Information (WCI) uses script type information in the collection filter to determine how to execute PowerShell and how to pass the script to it.

Use the following methods to pass a WCI script to PowerShell.
- **In-line**: The default WCI filter uses an in-line script to collect basic information about the PowerShell version, .NET version, and execution policy settings. The in-line option requires a collection script that is represented as a single line of PowerShell code. Because the filter runs an in-line script on the PowerShell command line, instead of using a file, the execution policy does not apply.

- **Script file**: For script-based filters in WCI, the default script type command line includes options to set the process-level execution policy to Remote Signed. The script requires that the execution policy be set to Remote Signed at the most restrictive level because the script runs from a file that resides locally on the VCM managed Windows machine. For WCI, VCM can execute collection scripts on managed machines where the machine and user level signing policies are set to any level, without requiring you to change the setting.

**Built-In PowerShell Policy Settings**

Before you use the WCI collection filter to run file-based PowerShell scripts on the VCM Collector and your VCM managed machines, you must change the execution policy on the VCM managed machines. PowerShell contains built-in execution policies that limit its use as an attack vector. By default, the execution policy is set to Restricted, which is the primary policy for script execution.

The following policy settings apply to PowerShell scripts.

- **AllSigned**: PowerShell scripts must be signed by a verifiable certificate from the Software Publishing Certificate store. The typical file extension is .ps1. For signed scripts, you can set the execution policy to **All Signed**. You must sign the scripts and distribute the appropriate certificates before you collect WCI data.

- **RemoteSigned**: A verifiable certificate must sign any PowerShell script that you download from the Internet using a supported browser such as Internet Explorer. Script files that are not required to be signed are scripts that you create locally or scripts that you download using a method that does not support flagging the file source. For unsigned scripts, you must set the execution policy to the most restrictive level of **Remote Signed**. You can set the policy directly by using a Group Policy Object (GPO) with a VCM remote command. You can use a registry change action or enforceable compliance. For example:

  HKLM\Software\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
  "ExecutionPolicy"="RemoteSigned"

- **Unrestricted**: All PowerShell script files run regardless of whether they are signed by a verifiable certificate.

- **Restricted**: You can use PowerShell interactively or to run commands directly from the command line. This setting is the default.

**References on PowerShell and Script Signing**

For information about Windows PowerShell and script signing policies, see the Microsoft Web site.

**Create an Example PowerShell Script for Scheduled Tasks**

Use a custom PowerShell script to collect Windows Custom Information (WCI) data from VCM managed Windows machines. With this example, you can learn how to use PowerShell scripts to collect WCI data for scheduled tasks.

Windows provides the `schtasks.exe` utility to report on scheduled tasks that you create in the Task Scheduler user interface or by using the `AT` command. The `schtasks.exe` utility enables you to manage scheduled tasks on a local or remote computer and to report on the scheduled tasks.
The `schtasks` command returns basic information about scheduled tasks. The data returned by `schtasks` includes multiple rows. PowerShell structures the `$schtasks` variable in an array. For example, `$schtasks[0]` represents the first row. To view the result set, use `$schtasks[n]`, which displays the following status:

- `$schtasks[0]` is blank.
- `$schtasks[2]` is the first row of task data.

**Prerequisites**

- Review the guidelines to create PowerShell scripts for WCI collections, and understand the challenges in PowerShell scripting. See "Guidelines in PowerShell Scripting for WCI" on page 102.
- Understand how to write and run PowerShell scripts. See "References on PowerShell and Script Signing" on page 106.

**Procedure**

1. On your VCM managed Windows machine, click **Start**.
2. Select **All Programs > Accessories > Windows PowerShell**.
   - On a 64-bit Windows machine, select **Windows PowerShell (x86)** to run the 32-bit version of PowerShell.
   - On a 32-bit Windows machine, select **Windows PowerShell**.
3. Run the command to set the source of data for the collection script.
   
   ```
   $schtasks = schtasks /query /v /fo:csv
   ```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/query /v</code></td>
<td>Displays additional information about scheduled tasks. Verbose formatting is difficult for automated processing.</td>
</tr>
<tr>
<td>schtasks /query /v /fo:csv</td>
<td>Displays verbose task output and sets the source of data for the collection script to a comma-separated value (csv) result set.</td>
</tr>
<tr>
<td>schtasks /query /?</td>
<td>Displays additional command options.</td>
</tr>
</tbody>
</table>

4. To return the data to the VCM Collector, parse the data into a structure that is compatible with the VCM XML format.

   The sample script parses the data as shown in the following code.

   ```
   ##########################################################################
   ###
   # This inspection script can be used to retrieve scheduled tasks information
   # for tasks created through the Scheduler UI or through the AT command.
   #
   ##########################################################################
   ```

   ```
   ##########################################################################
   ###
   #
   # This inspection script can be used to retrieve scheduled tasks information
   # for tasks created through the Scheduler UI or through the AT command.
   #
   ##########################################################################
   ```
function ToCMBase64String([string]$input_string)
{
    return [string]("cmbase4-" + [System.Convert]::ToBase64String
([System.Text.Encoding]::UNICODE.GetBytes
($input_string))).replace("=","-"
)
}

#################################################################
###
[string]$cihash | out-null
#create a hashtable to check for duplicate rows
$hasharray = @{}
$clTasks = "<Scheduled_Tasks>"
$schtasks = schtasks /query /v /fo:csv
if ($schtasks.count -gt 1)
{
    #depending on OS, the first row may be blank
    #use $k to determine whether to start at the first or second row
    if ($schtasks[0] -eq "")
    {
        $k = 1
    }
    else
    {
        $k = 0
    }
    $cols = $schtasks[$k].substring(1,$schtasks[$k].length-2).replace
("","",$split).split($split)
    #find the HostName and TaskName columns
    $hostcol = -1
    $namecol = -1
    $j = 0
    while (($j -lt $cols.count) -and (($hostcol -eq -1) -or ($namecol -eq -1)))
    {
        if ((([string]$cols[$j]).toupper() -eq "HOSTNAME")

{
$hostcol = $j++
}
else
{
    if (((string)$cols[$j]).toupper() -eq "TASKNAME")
    {
        $namecol = $j++
    }
    else
    {
        $j++
    }
}

#save first column name, to check for repeated column rows
$firstcol = $cols[0]

#encode each column name
for ($j=0;$j -lt $cols.count;$j++)
{
    $cols[$j] = (string)(ToCMBase64String($cols[$j]))
}

#loop through each row
#start at $k+1, because the first row may blank, and the first populated row is column names
for ($i=$k+1;$i -lt $schtasks.count;$i++)
{
    #make sure this is a data row
    $row = ([string]($schtasks[$i])).trim()
    if ($row.contains("",""))
    {
        #split the row
        $task = $schtasks[$i].substring(1,$schtasks[$i].length-2).replace("","","",$split).split($split)
        #some operating systems will return columns multiple times in the result set
if ($task[0] -ne $firstcol)
{
    #if we did not find a TaskName column, just tag each row as Task-n
    if ($namecol -gt -1)
    {
        $clTasks += "<" + [string](ToCMBase64String($task[$namecol])) + "">
    }
    else
    {
        $clTasks += ("<Task-" + ([string]($i-1)) + ">")
    }
    for ($j=0;$j -lt $task.count;$j++)
    {
        #skip the hostname field, since we are doing a local inspection
        if (-not($j -eq $hostcol))
        {
            $clTasks += ("<" + $cols[$j] + ">")
            $clTasks += $task[$j]
            $clTasks += ("</" + $cols[$j] + ">")
        }
    }
    #if we did not find a TaskName column, just tag each row as Task-n
    if ($namecol -gt -1)
    {
        $clTasks += "</" + [string](ToCMBase64String($task[$namecol])) + "">
    }
    else
    {
        $clTasks += ("</Task-" + ([string]($i-1)) + ">")
    }
} #end data row that is not columns repeated

} #end data row
$clTasks += "</Scheduled_Tasks>"
write-host $clTasks

5. After you generate your PowerShell script, perform the following steps:
   - Build a collection filter in VCM.
   - Paste the content of your script into the collection filter.
   - Collect data using the script-based collection filter.
     
     To view the collected WCI data in VCM, click Console and select Windows Operating System > Custom Information > List View.

What to do next

Develop your own custom PowerShell script. See "Create Your Own WCI PowerShell Collection Script" on page 113.

Windows Custom Information Change Management

VCM manages Windows Custom Information (WCI) data changes on a per-filter basis on VCM managed Windows machines. When multiple filters return data using the same top-level XML element name, each filter applies unique change detection.

When you use multiple collection filters to collect WCI data, follow these guidelines.

- Create filters that collect data in a parallel manner. See the following examples.
  - Use one filter to collect data from C:\ and another filter to collect data from C:\Windows.
  - Use a separate filter to collect data from C:\Windows with audit information and another filter to collect data from C:\Windows without audit information.
    
    When you use filters in an unparallel way, every time the file system updates to add a new file or remove an existing file, both filters generate "new file" and "deleted file" events, which causes overlap of the data.

- Use one filter to collect data from NetStat.

- Use multiple filters to collect data from the NTFS file system.
  
  For example, use one filter to collect data in C:\, and another filter to collect data in C:\Windows\System. These collections merge under the top-level element NTFSDirectory without overlap, because each filter collects separate parts of the file structure and avoids extra change reporting.

- Do not create filters that overlap collected WCI data. Overlap can occur if you use filters that do not collect data in a parallel manner.

- Do not use multiple filters to collect the same data for NetStat Open Ports.
  
  When the filters return data under the top-level element name and a managed machine starts to listen on port 80, each filter initially reports the data as a newly created value, which causes overlap of the
data reported.

- Do not create two filters to collect data on the File Permission With Audit data type from different parts of a managed machine's file system.

### Collecting Windows Custom Information

To collect Windows Custom Information (WCI) using script-based filters, you create and verify your custom PowerShell scripts, install PowerShell on the VCM managed machines, and use VCM to collect the WCI data.

#### Procedure

1. "Create Your Own WCI PowerShell Collection Script" on page 113
   Create or modify your Windows Custom Information (WCI) scripts to collect almost any data type that is accessible from VCM managed Windows machines. To return data in a VCM compatible, element-normal XML format, you create your own PowerShell script or obtain PowerShell scripts from VMware Professional Services or another source and modify them for your own collections.

2. "Verify that Your Custom PowerShell Script is Valid" on page 113
   Verify that your PowerShell script adheres to valid XML before you use the script to collect Windows Custom Information (WCI) from VCM managed machines.

3. "Install PowerShell" on page 114
   Verify that PowerShell 2.0 is installed on each VCM managed Windows machine used to collect Windows Custom Information (WCI).

4. "Collect Windows Custom Information Data" on page 115
   Use the Windows Custom Information (WCI) data type to perform user-defined, script-based collections on your VCM managed machines. To collect the custom data, you build a collection filter that includes a script with parameters to run the script and process the results.

5. "View Windows Custom Information Job Status Details" on page 116
   When you run Windows Custom Information (WCI) collection filter scripts, VCM captures detailed information and displays status about exit codes and standard error output for each job that processed the script or filter. You can view the job status details in Job Manager.

6. "Windows Custom Information Collection Results" on page 117
   Examine the results of your Windows Custom Information (WCI) collected data in the VCM tree views and list view.

7. "Run Windows Custom Information Reports" on page 118
   Generate your own reports or run existing reports on Windows Custom Information (WCI) data that you collected using your custom PowerShell scripts.

8. "Troubleshooting Custom PowerShell Scripts" on page 119
   If you encounter problems when you run custom PowerShell scripts, run the script as a .ps1 file and correct any errors before you use the script with a VCM collection filter.
Create Your Own WCI PowerShell Collection Script

Create or modify your Windows Custom Information (WCI) scripts to collect almost any data type that is accessible from VCM managed Windows machines. To return data in a VCM compatible, element-normal XML format, you create your own PowerShell script or obtain PowerShell scripts from VMware Professional Services or another source and modify them for your own collections.

WCI internally stores data in a hierarchy, so your collection script must provide the complete data structure in the standard tree view. The root element in the XML result data set becomes a top-level root element in the WCI data type node. Child elements appear in the same locations in VCM as the locations they populate in the XML document returned by the script.

Prerequisites

- Understand how to write and run PowerShell scripts. See "References on PowerShell and Script Signing" on page 106.
- Plan your data structure to display WCI data in a tree hierarchy based on the data structure specified in the user-defined collection scripts. For an example, see Windows Custom Information Tree View - Standard in the online help.
- Review the guidelines to create PowerShell scripts for WCI collections and understand the challenges. See "Guidelines in PowerShell Scripting for WCI" on page 102.
- Review the example PowerShell script to see a sample script used for a WCI collection. See "Create an Example PowerShell Script for Scheduled Tasks" on page 106.

Procedure

1. On your VCM Collector or managed Windows machine, click Start.
2. Select All Programs > Accessories > Windows PowerShell.
   - On a 64-bit Windows machine, select Windows PowerShell (x86) to run the 32-bit version of PowerShell.
3. Create your PowerShell script and save it to the location of your choice.

What to do next

Verify that your PowerShell script adheres to valid XML before you can use the script to collect WCI data from VCM managed machines. See "Verify that Your Custom PowerShell Script is Valid" on page 113.

Verify that Your Custom PowerShell Script is Valid

Verify that your PowerShell script adheres to valid XML before you use the script to collect Windows Custom Information (WCI) from VCM managed machines.

To verify that your script is valid, run the script in PowerShell.
Procedure

1. On your VCM Collector or managed Windows machine, open a command prompt.
2. Run `powershell.exe` from the command line.
3. Paste your script into the PowerShell window.
   - If your script does not run, press Enter.
4. Make sure that your script runs without errors.
   - Errors appear in red in the PowerShell window.
5. If errors occur, resolve them.
   - A valid script returns a set of XML content without any formatting, white space, carriage returns, or line feeds at the end of elements, nodes, or attributes.

What to do next

Install PowerShell on your VCM managed machines. See "Install PowerShell" on page 114.

Install PowerShell

Verify that PowerShell 2.0 is installed on each VCM managed Windows machine used to collect Windows Custom Information (WCI).

PowerShell 2.0 is supported on all platforms that support PowerShell 1.0.

- PowerShell is installed by default on Windows 2008 R2 and Windows 7 machines.
- You cannot install PowerShell on Windows 2000 or NT4 machines.

Because of its ability to set the execution policy at the process level, PowerShell 2.0 is the base requirement for WCI in VCM. If you run the standard WCI non-inline collection filters against PowerShell 1.0 VCM managed machines, the collection process will fail.

Procedure

1. On your VCM managed machine, check the following registry entry to verify whether PowerShell 2.0 is installed.
   a. **Key Location:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine`
   b. **Value Name:** `PowerShellVersion`
   c. **Value Type:** `REG_SZ`
   d. **Value Data:** `<1.0 | 2.0>`

   If you do not check the registry, the steps to determine if PowerShell 2.0 might differ depending on the platform type of your managed machine.

   If PowerShell is not installed on the target VCM managed machine, the WCI collection returns a Not Executed status. See "View Windows Custom Information Job Status Details" on page 116.

What to do next

Reboot the VCM managed machine after you install or upgrade PowerShell to ensure that collections work properly.
Collect Windows Custom Information Data

Use the Windows Custom Information (WCI) data type to perform user-defined, script-based collections on your VCM managed machines. To collect the custom data, you build a collection filter that includes a script with parameters to run the script and process the results.

When you use the script-based filter in a collection, the VCM Agent calls a script engine to run the script, parse the results to return the collected data to the VCM database, and display the results in the VCM Console. During the collection process, the VCM Agent starts PowerShell, which runs the script and generates the XML result file. The Agent parses the XML result into a format that VCM can use to check for changes and returns the changes to the Collector.

**CAUTION** Do not limit collections to deltas when you select a data type in the Collect wizard. If you limit collections to deltas, VCM purges all existing WCI data from the managed machine's master file and from the VCM database, and replaces the WCI data with newly collected data. You must select the option in the Collect wizard so that VCM does not purge WCI data during collections.

---

**Prerequisites**

See "Prerequisites to Collect Windows Custom Information" on page 100.

**Procedure**

1. On your VCM Collector, click Administration.
2. Select Collection Filters > Filters and click Add Filter.
3. On the Name and Description page, type a name and description for the filter and click Next.
4. On the Data Type page, select Windows.
5. Select the Custom Information (Win) data type and click Next.
6. On the Windows Custom Information Filter page, select the options to add and configure the filter and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Script Type</td>
<td>Set the format of your PowerShell script to <strong>PowerShell v2.0 Text Output</strong>.</td>
</tr>
<tr>
<td>Output Type</td>
<td>Set the resulting output for your PowerShell script to <strong>Element Normal XML</strong>.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Retain the default setting of 300 seconds to specify the amount of time the Agent allows a PowerShell script to run before it attempts to end the process. If the script takes more than 300 seconds to run on the VCM managed machine, increase the setting to 900.</td>
</tr>
<tr>
<td>Script</td>
<td>Paste the content of your PowerShell script into the Script text pane. Your script contains statements that are specific to the data type to collect.</td>
</tr>
<tr>
<td>Duplicate Handling</td>
<td>Set the method to handle duplicates to <strong>Increment</strong> to resolve duplicate violations of duplicate path attributes in the PowerShell script.</td>
</tr>
</tbody>
</table>

7. On the Important page, review the summary information and click Finish.

**What to do next**

Run a script-based collection filter to collect WCI data using from VCM managed Windows machines. See "Run the Script-Based Collection Filter” on page 116.
Run the Script-Based Collection Filter

Use a collection filter and your PowerShell script to collect Windows Custom Information (WCI) from VCM managed Windows machines.

Procedure

1. On your VCM Collector, click Collect.
2. On the Collection Type page, select Machine Data and click OK.
3. On the Machines page, select the managed machines from which to collect WCI data and click Next.
4. Click Select Data types to collect from these machines and click Next.
   - VCM runs a default collection filter for the data type you select.
5. Select Do not limit collection to deltas and click Next.
   - VCM does not purge WCI data during the collection.
7. Click Select data filters and click Next.
8. On the Filters page, select your WCI filter.
9. Click the arrow to move your filter to the selection area and click Next.
10. (Optional) On the Important page, select View Selected Filter Details to see details about your collection filter.
11. Click Close and click Finish.

What to do next

- To confirm that the job finished running, click Administration and select Job Manager > History > Other Jobs > Past 24 Hours.
- View the detailed status about exit codes and standard error output for each job that processed the script or filter. See "View Windows Custom Information Job Status Details" on page 116.

View Windows Custom Information Job Status Details

When you run Windows Custom Information (WCI) collection filter scripts, VCM captures detailed information and displays status about exit codes and standard error output for each job that processed the script or filter. You can view the job status details in Job Manager.

The following procedure displays data for an instant collection performed in the last 24 hours.

Prerequisites

- Verify that all prerequisite components exist on the VCM managed machine. If a prerequisite component such as PowerShell is not installed or available on the managed machine, the script cannot run and a status of Not Executed appears in the Status column. Because optional components such as PowerShell or other script engines might not be supported for installation on all VCM-supported OS versions, a Not Executed status does not result in a failure.
- Collect Windows Custom Information. See "Collect Windows Custom Information Data" on page 115.
Procedure

1. On your VCM Collector, click Administration.
2. Select Job Manager > History > Instant Collections > Past 24 Hours.
3. In the Instant Collections pane, select a collection job that includes WCI data.
4. In the Job History Machine Detail pane, select View Details.
   A single row appears for each WCI filter that ran in the collection job. Information about the WCI script and the script results parsing appears in the row.
5. In the View Details by Machine window, select the managed machines to view and click OK.
   Detailed job history results appear for the WCI filters and managed machines.
   - If a WCI collection job encounters errors on a VCM managed machine, VCM reports detailed information about the failure. Failures can occur when PowerShell starts, during script execution, or when interpreting the script results.
   - If PowerShell is not installed on the managed machine, an error can occur in the PowerShell startup process. Because PowerShell is an optional component, a status of Not Executed can appear in the job details to indicate the skipped steps. The Not Executed status does not appear as an error in the VCM job.
   - If a PowerShell script generates errors due to defects in the script, such as syntactical or typographical errors, VCM reports the status as finished with errors in the collection job.

What to do next

- Review the WCI collection results. See "Windows Custom Information Collection Results" on page 117.
- Generate your own reports. See "Run Windows Custom Information Reports" on page 118.

Windows Custom Information Collection Results

Examine the results of your Windows Custom Information (WCI) collected data in the VCM tree views and list view.

Prerequisites

Collect WCI data and confirm that the WCI collection job finished. Click Administration and select Job Manager > History > Other Jobs > Past 24 Hours. See "Collect Windows Custom Information Data" on page 115.
**Procedure**

1. On your VCM Collector, click **Console**.
2. Select **Windows > Operating System > Custom Information**.
3. Select a view of the collected WCI data.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tree View - Standard</td>
<td>Tree hierarchy view based on the data structure in your PowerShell script.</td>
</tr>
<tr>
<td>Tree View - Consolidated</td>
<td>Tree hierarchy that displays data across multiple elements simultaneously</td>
</tr>
<tr>
<td></td>
<td>with the data consolidated from one level of the tree. The child node</td>
</tr>
<tr>
<td></td>
<td>properties and values appear in each node.</td>
</tr>
<tr>
<td>List View</td>
<td>Data organized by a list of top-level elements. You can filter, sort,</td>
</tr>
<tr>
<td></td>
<td>or group the data.</td>
</tr>
</tbody>
</table>

**What to do next**

Generate your own reports. See "Run Windows Custom Information Reports" on page 118.

**Run Windows Custom Information Reports**

Generate your own reports or run existing reports on Windows Custom Information (WCI) data that you collected using your custom PowerShell scripts.

**Prerequisites**

Collect WCI data. See "Collect Windows Custom Information Data" on page 115.

**Procedure**

1. On your VCM Collector, click **Reports**.
2. Select **Machine Group Reports > Windows > Custom Information**.
3. Select a custom information report.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netstat Open Ports</td>
<td>Reports port and protocol information from the netstat -A command.</td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>SQL SMO Database</td>
<td>Reports the database details collected.</td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>SQL SMO Instance</td>
<td>Reports basic information about the SQL Server instances collected.</td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **Run**.

The report displays information about the collected WCI data. For example, the NetStat Open Ports Information report displays the protocol, port, remote port, local address, foreign address, port state, and the collection filter used in the collection.
Troubleshooting Custom PowerShell Scripts

If you encounter problems when you run custom PowerShell scripts, run the script as a .ps1 file and correct any errors before you use the script with a VCM collection filter.

Prerequisites

- Verify that your script runs in PowerShell. See "Verify that Your Custom PowerShell Script is Valid" on page 113.

Procedure

1. On your VCM Collector, save the script to a file that has the .ps1 extension.
2. Run the script file from a command line using PowerShell 2.0 or PowerShell 1.0.
   - For PowerShell 2.0, run:
     ```
     PowerShell -command set-executionpolicy RemoteSigned -scope Process ;
     scriptname.ps1 > resultfile.xml
     ```
   - For PowerShell 1.0, set the execution policy to Remote Signed or use a less restrictive policy, and run:
     ```
     PowerShell -file scriptname.ps1 > resultfile.xml
     ```
     When the script is finished running, it generates the XML file.
3. Verify that you can open the XML file in Internet Explorer.
   - If you cannot see the entire file, allow blocked content.
   - If Internet Explorer cannot parse the XML file, you must correct any formatting errors.
     If you have Visual Studio installed, you can use it to locate formatting errors in large XML files.

What to do next

- Re-run your custom PowerShell script to verify that it runs correctly. See "Collect Windows Custom Information Data" on page 115.
- View the detailed status about exit codes and standard error output for each job that processed the script or filter. See "View Windows Custom Information Job Status Details" on page 116.
- After the Windows Custom Information data is available in the VCM database, you can generate reports and enforce compliance. See the online help.
You configure your virtual and physical Linux and UNIX machines in VCM so that you can manage them to ensure functionality and compliance with standards.

This chapter includes the following topics:

- Configure Linux and UNIX Machines 121
- Upgrade Requirements for UNIX/Linux Machines 122
- Add UNIX/Linux Machines 122
- License UNIX/Linux Machines 123
- Install the Agent on UNIX/Linux Machines 124
- Collect UNIX/Linux Data 131
- UNIX/Linux Collection Results 132
- Configuring Oracle Instances 133

**Configure Linux and UNIX Machines**

To collect UNIX/Linux data and to manage your physical or virtual UNIX/Linux machines, you must add the machines, license them for use, and install the appropriate VCM Agent.

**Prerequisites**

Review the upgrade requirements to determine if the machines on which you are installing the current Agent are supported platforms and machine type. See "Upgrade Requirements for UNIX/Linux Machines" on page 122.

**Procedure**

1. "Add UNIX/Linux Machines" on page 122
    
    Add UNIX/Linux machines to the Available Machines list to make the machines available for licensing.

2. "License UNIX/Linux Machines" on page 123
    
    License UNIX/Linux machines before you install the Agent and begin to manage them. You license the machines displayed in the Available Machines list.

3. "Install the Agent on UNIX/Linux Machines" on page 124
    
    Install the appropriate version of the VCM Agent on each of your licensed target machines to enable
communication between the Collector and the managed UNIX/Linux machines.

4. “Collect UNIX/Linux Data” on page 131

When the UNIX/Linux machines are licensed and the Agent is installed, you collect data from those machines.

Continuous machine management is based on the latest data you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data. See "UNIX/Linux Collection Results" on page 132.

Upgrade Requirements for UNIX/Linux Machines

To use new VCM functionality, you must upgrade the VCM Agent on target machines based on machine type. You must consider several requirements if you are upgrading from a previous Agent version to the current version on your managed UNIX and Linux machines.

When you upgrade the UNIX Agent on Red Hat machines, be aware of the licensing changes between VCM versions. In VCM 5.6, physical and virtual machines are licensed as servers or workstations.

For general UNIX and Linux machine requirements, see the VCM Installation Guide.

Add UNIX/Linux Machines

Add UNIX/Linux machines to the Available Machines list to make the machines available for licensing.

If you add a large number of machines, you can use other methods to add the machines. See the online help for procedures to import machine information from a file or use IP Discovery.

---

**NOTE** You can use the Discovered Machines Import Tool (DMIT), which imports machines discovered by the Network Mapper (Nmap), to import many physical and virtual machines at one time into the VCM database. Download DMIT from the VMware Web site.

---

**Prerequisites**

Verify that you know the name or IP address, domain, domain type, machine type, and the communication port for the machines to add.

**Procedure**

1. Click **Administration**.
2. Select **Machines Manager** > **Available Machines**.
3. Click **Add Machines**.
4. On the Add Machines page, select **Basic** and click **Next**.
5. On the Manually Add Machines - Basic page, add the machine information.
a. Configure machine information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine</td>
<td>Type the name of the machine. You can use NetBIOS or Fully-Qualified Domain Name (FQDN) notation for the name. If your Collector cannot resolve a host name with a DNS Server, use an IP address rather than a machine name.</td>
</tr>
<tr>
<td>Domain Type</td>
<td>Type or select the domain to which the machine belongs.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the domain type.</td>
</tr>
<tr>
<td>Machine Type</td>
<td>Select the machine type.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port number. The default value is 26542 when you select a UNIX/Linux or Mac OS X machine type. The port number must be the same number used when you install the Agent on the managed UNIX/Linux machine.</td>
</tr>
</tbody>
</table>

b. Click Add.

c. To add other machines, configure the machine information and click Add.

d. After you add the target machines, click Next.

6. On the Important page, review the machine information and click Finish. The machine is added to the Available Machines data grid.

What to do next
License the machine. See "License UNIX/Linux Machines" on page 123.

License UNIX/Linux Machines
License UNIX/Linux machines before you install the Agent and begin to manage them. You license the machines displayed in the Available Machines list.

Prerequisites
- Verify that you added the UNIX/Linux machines. See "Add UNIX/Linux Machines" on page 122.
- Determine if your managed Red Hat workstations and servers are affected by an upgrade from a previous version of VCM. See "Upgrade Requirements for UNIX/Linux Machines" on page 122.
- Verify that the machines you are licensing have a specified Machine Type. Machines without a Machine Type value will not be licensed.

Procedure
1. Click Administration.
2. Select Machines Manager > Available Machines.
3. Select the machines and click License.
4. On the Machines page, verify that the Selected list includes the machines to license and click Next.
5. On the Product License Details page, review the licensed machine count and click Next.
6. On the Important page, click Finish.

What to do next
Install the Agent on the target machines. See "Install the Agent on UNIX/Linux Machines" on page 124.

Install the Agent on UNIX/Linux Machines

Install the appropriate version of the VCM Agent on each of your licensed target machines to enable communication between the Collector and the managed UNIX/Linux machines.

Installing the Agent on UNIX/Linux machines is a manual operation. You can run the installation process in silent mode or interactive mode. To run the installation in silent mode, you must edit the configuration options in the csi.config file. The file is edited to accommodate different target machine types.

A Deployment Utility is available in C:\Program Files (x86)\VMware\VCM\Tools to assist you with your UNIX/Linux configuration for selected steps. See the utility’s online help for more information.

```
IMPORTANT Ensure that you install the Agent on newly managed machines rather than upgrading currently managed machines. If you are upgrading, see "Upgrade Requirements for UNIX/Linux Machines" on page 122.
```

Prerequisites

- Verify that the machine on which you intend to install the Agent has enough free disk space. For more information, see the VCM Installation Guide.
- If you run an installation in silent mode, modify the appropriate csi.config file variable options. See "Installation Options for Linux or UNIX csi.config" on page 128.
- If you select (x) inetd/launchd for CSI_AGENT_RUN_OPTION, verify that (x) inetd/launchd is running on the target machines. On some versions, when (x) inetd/launchd services are not configured, (x) inetd/launchd will not stay running. To ensure the Agent installation finishes successfully, pass a - stayalive option to (x) inetd/launchd. See "Installation Options for Linux or UNIX csi.config" on page 128.
- Log in to the target UNIX/Linux machine as root.
- Disable or reconfigure firewalls on SUSE and Red Hat machines to install the Agent.
- Select the method that you want to use to copy files to the target machines. You can use ftp, sftp, or cp using an NFS share. If you use ftp to copy the package to your machine, you must use binary mode.
- If you are collecting non-ASCII information from the target machines, install a UTF-8 locale. To determine the locales installed on your operating system, use the locale -a command.
Procedure

1. Copy the appropriate Agent binary installation package from the Collector to the machine on which you will install the Agent.

   The Agent packages are located on the Collector in `\Program Files (x86) \VMware\VCM\Installer\Packages`.

<table>
<thead>
<tr>
<th>Operating System Version</th>
<th>Agent Binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat (Enterprise) Linux Edition (Version 3.0, 4.0, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 6, 6.1, 6.2)</td>
<td>CMAgent.&lt;version&gt;.Linux</td>
</tr>
<tr>
<td>Red Hat 3.0 requires the CMAgent.5.4.0.Linux Agent.</td>
<td></td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (9, 10.0–10.4, 11.0–11.1)</td>
<td></td>
</tr>
<tr>
<td>Debian (4). SUSE 9 requires the CMAgent.5.4.0.Linux Agent.</td>
<td></td>
</tr>
<tr>
<td>Solaris (Versions 9 and 10 supported on Sparc)</td>
<td>CMAgent.&lt;version&gt;.SunOS</td>
</tr>
<tr>
<td>Solaris (Version 10 for x86)</td>
<td>CMAgent.&lt;version&gt;.SunOS.x86.5.10</td>
</tr>
<tr>
<td>HP-UX 11i Versions 1.0, 2.0, 3.0 (11.11, 11.23, and 11.31; Supported on PA-RISC)</td>
<td>CMAgent.&lt;version&gt;.HP-UX.11.pa</td>
</tr>
<tr>
<td>HP-UX 11i Version 2.0, 3.0 (11.23 and 11.31- Supported on Itanium)</td>
<td>CMAgent.&lt;version&gt;.HPUX.11.ia64</td>
</tr>
<tr>
<td>AIX Version 5L (5.3, 6L (6.1), 7.1)</td>
<td>CMAgent.&lt;version&gt;.AIX.5</td>
</tr>
</tbody>
</table>

2. On the target machine, run `chmod u+x <filename>` to set the execute permission for the file owner on the Agent binary file.

3. In the directory to which you copied the file, run `./CMAgent.<version>..<Agent binary name>` to create the necessary directory structure and extract the files.

To force an overwrite of any existing files, include the `-o` option. For example:

`./CMAgent.<version>..SunOS -o`

The command and output is similar to the following example, but with different file names depending on the operating system.

```
# ./CMAgent.<version>..SunOS
creating: CSIIInstall/
creating: CSIIInstall/packages/
inflating: CSIIInstall/packages/Agent.1.0.SunOS
inflating: CSIIInstall/packages/CFC.1.0.SunOS
inflating: CSIIInstall/packages/ECMU.1.0.SunOS
inflating: CSIIInstall/packages/ThirdParty.1.0.SunOS
inflating: CSIIInstall/packages/cis.1.0.SunOS
extracting: CSIIInstall/packages/package.sizes.SunOS
inflating: CSIIInstall/packages/python.23.SunOS
creating: CSIIInstall/scripts/
inflating: CSIIInstall/scripts/checksum
inflating: CSIIInstall/scripts/BootStrapInstall.sh
inflating: CSIIInstall/scripts/AltSource_filesystem.sh
```
inflating: CSIInstall/scripts/AltSource_ftp.sh
inflating: CSIInstall/scripts/AltSource_rcp.sh
inflating: CSIInstall/scripts/AltSource_sftp.sh
inflating: CSIInstall/scripts/AltSource_wget.sh

extracting: CSIInstall/scripts/AltSourceCmd
inflating: CSIInstall/InstallCMAgent
inflating: CSIInstall/csi.config
inflating: CSIInstall/CMAgent.<version.OS>
creating: CSIInstall/.security/certificates/
inflating: CSIInstall/.security/certificates/<EnterpriseCertificate>

4. Run `cd <extractedpath>/CSIInstall` to change the directory to the location where the InstallCMAgent executable file was extracted.

5. Run `ls -la` to validate that the correct files are in the `<extractedpath>/CSIInstall` directory.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallCMAgent</td>
<td>Installation script.</td>
</tr>
<tr>
<td>csi.config</td>
<td>Configuration file for the installation. This is the file you can modify to include installation options for silent rather than interactive installation processes.</td>
</tr>
<tr>
<td>packages</td>
<td>Installation packages.</td>
</tr>
<tr>
<td>scripts</td>
<td>Scripts required for the installation.</td>
</tr>
</tbody>
</table>

6. (Optional) Edit the csi.config file to customize the installation variables and save your changes.

   a. Run the `chmod u+x csi.config` command to add write file permissions if the file has only read permissions set.
   
   b. Modify the csi.config file options based on your local requirements and save the file.
   
   c. Copy the modified and saved csi.config file to the extracted location.
   
      For example, `# cp /<safelocation>/csi.config /<extractedlocation>/CSIInstall/csi.config`

7. Run InstallCMAgent in either silent mode or interactive mode.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent mode</td>
<td>Run the <code># ./CSIInstall/InstallCMAgent -s</code> command. Hold down the Option key and press S. Install the Agent using the silent mode if you manually edited the csi.config file, if you modified the csi.config file using the interactive method, or if you are using a custom configuration file that you saved from a previous Agent installation. This mode uses the values specified in csi.config without prompting for input. When the silent installation finishes, a summary of the installation process and status appears. Verify that the installation finished without errors.</td>
</tr>
<tr>
<td>Interactive mode</td>
<td>Run the <code># ./CSIInstall/InstallCMAgent</code></td>
</tr>
<tr>
<td>Option</td>
<td>Action</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>command.</td>
<td>Install the Agent using the interactive mode if you did not modify the csi.config and to respond to each prompt to accept or change each parameter in the csi.config file as it runs. As a result of your responses, the csi.config is modified.</td>
</tr>
<tr>
<td></td>
<td>The preinstallation stage of interactive mode checks for a valid user, CSI_USER. If the user exists, you are not prompted for these configuration values.</td>
</tr>
<tr>
<td></td>
<td>- CSI_USER_NO_LOGIN_SHELL</td>
</tr>
<tr>
<td></td>
<td>- CSI_USER_PRIMARY_GROUP</td>
</tr>
<tr>
<td></td>
<td>- CSI_USER_PRIMARY_GID</td>
</tr>
<tr>
<td></td>
<td>- CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID</td>
</tr>
<tr>
<td></td>
<td>You are prompted for these values only when the CSI_USER user account is not found.</td>
</tr>
<tr>
<td></td>
<td>You can check the installation status in the installation log file. The file is located in <code>&lt;CSI_PARENT_DIRECTORY&gt;/log/install.log</code>.</td>
</tr>
<tr>
<td>8. Run <code>ls -la /CSI_PARENT_DIRECTORY/CMAgent</code> to verify that all the required files and directories were installed.</td>
<td></td>
</tr>
<tr>
<td>/CSI_PARENT_DIRECTORY/CMAgent is the default directory. If you changed the directory name during installation, modify the <code>ls -la</code> command to display the custom directory name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>You can check the installation status in the installation log file. The file is located in <code>&lt;CSI_PARENT_DIRECTORY&gt;/log/install.log</code>.</td>
</tr>
<tr>
<td>9. Run `# netstat -na</td>
<td>grep &lt;port_number&gt;` to verify that the Agent is installed correctly, listening on the assigned port, and ready to collect data.</td>
</tr>
<tr>
<td>The default <code>&lt;port_number&gt;</code> is 26542 for VCM installations.</td>
<td></td>
</tr>
<tr>
<td>10. If you are installing on SUSE, start xinetd using the <code>#/etc/init.d/xinetd start</code> command after the installation completes.</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

Run a collection for UNIX/Linux data. See "Collect UNIX/Linux Data on page 131."
## Installation Options for Linux or UNIX csi.config

The installation options are variables you add or modify in the `csi.config` file used when you install the Agent. You can create several versions of this file based on operating system or specific settings, but do not change the file name.

<table>
<thead>
<tr>
<th>Installation Options with Default Values</th>
<th>Description</th>
</tr>
</thead>
</table>
| CSI_AGENT_RUN_OPTION                     | You can install the Agent as a daemon process or installed to be run by `inetd/xinetd/launchd`.  
  - A value of inetd installs the Agent for execution by `inetd/xinetd/launchd`.  
  - A value of daemon installs the agent for execution as a daemon process. |
| CSI_NO_LOGIN_SHELL= +S:+A:+/sbin/noshell+/bin/false+/sbin/false+/usr/bin/false+/sbin/nologin | The `CSI_USER` account must not have a login shell. This parameter lists all valid no-login shells and is used to verify the `CSI_USER` has no-login shell.  
  If your system has a valid no login shell that is not listed, you append a plus sign and add the no login shell to the list.  
  The options available for this parameter include:  
  - +S means only for Solaris  
  - +A means only for AIX  
  - +H means only for HP-UX  
  - +L means only for Linux  
  - + means for all operating systems |
| CSI_CREATE_USER=Y                        | Keep the default value. Indicates whether the user will be created.  
  When you install in trusted mode on HP-UX v1.0 (11.11), the user must exist on the target machine. If you attempt to install and create the user, the installation of the Agent fails. |
<p>| CSI_USER_ID=501                          | Keep the default value. Integer value for the user ID of the created user. |
| CSI_USER_NO_LOGIN_SHELL=/bin/false       | Keep the default value. Indicates the no-login shell value to use when you create the user. |
| CSI_USER_PRIMARY_GROUP=csi_acct          | Keep the default value. Group name to use when you create a new user as the user’s primary group. This group is for low security access. Most inspections are executed with the lowest possible privileges using this group while also preventing access by way of this group to the high security group privileges. |
| CSI_CREATE_USER_PRIMARY_GROUP=Y         | Keep the default value. Indicates the need to create a low-security primary group for the <code>CSI_USER</code>. |
| CSI_USER_PRIMARY_GID=501                 | Keep the default value. Create user’s primary Group ID. |
| CSI_USER_USE_NEXT_                       | Keep the default value. Setting this option to Y allows the Group ID... |</p>
<table>
<thead>
<tr>
<th>Installation Options with Default Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVAILABLE_LOCAL_GID=Y</td>
<td>to be the next available local Group ID over CSI_USER_PRIMARY_GID.</td>
</tr>
<tr>
<td>CSI_USER=csi_acct</td>
<td>Keep the default value. The user assigned to the cfgsoft group. The CSI listener process runs under this user.</td>
</tr>
<tr>
<td>CSI_CFGSOFT_GID=500</td>
<td>Keep the default value. The Group ID of the cfgsoft group. This value can change if the GID is already in use. This group is for high-security access. Some inspections require root privileges, which are provided indirectly through this group and setuid to root.</td>
</tr>
<tr>
<td>CSI_CREATE_LOCAL_GROUP=Y</td>
<td>Keep the default value. Setting this option to Y allows the cfgsoft group to be created. This setting allows the system call to groupadd.</td>
</tr>
<tr>
<td>CSI_USE_NEXT_AVAILABLE_LOCAL_GID=Y</td>
<td>Keep the default value. Setting this option to Y allows this Group ID to be the next available local Group ID starting at CSI_CFGSOFT_GID.</td>
</tr>
<tr>
<td>CSI_AGENT_PORT=26542</td>
<td>Keep the default value. Specifies the port on which the Agent listens.</td>
</tr>
<tr>
<td>CSI_CREATE_LOCAL_SERVICE=Y</td>
<td>Keep the default value. Setting CSI_CREATE_LOCAL_SERVICE to Y allows the system to create the local service (copy files to system directories).</td>
</tr>
<tr>
<td>CSI_REFRESH_INETD=Y</td>
<td>Setting this option to Y allows the system to refresh xinetd (Linux) or inetd (Solaris, AIX, and HP-UX). Keep default value only if you are running your agent as inetd. If you are running your agent as a daemon, select CSI_REFRESH_INETD=N</td>
</tr>
<tr>
<td>CSI_NICE=10</td>
<td>Keep the default value. Sets the nice value for the agent listener process.</td>
</tr>
<tr>
<td>CSI_CERTIFICATE_PATH=</td>
<td>Specifies the path to Collector Certificates. The certificates specified at this path are copied to the Agent. If your Collector Certificates are stored in an accessible location on this machine, you use this option to put the certificates in the Agent location. You should install the Enterprise Certificates so that multiple collector instances collecting from the same set of Agents is supported. If this package was copied from a collector installation, this package already contains that Collector’s Enterprise Certificate.</td>
</tr>
<tr>
<td>CSI_PARENT_DIRECTORY=/opt</td>
<td>Specifies the parent directory of the CM Agent. The root directory of CMAgent will be CSI_PARENT_DIRECTORY/CMAgent.</td>
</tr>
<tr>
<td>CSI_PARENT_DATA_DIR=/opt</td>
<td>Specifies the parent directory of the CMAgent data directory. The data directory will be CSI_PARENT_DATA_DIRECTORY/CMAgent/data.</td>
</tr>
<tr>
<td>CSI_PARENT_LOG_DIR=default</td>
<td>Specifies where agent operational log files are kept. The log directory is CSI_PARENT_LOG_DIR/CMAgent/log. The default value indicates to use these values.</td>
</tr>
<tr>
<td>Installation Options with Default Values</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Linux:</strong> /var/log</td>
<td></td>
</tr>
<tr>
<td><strong>AIX, HP-UX, and Solaris:</strong> /var/adm</td>
<td></td>
</tr>
</tbody>
</table>

**CSI_KEEP_CSIINSTALL=N**

Recommend keeping the default value. After a successful installation, the temp installation directory CSIInstall is deleted. To keep this installation directory, set this parameter to Y.

**CSI_LOCALE=**

Keep the locale configuration option unspecified in the csi.config file when installing the Agent.

If you configure the value, it supersedes the data encoding locale on the target operating system. The locale, which should be a UTF-8 locale, affects the internal data conversions on non-ASCII data performed by VCM, but the setting does not affect how the collected data is displayed in VCM. This configuration value is used to resolve any problems with data conversions after you install the Agent.

If this value is left blank, the Agent installation scripts attempt to find an appropriate value for the CSIRegistry base on the following rules presented in order of precedence.

1. The optional CSI_LOCALE value set is in the csi.config file.
   
   By default, the entry is blank in the csi.config file package in the Agent. If this value is set, the Agent installation script uses the provided value. During the installation of the Agent, the value is checked against the operating system to ensure that it is a valid value. If the value is not valid, it is still used and is set as the value in the CSIRegistry, but the process logs and the displays an installation error. The Agent uses what is in the CSIRegistry.

2. The default locale on the target operating system at installation time is [some locale value].utf8. For example, en_US.UTF-8.

   The value is added to the CSIRegistry.

3. The default locale on the target operating system is not UTF-8, but has a UTF-8 locale installed. For example, if the default locale is en_US.UTF8-15 and en_US.UTF-8 is installed on the system, en_US.UTF-8 is used.

   The UTF-8 locale is added to the CSIRegistry.

4. No default locales are specified on the target operating system.

   The Agent installation script runs the locale -a command and adds the first installed UTF-8 locale that it finds to the CSIRegistry.

5. The operating system is not configured for any internationalization.

   C, which is the locale that is used to specify plain ASCII, is
<table>
<thead>
<tr>
<th>Installation Options with Default Values</th>
<th>Description</th>
</tr>
</thead>
</table>
| added to the CSIRegistry, but the process logs and displays an i18n warning.  
If you interactively install the Agent, the Agent installation scripts use the previous precedence rules to evaluate and generate a default value that is displayed during the installation of the Agent.  
If you select a non-UTF-8 locale, the Agent installation uses the locale, but the process logs and displays a warning. If you select a locale that does not exist on the operating system, the Agent installation uses the locale, but the process logs and displays an error. |

Manually Uninstall the UNIX/Linux Agent

When you install the Agent, an uninstall file, UninstallCMAgent, is created in <path>/CMAgent/uninstall. You use the file to manually uninstall the Agent from the managed machine.

The uninstall reverses all changes made by installation. However, the installation log files are retained in <AgentRoot>/install.<AgentRoot> defaults to the CMAgent directory that was created during installation.

Prerequisite

To save a copy of the configuration file to use on other machines, copy csi.config to a secure location. The file is located in <path>/CMAgent/install.

Procedure

1. Navigate up one level from the uninstall directory in the CMAgent directory.
2. Run the # ./uninstall/UninstallCMAgent command to uninstall the Agent.

What to do next

After you run UninstallCMAgent, delete the remaining the CMAgent directory before you install a new Agent.

Collect UNIX/Linux Data

When the UNIX/Linux machines are licensed and the Agent is installed, you collect data from those machines.

Collecting data from machines adds the collected machine information to the VCM database and makes the machine data available for reporting, running compliance, and other management options. The collection process for UNIX/Linux collection is similar to other collections, including Windows, except that you select UNIX data types during the collection instead of Windows data types.

Prerequisites

- License the target machines. See “License UNIX/Linux Machines” on page 123.
- Install the Agent on the target machines. See “Install the Agent on UNIX/Linux Machines” on page 124.
Procedure

1. Click Collect.
2. On the Collection Type page, select Machine Data and click OK.
3. On the Machines page, select the machines from which you are collecting data and click Next.
4. On the Data Types page, configure the collection and click Next.
   a. Select the Select All check box.
   b. Select Use default filters.
5. On the Important page, verify that there are no conflicts with previously scheduled or running jobs, and click Finish.
   The amount of time the first collection requires is determined by the number of machines and network connectivity.
6. Click Administration and select Job Manager > History > Instant Collections > Past 24 Hours to determine if the collection finished.

What to do next

- Review your collected data. See “UNIX/Linux Collection Results” on page 132.

Updates to UNIX Patch Assessment Content Affects UNIX Agent Performance

By default, VCM Patching checks for patch updates every 4 hours. The time required to perform this action depends on the amount of new content downloaded to the Collector during the update process.

When the UNIX patch assessment content is pushed out to the UNIX Agents, the time required to run jobs such as collections and remote commands increases slightly. The time required varies based on how much new or updated content must be synchronized between the Collector and the Agent. This content push occurs when the first communication is initiated after installing the UNIX Agent package or when the Collector has platform-applicable patch content that was added after the last communication between the Agent and the Collector.

UNIX/Linux Collection Results

UNIX/Linux data is displayed in VCM and is available for several management actions.

The displayed data is only as current as the last time you collected the data.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Displays dashboards and summary reports based on collected data. You use the Console to view data relevant to day-to-day operations, troubleshooting, and analysis. To view the dashboards, click Console and select Dashboards &gt; UNIX. To view the summary reports, click Console and select UNIX tab &gt; Operating System &gt; Machines &gt; General. You can view the data in a summary report or data grid format.</td>
</tr>
<tr>
<td>Reports</td>
<td>Runs preconfigured VCM reports or create custom reports. Reports are run against currently collected data. Depending on the volume or complexity of the data requested in a report, it may take time to generate the report. Refer to the online help for information about scheduling and disseminating reports. To use the reporting options, click Reports and select Machine Group Reports &gt; UNIX.</td>
</tr>
</tbody>
</table>
### Configuring Oracle Instances

To manage your Oracle instances, you must discover or add the instances, modify the configuration values, and collect management view data from the instances.

An Oracle instance consists of shared memory structures and background processes that run the Oracle database. When you use VCM to collect Oracle management view data from multiple instances, you can run compliance and reports to ensure that all your instances are configured as expected.

**Prerequisites**

Add, license, and install the Agent on the Oracle instance host Solaris machines. See "Configure Linux and UNIX Machines" on page 121.

**Procedure**

1. "Discover Oracle Instances" on page 133
   
   To discover Oracle instances, you run a collection on supported UNIX/Linux machines where Oracle is installed. The Oracle instance discovery process is based on data that you collect from the `oratab` file on managed Solaris machines on which Oracle is installed.

2. "Edit Oracle Instances" on page 134
   
   You edit Oracle instance configuration to modify the discovered or added values for Oracle Home, Oracle Software Owner, DBA Group, and Oracle Collection User.

3. "Collect Oracle Data" on page 138
   
   To collect Oracle data, you must collect the Oracle data types from the machines hosting the Oracle instances.

   Continuous Oracle instance management is based on the latest data you collect from target instances. You can view data and run actions, such as reports or compliance, based on the collected data. See "Oracle Collection Results" on page 139.

### Discover Oracle Instances

To discover Oracle instances, you run a collection on supported UNIX/Linux machines where Oracle is installed. The Oracle instance discovery process is based on data that you collect from the `oratab` file on managed Solaris machines on which Oracle is installed.

**Prerequisites**

Add, license, and install the Agent on the Oracle instance host Solaris machines. See "Configure Linux and UNIX Machines" on page 121.
Procedure

1. Click Collect.
2. On the Collection Type page, select Machine Data and click OK.
3. On the Machines page, select the machines hosting the Oracle instances, select Do not limit collection to deltas, and click Next.
4. On the Data Types page, configure the collected data types.
   a. Expand the UNIX data type.
   b. Select Machines - General and Oracle - Management Views.
   c. Select Use default filters and click Next.
5. On the Important page, verify that there are no conflicts with scheduled or running jobs, and click Finish.
   The amount of time the first collection requires is determined by the number of machines and network connectivity.
6. Click Administration and select Job Manager > History > Instant Collections > Past 24 Hours to determine if the collection finished successfully.

What to do next

- Click Administration and select Machines Manager > Additional Components > VCM for Oracle and verify that the discovered configuration information is correct and that it includes an Oracle Collection User. If the information about the instance does not include a valid Oracle Collection User value, see "Edit Oracle Instances" on page 134. If the instance is not included in the data grid, see "Add Oracle Instances" on page 135.
- If VCM discovered your Oracle instances and the Oracle Collection User account is correctly configured, collect data from the target instances. See "Collect Oracle Data" on page 138.

Edit Oracle Instances

You edit Oracle instance configuration to modify the discovered or added values for Oracle Home, Oracle Software Owner, DBA Group, and Oracle Collection User.

To collect from Oracle instances, the target instances must have a configured Oracle Collection User created on the instance.

Prerequisites

- Add, license, and install the Agent on Solaris machines hosting Oracle instances. See "Configure Linux and UNIX Machines" on page 121.
- Collect from the target Solaris machines using the Machines - General and Oracle - Management Views data types. The collection process discovers Oracle instances from the oratab file on Solaris machines. See "Discover Oracle Instances" on page 133.
- Verify that the collected configuration information is correct and that it includes an Oracle Collection User. Select Administration > Machines Manager > Additional Components > VCM for Oracle and review the data grid values. If the instance is not in the data grid, add the instance. See "Add Oracle Instances" on page 135. If the information about the instance does not include a valid Oracle Collection User value, edit the instance to update the configuration information.
Procedure

1. Click Administration.
2. Select Machines Manager > Additional Components > VCM for Oracle.
3. Select the target instances and click Edit.
4. On the Select Machines page, verify that the target Oracle instance machines are in the selected machines list and click Next.
5. On the Configuration Values page, configure the missing or incorrect values.
   a. Type the configuration values.
   
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Home</td>
<td>File path to the location of the Oracle software for the Oracle instance (user-defined).</td>
</tr>
<tr>
<td>Oracle SW Owner</td>
<td>User account that owns the Oracle software for the Oracle instance (user-defined).</td>
</tr>
<tr>
<td>DBA Group</td>
<td>Database administrator group account for the Oracle instance.</td>
</tr>
<tr>
<td>Oracle Collection User</td>
<td>User account that VCM uses to collect from the Oracle instance.</td>
</tr>
</tbody>
</table>
   
   b. To create the OS-authenticated Oracle collection user on the target Oracle instances, select Configure Oracle Collection User for the Added Instance.
      If you do not select this option, you must create the Oracle Collection User using either the Config User action or the Install Oracle Collection Account remote command. See the online help.
   c. Click Next.
6. On the Important page, click Finish.
7. If you selected the Configure Oracle Collection User for the Added Instance option, on the Select Oracle instances page, add the target machines to the selected list and click Next.
8. On the Schedule page, select Run Action now and click Next.

What to do next

- If your target Oracle instance is Oracle 10g, you must set user permissions. See "Grant Permissions for the Oracle Collection User Account on Oracle 10g" on page 137.
- To begin managing your Oracle instances, you must collect data from the target instances. See "Collect Oracle Data" on page 138.

Add Oracle Instances

Adding Oracle instances identifies host Solaris machines and provides the Oracle SID, Oracle Home, Oracle Software Owner, DBA Group, and Oracle Collection User for the added instances.

You add Oracle instances if the collection of the Oracle instances from the host machines does not retrieve Oracle Home, Oracle SID and Oracle Software Owner from the oratab file on host machines.
Prerequisites

- Add, license, and install the Agent on Solaris machines hosting Oracle instances. See "Configure Linux and UNIX Machines" on page 121.
- Collect from the target Solaris machines using the following data types.
  
  Machines - General
  Oracle - Management Views

  The collection process discovers Oracle instances from the `oratab` file on Solaris machines. See "Discover Oracle Instances" on page 133.

Procedure

1. Click Administration.
2. Select Machines Manager > Additional Components > VCM for Oracle.
3. Click Add.
4. On the Select Machines page, add the target Oracle instance machines to the selected machines list and click Next.
5. On the Configuration Values page, add instances.
   a. Type the configuration values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle SID</td>
<td>(Add only) Name or system ID of the Oracle instance, used to identify a particular database on a machine. Each database on a machine must have a unique SID.</td>
</tr>
<tr>
<td>Oracle Home</td>
<td>File path to the location of the Oracle software for the Oracle instance (user-defined).</td>
</tr>
<tr>
<td>Oracle SW Owner</td>
<td>User account that owns the Oracle software for the Oracle instance (user-defined).</td>
</tr>
<tr>
<td>DBA Group</td>
<td>Database administrator group account for the Oracle instance.</td>
</tr>
<tr>
<td>Oracle Collection User</td>
<td>User account that VCM uses to collect from the Oracle instance.</td>
</tr>
</tbody>
</table>

   b. Select Configure Oracle Collection User for the Added Instance to create the OS-authenticated Oracle collection user on the target Oracle instances.
      
      If you do not select this option, you must create the Oracle Collection User using either the Config User action or the Install Oracle Collection Account remote command. See the online help.
   c. Click Add.
   d. Continue adding configurations to apply to the selected machines or click Next.
6. On the Important page, click Finish.
7. If you selected the Configure Oracle Collection User for the Added Instance option, on the Select Oracle instances page, add the target machines to the selected list and click Next.
8. On the Schedule page, select Run Action now and click Next.
What to do next

- If your target Oracle instance is Oracle 10g, set user permissions. See "Grant Permissions for the Oracle Collection User Account on Oracle 10g" on page 137.
- To begin managing your Oracle instances, collect data from the target instances. See "Collect Oracle Data" on page 138.

Create the Oracle Collection User Account with the Config User Action

You can create an OS-authenticated Oracle collection user account on target Oracle instances from VCM. This action allows you to manage the collection user account from VCM rather than managing the account in each Oracle instance. VCM must have the appropriate Oracle database access to collect data from Oracle instances. VCM uses the Oracle Collection User account to connect to the Oracle database and collect Oracle data.

Prerequisites

Verify that the Oracle instance is added to VCM. See "Add Oracle Instances" on page 135.

Procedure

1. Click Administration.
2. Select Machines Manager > Additional Components > VCM for Oracle.
3. Click Config User.
4. On the Select Machines page, add the target Oracle instances to the selected instances list and click Next.
5. On the Schedule page, select Run Action now and click Next.
6. On the Important page, click Finish

What to do next

If your target Oracle instance is Oracle 10g, you must set user permissions. See "Grant Permissions for the Oracle Collection User Account on Oracle 10g" on page 137.

Grant Permissions for the Oracle Collection User Account on Oracle 10g

For Oracle 10g installations, you must give the Oracle Collection User accounts read/execute permission to the required directories and files in Oracle Home.

By default, Oracle 10g has the permissions set to prevent users who are not part of the Oracle DBA Group from accessing and running files in the Oracle Home directory. Oracle Collection User accounts do not typically belong to the Oracle DBA Group and must be granted permissions on the required files.

Prerequisites

Verify that you added VCM-created Oracle Collection User accounts to Oracle instances. See "Create the Oracle Collection User Account with the Config User Action" on page 137.
Procedure

1. On the Oracle instance, run `chmod o+rx <top level oracle install>` to grant permission for the Oracle Collection User on the required Oracle directories.
   
   For example, `/opt/oracle`, `/oracle`, and so on.

2. Run `chmod o+rx <top level oracle install>` for every directory level from the top level install down to `$ORACLE_HOME`.
   
   For example, if the top level is `/oracle` and `$ORACLE_HOME` is `/oracle/app/product/10.20.0/db_1`, then these are the required files.
   ```bash
   chmod o+rx /oracle/app
   chmod o+rx /oracle/app/product
   chmod o+rx /oracle/app/product/10.20.0
   chmod o+rx /oracle/app/product/10.20.0/db_1
   ```

3. Verify that the `$ORACLE_HOME` environment variable is set, and update the mode for these files.
   ```bash
   chmod o+rx $ORACLE_HOME
   chmod o+rx $ORACLE_HOME/jdbc
   chmod o+rx $ORACLE_HOME/jdbc/lib
   chmod o+rx $ORACLE_HOME/ldap
   chmod o+rx $ORACLE_HOME/ldap/mesg
   chmod o+r $ORACLE_HOME/ldap/mesg/*
   chmod o+rx $ORACLE_HOME/network
   chmod o+rx $ORACLE_HOME/network/admin
   chmod o+rx $ORACLE_HOME/sqlplus
   chmod o+rx $ORACLE_HOME/sqlplus/mesg
   chmod o+r $ORACLE_HOME/sqlplus/mesg/spplus.msb
   chmod o+r $ORACLE_HOME/sqlplus/mesg/sp2us.msb
   chmod o+rx $ORACLE_HOME/nls
   chmod o+rx $ORACLE_HOME/nls/data
   chmod o+r $ORACLE_HOME/nls/data/lxlboot.nlb
   chmod o+r $ORACLE_HOME/nls/data/*/nls/data/
   chmod o+rx $ORACLE_HOME/oracore
   chmod o+rx $ORACLE_HOME/oracore/zoneinfo
   chmod o+r $ORACLE_HOME/oracore/zoneinfo/timezlr.dat
   ```

Collect Oracle Data

To collect Oracle data, you must collect the Oracle data types from the machines hosting the Oracle instances.
Prerequisites
Verify that the Oracle instances are added to VCM and correctly configured. See "Edit Oracle Instances" on page 134.

Procedure
1. On the toolbar, click Collect.
2. On the Collection Type page, select Machine Data and click OK.
3. On the Machines page, select the Solaris machines hosting the Oracle instances.
4. Select Do not limit collection to deltas and click Next.
5. On the Data Types page, configure the collected data type.
   a. Expand the UNIX data type.
   b. Select Oracle - Management Views.
   c. Select Use default filters.
   d. Click Next.
6. On the Important page, verify that there are no conflicts with previously scheduled or running jobs, and click Finish.

   The amount of time the first collection requires is determined by the number of machines and network connectivity.

   What to do next
   • Select Administration > Job Manager > History > Instant Collections > Past 24 Hours to determine if the collection finished successfully.
   • Review collected data and manage your Oracle instances. See "Oracle Collection Results" on page 139.

Oracle Collection Results
You use the collected Oracle data to manage your Oracle instances. The data is available for several management actions.

The displayed data is only as current as the last time that you collected the data.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Displays security information for users, roles, privileges, configuration settings, and database parameters for Oracle instances. The data in these views is collected from views in each Oracle instance on supported Solaris machines. To view the collected data, click Console and select Enterprise Applications &gt; Oracle &gt; Management Views.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Determines if the collected data from target machines meets specified compliance values. To run compliance checks, click Compliance and select Machine Group Compliance and follow the steps described in the online help to create rule groups, rules, filters, and templates.</td>
</tr>
<tr>
<td>Reports</td>
<td>Creates custom Oracle reports based on collected Oracle management views data. Reports are run against currently collected data.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Depending on the volume or complexity of the data requested in a report, it might take time to generate the report. See the online help for information about scheduling and disseminating reports. To create Oracle reports, click Reports and select Machine Group Reports.</td>
</tr>
</tbody>
</table>
Configuring Mac OS X Machines

You configure your virtual and physical Mac OS X machines in VCM so that you can manage them to ensure functionality and compliance with standards.

This chapter includes the following topics:

- Configure Mac OS X Machines 141
- Add Mac OS X Machines 142
- License Mac OS X Machines 143
- Install the Agent on Mac OS X Machines 143
- Collect Mac OS X Data 149
- Mac OS X Collection Results 151

Configure Mac OS X Machines

To collect Mac OS X data and to manage your physical or virtual Mac OS X machines, you must add the machines, license them for use, and install the appropriate VCM Agent.

Mac OS X machines are managed in conjunction with UNIX machines.

Procedure

1. "Add Mac OS X Machines" on page 142
   Add Mac OS X machines to the Available Machines list to make the machines available for licensing.

2. "License Mac OS X Machines" on page 143
   License Mac OS X machines before you install the Agent and begin to manage them. You license the machines displayed in the Available Machines list.

3. "Install the Agent on Mac OS X Machines" on page 143
   Install the appropriate version of the VCM Agent on each of your licensed target machines to enable communication between the Collector and the managed Mac OS X machines.

4. "Collect Mac OS X Data" on page 149
   When the Mac OS X machines are licensed and the Agent is installed, you collect data from those machines.

Continuous machine management is based on the latest data you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data. See "UNIX/Linux Collection Results" on page 132.
Add Mac OS X Machines

Add Mac OS X machines to the Available Machines list to make the machines available for licensing.

If you add a large number of machines, you can use other methods to add the machines. See the online help for procedures to import machine information from a file or use IP Discovery.

**NOTE** You can use the Discovered Machines Import Tool (DMIT), which imports machines discovered by the Network Mapper (Nmap), to import many physical and virtual machines at one time into the VCM database. Download DMIT from the VMware Web site.

**Prerequisites**

Verify that you know the name or IP address, domain, domain type, machine type, and the communication port for the machines to add.

**Procedure**

1. Click **Administration**.
2. Select **Machines Manager > Available Machines**.
3. Click **Add Machines**.
4. On the Add Machines page, select **Basic** and click **Next**.
5. On the Manually Add Machines - Basic page, add the machine information.
   a. Configure machine information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine</td>
<td>Type the name of the machine.</td>
</tr>
<tr>
<td></td>
<td>You can use NetBIOS or Fully-Qualified Domain Name (FQDN) notation for the name. If your Collector cannot resolve a host name with a DNS Server, use an IP address rather than a machine name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Type or select the domain to which the machine belongs.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the domain type.</td>
</tr>
<tr>
<td>Machine Type</td>
<td>Select the machine type.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port number.</td>
</tr>
<tr>
<td></td>
<td>The default value is 26542 when you select a UNIX/Linux or Mac OS X machine type.</td>
</tr>
<tr>
<td></td>
<td>The port number must be the same number used when you install the Agent on the managed Mac OS X machine.</td>
</tr>
</tbody>
</table>

   b. Click **Add**.
   c. To add other machines, configure the machine information and click **Add**.
   d. After you add the target machines, click **Next**.

6. On the Important page, review the machine information and click **Finish**.

   The machine is added to the Available Machines data grid.
What to do next
License the machine. See "License Mac OS X Machines" on page 143.

License Mac OS X Machines
License Mac OS X machines before you install the Agent and begin to manage them. You license the machines displayed in the Available Machines list.

Prerequisites
- Verify that you added the Mac OS X machines. See "Add Mac OS X Machines" on page 142.
- Verify that the machines you are licensing have a specified Machine Type. Machines without a Machine Type value will not be licensed.

Procedure
1. Click Administration.
2. Select Machines Manager > Available Machines.
3. Select the machines and click License.
4. On the Machines page, verify that the Selected list includes the machines to license and click Next.
5. On the Product License Details page, review the licensed machine count and click Next.
6. On the Important page, click Finish.

What to do next
Install the Agent on the target machines. See "Install the Agent on Mac OS X Machines" on page 143.

Install the Agent on Mac OS X Machines
Install the appropriate version of the VCM Agent on each of your licensed target machines to enable communication between the Collector and the managed Mac OS X machines.

Installing the Agent on Mac OS X machines is a manual operation. The Agent is packaged as a Universal Binary Installer. You can run the installation process in silent mode or interactive mode. To run the installation in silent mode, you must edit the configuration options in the csi.config file. The file is edited to accommodate different target machine types.

Prerequisites
- Verify that the machine on which you intend to install the Agent has enough free disk space. For more information, see the VCM Installation Guide.
- If you run an installation in silent mode, modify the appropriate csi.config file variable options. See "Installation Options for Max OS X csi.config " on page 146.
- If you select (x) inetd/launchd for CSI_AGENT_RUN_OPTION, verify that (x) inetd/launchd is running on the target machines. On some versions, when (x) inetd/launchd services are not configured, (x) inetd/launchd will not stay running. To ensure the Agent installation completes successfully, pass a - stayalive option to (x) inetd/launchd. See "Installation Options for Max OS X csi.config " on page 146.
- Log in to the target Mac OS X machine as root, or have sudo as root.
Select the method that you want to use to copy files to the target machines. You can use ftp, sftp, or cp using an NFS share. If you use ftp to copy the package to your machine, you must use binary mode.

If you are collecting non-ASCII information from the target machines, install a UTF-8 locale. To determine the locales installed on your operating system, use the `locale -a` command.

**Procedure**

1. Copy the appropriate Agent binary installation package from the Collector to the machine on which you will install the Agent.

   The Agent packages are located on the Collector in `\Program Files (x86)\VMware\VCM\Installer\Packages`

<table>
<thead>
<tr>
<th>Operating System Version</th>
<th>Agent Binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac OS X (Version 10.5, 10.6, 10.7)</td>
<td>CMAgent.&lt;version&gt;.Darwin</td>
</tr>
</tbody>
</table>

2. On the target machine, run `chmod u+x <filename>` to set the execute permission for the file owner on the Agent binary file.

3. In the directory to which you copied the file, run `./CMAgent.<version>.<Agent binary name>` to create the necessary directory structure and extract the files.

   To force an overwrite of any existing files, include the `-o` option. For example:
   
   `./CMAgent.<version>.Darwin -o`

   The command and output is similar to the following example, but with different file names depending on the operating system.

   ```
   # ./CMAgent.<version>.Darwin
   creating: CSIInstall/
   inflating: CSIInstall/CMAgent.5.1.0.Darwin.i386
   inflating: CSIInstall/CMAgent.5.1.0.Darwin.ppc
   inflating: CSIInstall/csi.config
   inflating: CSIInstall/InstallCMAgent
   
   4. Run `cd <extractedpath>/CSIInstall` to change the directory to the location where the InstallCMAgent executable file was extracted.

5. Run `ls -la` to validate that the correct files are in the `<extractedpath>/CSIInstall` directory.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallCMAgent</td>
<td>Installation script.</td>
</tr>
<tr>
<td>csi.config</td>
<td>Configuration file for the installation. This is the file you can modify to include installation options for silent rather than interactive installation processes.</td>
</tr>
<tr>
<td>packages</td>
<td>Installation packages.</td>
</tr>
<tr>
<td>scripts</td>
<td>Scripts required for the installation.</td>
</tr>
</tbody>
</table>

6. (Optional) Edit the `csi.config` file to customize the installation variables and save your changes.
a. Run the `chmod u+x csi.config` command to add write file permissions if the file has only read permissions set.

b. Modify the `csi.config` file options based on your local requirements and save the file.

c. Copy the modified and saved `csi.config` file to the extracted location.

   For example, `# cp /<safelocation>/csi.config /<extractedlocation>/CSIInstall/csi.config`.

7. Run `InstallCMAgent` in either silent mode or interactive mode.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent mode</td>
<td>Run the <code># ./CSIInstall/InstallCMAgent -s</code> command.</td>
</tr>
<tr>
<td></td>
<td>Install the Agent using the silent mode if you manually edited the <code>csi.config</code> file, if you modified the <code>csi.config</code> file using the interactive method, or if you are using a custom configuration file that you saved from a previous Agent installation. This mode uses the values specified in <code>csi.config</code> without prompting for input. When the silent installation finishes, a summary of the installation process and status appears. Verify that the installation finished without errors.</td>
</tr>
</tbody>
</table>

| Interactive mode | Run the `# ./CSIInstall/InstallCMAgent` command.                                                                                       |
|                  | Install the Agent using the interactive mode if you did not modify the `csi.config` and to respond to each prompt to accept or change each parameter in the `csi.config` file as it runs. As a result of your responses, the `csi.config` is modified. The preinstallation stage of interactive mode checks for a valid user, `CSI_USER`. If the user exists, you are not prompted for these configuration values. |
|                  | - `CSI_USER_NO_LOGIN_SHELL`                                                                                                             |
|                  | - `CSI_USER_PRIMARY_GROUP`                                                                                                             |
|                  | - `CSI_USER_PRIMARY_GID`                                                                                                               |
|                  | - `CSI_USER_USE_NEXTAVAILABLE_LOCAL_GID`                                                                                               |
|                  | You are prompted for these values only when the `CSI_USER` user account is not found. The User and the Group are created in the local directory service storage. |

You can check the installation status in the installation log file. The file is located in `<CSI_PARENT_DIRECTORY>/log/install.log`.

8. Run `ls -la /CSI_PARENT_DIRECTORY/CMAgent` to verify that all the required files and directories
were installed.

/CSI_PARENT_DIRECTORY/CMAgent is the default directory. If you changed the directory name during installation, modify the ls -la command to display the custom directory name.

drwxr-x--- 3 root cfgsoft 4096 Jul 2 17:34 Agent
drwxr-x--- 3 root cfgsoft 4096 Jul 2 17:34 CFC
-rw-rw---- 1 root cfgsoft 49993 Jul 2 17:34 CSIRegistry
-rw-rw---- 1 root cfgsoft 0 Jul 2 17:34 .CSIRegistry.lck
drwxrwx--- 3 csi_acct cfgsoft 4096 Jul 2 17:34 data
drwxrwx--- 3 root cfgsoft 4096 Jul 2 17:34 ECMu
drwxr-x--- 6 root cfgsoft 4096 Jul 2 17:34 install
lrwxrwxrwx 1 root root 20 Jul 2 17:34 log -> /var/log/CMAgent/log
dr-xr-x-x 3 root cfgsoft 4096 Jul 2 17:34 ThirdParty
drwx-xr-x 2 root root 4096 Jul 2 17:34 uninstall

9. Run `# netstat -na | grep <port_number>` to verify that the Agent is installed correctly, listening on the assigned port, and ready to collect data.

The default <port_number> is 26542 for VCM installations.

What to do next
Run a collection for Mac OS X data. See "Collect Mac OS X Data" on page 149.

Installation Options for Max OS X csi.config

The installation options are variables you add or modify in the csi.config file used when you install the Agent. You can create several versions of this file based on operating system or specific settings, but do not change the file name.

<table>
<thead>
<tr>
<th>Installation Options with Default Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSI_AGENT_RUN_OPTION=run by inetd/xinetd/launchd.</td>
<td>You can install the Agent as a daemon process or installed to be run by inetd/xinetd/launchd.</td>
</tr>
<tr>
<td>CSI_NO_LOGIN_SHELL=+/sbin/noshell+/bin/false+/sbin/false+/usr/bin/false+/bin/nologin</td>
<td>The CSI_USER account must not have a login shell. This parameter lists all valid no-login shells and is used to verify the CSI_USER has no-login shell.</td>
</tr>
<tr>
<td></td>
<td>If your system has a valid no login shell that is not listed, you append a plus sign and add the no login shell to the list.</td>
</tr>
<tr>
<td></td>
<td>The options available for this parameter include:</td>
</tr>
<tr>
<td></td>
<td>+D means only for Darwin (Mac OS X)</td>
</tr>
<tr>
<td></td>
<td>+ means for all operating systems</td>
</tr>
<tr>
<td>CSI_CREATE_USER=Y</td>
<td>Keep the default value. Indicates whether the user will be created.</td>
</tr>
<tr>
<td>CSI_USER_ID=501</td>
<td>Keep the default value. Integer value for the user ID of the created user.</td>
</tr>
<tr>
<td>Installation Options with Default Values</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSI_USER_NO_LOGIN_=SHELL=/bin/false</td>
<td>Keep the default value. Indicates the no-login shell value to use when you create the user.</td>
</tr>
<tr>
<td>CSI_USER_PRIMARY_GROUP=csi_acct</td>
<td>Keep the default value. Group name to use when you create a new user as the user's primary group. This group is for low security access. Most inspections are executed with the lowest possible privileges using this group while also preventing access by way of this group to the high security group privileges.</td>
</tr>
<tr>
<td>CSI_CREATE_USER_PRIMARY_GROUP=Y</td>
<td>Keep the default value. Indicates the need to create a low-security primary group for the CSI_USER.</td>
</tr>
<tr>
<td>CSI_USER_PRIMARY_GID=501</td>
<td>Keep the default value. Create user's primary Group ID.</td>
</tr>
<tr>
<td>CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID=Y</td>
<td>Keep the default value. Setting this option to Y allows the Group ID to be the next available local Group ID over CSI_USERPRIMARYGROUP.</td>
</tr>
<tr>
<td>CSI_USER=csi_acct</td>
<td>Keep the default value. The user assigned to the cfgsoft group. The CSI listener process runs under this user.</td>
</tr>
<tr>
<td>CSI_CFGSOFT_GID=500</td>
<td>Keep the default value. The Group ID of the cfgsoft group. This value can change if the GID is already in use. This group is for high-security access. Some inspections require root privileges, which are provided indirectly through this group and setuid to root.</td>
</tr>
<tr>
<td>CSI_CREATE_LOCAL_GROUP=Y</td>
<td>Keep the default value. Setting this option to Y allows the cfgsoft group to be created. This setting allows the system call to groupadd.</td>
</tr>
<tr>
<td>CSI_USE_NEXT_AVAILABLE_LOCAL_GID=Y</td>
<td>Keep the default value. Setting this option to Y allows this Group ID to be the next available local Group ID starting at CSI_CFGSOFT_GID.</td>
</tr>
<tr>
<td>CSI_AGENT_PORT=26542</td>
<td>Keep the default value. Specifies the port on which the Agent listens.</td>
</tr>
<tr>
<td>CSI_CREATE_LOCAL_SERVICE=Y</td>
<td>Keep the default value. Setting CSI_CREATE_LOCAL_SERVICE to Y allows the system to create the local service (copy files to system directories).</td>
</tr>
<tr>
<td>CSI_REFRESH_INETD=Y</td>
<td>This option does not apply to Mac OS X.</td>
</tr>
<tr>
<td>CSI_NICE=10</td>
<td>Keep the default value. Sets the nice value for the agent listener process.</td>
</tr>
<tr>
<td>CSI_CERTIFICATE_PATH=</td>
<td>Specifies the path to Collector Certificates. The certificates specified at this path are copied to the Agent. If your Collector Certificates are stored in an accessible location on this machine, you use this option to put the certificates in the Agent location. You should install the Enterprise Certificates so that multiple collector instances collecting from the same set of Agents is supported. If this package was copied from a collector installation, this package already</td>
</tr>
<tr>
<td>Installation Options with Default Values</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSI_PARENT_DIRECTORY=/opt</td>
<td>Specifies the parent directory of the CM Agent. The root directory of CMAgent will be CSI_PARENT_DIRECTORY/CMAgent.</td>
</tr>
<tr>
<td>CSI_PARENT_DATA_DIRECTORY=/opt</td>
<td>Specifies the parent directory of the CMAgent data directory. The data directory will be CSI_PARENT_DATA_DIRECTORY/CMAgent/data.</td>
</tr>
<tr>
<td>CSI_PARENT_LOG_DIRECTORY=default</td>
<td>Specifies where agent operational log files are kept. The log directory is CSI_PARENT_LOG_DIRECTORY/CMAgent/log. The default value indicates to use these values.</td>
</tr>
<tr>
<td>CSI_KEEP_CSIINSTALL=Y</td>
<td>Recommend keeping the default value. After a successful installation, the temp installation directory CSIInstall is deleted. To keep this installation directory, set this parameter to Y.</td>
</tr>
<tr>
<td>CSI_LOCALE=</td>
<td>Keep the locale configuration option unspecified in the csi.config file when installing the Agent. If you configure the value, it supercedes the data encoding locale on the target operating system. The locale, which should be a UTF-8 locale, affects the internal data conversions on non-ASCII data performed by VCM, but the setting does not affect how the collected data is displayed in VCM. This configuration value is used to resolve any problems with data conversions after you install the Agent.</td>
</tr>
</tbody>
</table>

If this value is left blank, the Agent installation scripts attempt to find an appropriate value for the CSIRegistry base on the following rules presented in order of precedence.

1. The optional CSI_LOCALE value set is in the csi.config file.
   By default, the entry is blank in the csi.config file package in the Agent. If this value is set, the Agent installation script uses the provided value. During the installation of the Agent, the value is checked against the operating system to ensure that it is a valid value. If the value is not valid, it is still used and is set as the value in the CSIRegistry, but the process logs and displays an installation error. The Agent uses what is in the CSIRegistry.

2. The default locale on the target operating system at installation time is [some locale value].utf8. For example, en_US.UTF-8.
   The value is added to the CSIRegistry.

3. The default locale on the target operating system is not UTF-8, but has a UTF-8 locale installed. For example, if the default locale is en_US.UTF8-15 and en_US.UTF-8 is installed on the system, en_US.UTF-8 is used.
installation Options with Default Values

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The UTF-8 locale is added to the CSIRegistry.</td>
</tr>
</tbody>
</table>

4. No default locales are specified on the target operating system.
   The Agent installation script runs the locale -a command and adds the first installed UTF-8 locale that it finds to the CSIRegistry.

5. The operating system is not configured for any internationalization.
   The Agent installation script runs the locale -a command and adds the first installed UTF-8 locale that it finds to the CSIRegistry, but the process logs and displays an i18n warning.

If you interactively install the Agent, the Agent installation scripts use the previous precedence rules to evaluate and generate a default value that is displayed during the installation of the Agent.
If you select a non-UTF-8 locale, the Agent installation uses the locale, but the process logs and displays a warning. If you select a locale that does not exist on the operating system, the Agent installation uses the locale, but the process logs and displays an error.

Manually Uninstall the Mac OS X Agent

When you install the Agent, an uninstall file, UninstallCMAgent, is created in <path>/CMAgent/uninstall. You use the file to manually uninstall the Agent from the managed machine.

The uninstall reverses all changes made by installation. However, the installation log files are retained in <AgentRoot>/install. <AgentRoot> defaults to the CMAgent directory that was created during installation.

Prerequisite

To save a copy of the configuration file to use on other machines, copy csi.config to a secure location. The file is located in <path>/CMAgent/install.

Procedure

1. Navigate up one level from the uninstall directory in the CMAgent directory.
2. Run the # ./uninstall/UninstallCMAgent command to uninstall the Agent.

What to do next

After you run UninstallCMAgent, delete the remaining the CMAgent directory before you install a new Agent.

Collect Mac OS X Data

When the Mac OS X machines are licensed and the Agent is installed, you collect data from those machines.
Collecting data from machines adds the collected machine information to the VCM database and makes the machine data available for reporting, running compliance, and other management options. The collection process for Mac OS X collection is similar to other collections, including Windows, except that you select Mac OS X data types during the collection instead of Windows data types.

**Prerequisites**

- License the target machines. See "License Mac OS X Machines" on page 143.
- Install the Agent on the target machines. See "Install the Agent on Mac OS X Machines" on page 143.

**Procedure**

1. Click Collect.
2. On the Collection Type page, select Machine Data and click OK.
3. On the Machines page, select the machines from which you are collecting data and click Next.
4. On the Data Types page, configure the collection and click Next.
   a. Select the Select All check box.
   b. Select Use default filters.
5. On the Important page, verify that there are no conflicts with previously scheduled or running jobs, and click Finish.
   The amount of time the first collection requires is determined by the number of machines and network connectivity.
6. Click Administration and select Job Manager > History > Instant Collections > Past 24 Hours to determine if the collection finished.

**What to do next**

- Review your collected data. See "Mac OS X Collection Results" on page 151.

**Collected Mac OS X Data Types**

The collected Mac OS X data types that you can collect include related UNIX/Linux and specific Mac OS X data types.

- Custom Information - subset of CITs
- Environment Settings - Properties
- File System - File Structure
- IP Information - General
- IP Information - Routing
- IP Information - Interfaces (IF)
- IP Information - Open Ports
- Machines - General
- Machines - Power Management
- Processes - launchctl
Mac OS X Collection Results

Mac OS X data is displayed in VCM and is available for several management actions.

The displayed data is only as current as the last time you collected the data.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Displays dashboards and summary reports based on collected data. You use the Console to view data relevant to day-to-day operations, troubleshooting, and analysis. The displayed data is based on the collected Mac OS X data types. See the online help for a list of currently collected data types. To view the dashboards, click Console and select Dashboards &gt; UNIX. To view the summary reports, click Console and select UNIX tab &gt; Operating System &gt; Machines &gt; General. You can view the data in a summary report or data grid format.</td>
</tr>
<tr>
<td>Reports</td>
<td>Runs preconfigured VCM reports or create custom reports. Reports are run against currently collected data. Depending on the volume or complexity of the data requested in a report, it may take time to generate the report. Refer to the online help for information about scheduling and disseminating reports. To use the reporting options, click Reports and select Machine Group Reports &gt; UNIX.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Determines if the collected data from target machines meets specified compliance values, and allows you to run compliance remediation actions. To run a compliance check, click Compliance and select Machine Group Compliance and follow the steps described in the online help to create rule groups, rules, filters, and templates.</td>
</tr>
<tr>
<td>Patching</td>
<td>Assesses target machines to determine if the machines have the most current patches. If the patches are not yet installed, you can install the latest patches on the target machines. To assess and patch machines, select Patching, and select your target operating system.</td>
</tr>
</tbody>
</table>
VCM Patching is the VCM patch assessment, deployment, and verification capability, which ensures continuous security throughout your environment by proactive compliance of your IT infrastructure. VCM Patching ensures that your machines have the latest security patches and other software installed. You can evaluate each machine in your environment to ensure that the machines have the latest Microsoft security bulletins or supported UNIX and Linux vendor patches installed, and deploy the recommended patches to each machine.

VCM 5.6 and later does not include the Patch Administrator role. If you previously assigned the Patch Administrator role to a user, either reassign a different role to the user or let the user know that the role no longer exists.

Before you patch Windows 2008 servers and Windows 7 machines, verify that the Windows Update service is running. This service must not be disabled or the patch deployment will fail.

**IMPORTANT** For VCM Patching to assess Windows systems correctly, you must have a current collection of File System, Hot Fix, Registry, and Services data. VCM Patching uses the File System, Registry, and Services data to determine which applications that might require patches are installed and running, and uses the Hot Fix data to determine which patches are installed on the machines. VCM Patching for UNIX and Linux machines collects the data when you perform an assessment.

This chapter includes the following topics:

- UNIX and Linux Patch Assessment and Deployment
- Getting Started with VCM Patching
- Running VCM Patching Reports
- Customize Your Environment for VCM Patching

**VCM Patching for Windows Machines**

VCM Patching for Windows machines helps you deploy patches to bring Windows machines into compliance.

- **Bulletins**: Lists Microsoft bulletins available to VCM Patching. View these bulletins either by bulletin or by affected product.
- **Assessment Templates**: Contains one or more patch bulletins. When you run an assessment, Windows machines that require the patches appear. You can select bulletins or product names to create templates.
- **Imported Templates**: Associates Windows machines with patches for the deployment of those patches.
to selected machines. Use these user-defined templates with Windows machines.

- **VCM Patching Administration**: Configures email notifications, proxy server and logon information, machine group mapping for custom patching, and administration tasks for Windows, UNIX, and Linux machines.

**VCM Patching for UNIX and Linux Machines**

VCM Patching for UNIX and Linux machines helps you deploy patches to bring UNIX and Linux machines into compliance.

- **Bulletins**: Lists vendor bulletins available to VCM Patching.
- **Assessment Templates**: Contains one or more patch bulletins. When you run an assessment, UNIX and Linux machines that require the patches appear. You can select bulletins or product names to create templates.
- **Imported Templates**: Associates UNIX and Linux machines with patches for the deployment of those patches to selected machines. Use these user-defined templates with UNIX and Linux machines.
- **Assessment Results**: Displays the results of your patch assessment for all bulletins or for specific bulletins.
- **VCM Patching Administration**: Configures email notifications, proxy server and logon information, machine group mapping for custom patching, and administration tasks for Windows, UNIX, and Linux machines.

**UNIX and Linux Patch Assessment and Deployment**

VCM Patching includes UNIX and Linux patch assessment and deployment, which you use to determine the patch status of UNIX and Linux machines.

---

**NOTE**  Assessments of UNIX and Linux machines operate differently from Windows assessments. UNIX and Linux assessments require you to collect new data. Windows assessments are performed against previously collected data.

---

Before you use VCM Patching to install patches on UNIX and Linux machines, you must collect patch assessment data from those machines.

VCM Patching for UNIX and Linux involves the following steps.

1. Check for patch bulletin updates from the download site.
   - New PLS files are downloaded to the VCM Collector.
2. Use VCM to collect and assess machine data from managed machines.
   - During the collection, the PLS files are sent to the managed UNIX/Linux machines.
3. Use VCM to explore the assessment results and determine the patches to deploy.
4. Acquire and store the patches using FTP, HTTP, or any other method.
5. Use the VCM Deploy wizard to install the UNIX patches on the managed machines.

VCM Patching for UNIX and Linux is illustrated in the following diagram.
To verify that VCM supports your UNIX and Linux machines for patch deployment, see the VCM Installation Guide.

VCM provides patch assessment content in a new format for several Red Hat and SUSE versions. See “New UNIX Patch Assessment Content” on page 155. For the operating system versions supported, see the VCM Installation Guide.

**New UNIX Patch Assessment Content**

VCM provides patch assessment content in a new format for several Red Hat and SUSE versions. For the operating system versions supported, see the VCM Installation Guide. All other UNIX and Linux versions use the standard content architecture.

When the VCM 5.4.1 or later Agent is installed on these machines, VCM supports patch assessments using the new content architecture.

With the new patch assessment content, VCM updates the information required to assess the patch status of your VCM managed Red Hat and SUSE machines. Results for the new and standard patch assessment content formats appear together in a single view in VCM. Use these results to analyze the patch status of all versions of your Red Hat and SUSE machines regardless of the VCM Agent version installed on them.

Patch deployment to all Red Hat and SUSE managed machines that include a combination of VCM pre-5.4.1 and 5.4.1 or later Agents installed uses a single action. In earlier versions of supported Red Hat and SUSE operating systems that have a pre-5.4.1 Agent installed, the pre-5.4.1 content is enabled automatically for patch assessments.

**Patch Bulletin Name Changes**

In the assessment results, patch bulletins appear with titles that differ from the standard content.

<table>
<thead>
<tr>
<th>Managed Machine</th>
<th>New Bulletin Title</th>
<th>Standard Bulletin Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUSE SLES 10.0–10.4, 11.0–11.1</td>
<td>Novell SUSE 2010-09-16 x86_64: Security update for bzip2</td>
<td>Novell Linux 2010-09-16 x86_64: Security update for bzip2</td>
</tr>
</tbody>
</table>
The .pls files use new names. Red Hat file names include Red Hat instead of RH, and SUSE file names include Novell SUSE instead of Novell Linux.

Patch Assessment Content Private Repository

The new patch assessment content architecture uses a private YUM repository to contain the VCM patch assessment content for Red Hat and SUSE machines. This content supports several Red Hat and SUSE versions that have the VCM 5.4.1 or later Agent installed.

The VCM 5.4.1 installation process installs the repository in the CMAgent directory on the Collector machine. During a UNIX patch assessment of the Red Hat or SUSE machines, VCM copies the repository from the Collector to the managed machines. VCM Patching accesses the content in this repository to perform the patch assessments on those machines.

Installed Patch Assessment Files

A patch assessment of the Red Hat and SUSE machines creates several files in the /tmp directory. These files include yrl.txt, yli.txt, and yls.txt. At the start of each patch assessment process, VCM removes these files and recreates them during the patch assessment.

When you perform a patch assessment of the Red Hat or SUSE machines, the VCM 5.4.1 or later Agent installation process uses a script named mcescan to access the local private repository on the managed machine. The mcescan script resides in the /usr/bin/ directory on the managed machine.

Patch Assessment Content Download Settings

The administration settings in VCM enable the patch assessment content download to the Collector. During a patch assessment, the Collector copies the patch assessment content to your Red Hat and SUSE machines based on the VCM Linux Agent installed on those machines.

- Managed machines that have the VCM 5.4.1 or later Agent installed use the new content architecture.
- Managed machines that have the VCM 5.4.0 or earlier Agent installed use the standard content architecture.

Getting Started with VCM Patching

Use VCM Patching to assess the state of managed Windows, UNIX, and Linux machines, and deploy patches to those machines.

- “Getting Started with VCM Patching for Windows Machines” on page 156
- “Getting Started with VCM Patching for UNIX and Linux Machines” on page 164

Getting Started with VCM Patching for Windows Machines

Use VCM Patching to determine the patch status of Windows machines and deploy patches to those machines.

Prerequisites

To deploy patches to Windows or UNIX/Linux machines, UNIX machines in single-user mode, or AIX machines, you must understand the actions in the deployment and perform several prerequisites. See “Prerequisites for Patch Deployment” on page 159.
Procedure

1. "Check for Updates to Bulletins" on page 157
   Use VCM Patching to check the Web for updates to patch bulletins, which you can use in assessments of machines to enforce compliance.

2. "Collect Data from Windows Machines by Using the VCM Patching Filter Sets" on page 157
   Collect data from Windows machines to obtain the current patch status. VCM Patching requires you to collect current information about the File System, Hotfixes, Registry, and Services Windows data types.

3. "Assess Windows Machines" on page 158
   Use an assessment template to assess the patching status of Windows machines.

4. "Review VCM Patching Windows Assessment Results" on page 159
   View the assessed Windows machines. The Assessment Results data grid displays the Windows machines that were assessed, the patch status for each machine, and details about the patches.

5. "Deploy Patches to Windows Machines" on page 163
   Deploy patches to Windows machines that are managed by VCM Patching.

6. "Collect Data from Windows Machines by Using the VCM Patching Filter Sets" on page 157
   Collect data again from Windows machines to obtain the updated patch status.

7. "Assess Windows Machines" on page 158
   Run another assessment to assess the updated patch status of Windows machines.

Check for Updates to Bulletins

Use VCM Patching to check the Web for updates to patch bulletins, which you can use in assessments of machines to enforce compliance.

Procedure

1. Click Patching.

2. Select Windows > Bulletins.

3. To obtain a comprehensive view of all released bulletins, click By Bulletin.

4. To find a bulletin for an installed software product, click By Affected Product.

5. Select Check for Update.

6. If updates exist, download the updates.
   Follow the prompts to update your bulletins, force an update to the bulletins, or cancel the request.

7. Click Finish to submit the download job to the pending job queue.
   When the job is finished running, the content is available in VCM.

Collect Data from Windows Machines by Using the VCM Patching Filter Sets

Collect data from Windows machines to obtain the current patch status. VCM Patching requires you to collect current information about the File System, Hotfixes, Registry, and Services Windows data types.
Procedure

1. On the toolbar, click Collect.
2. Select the Windows machines from which to collect data.
3. Select Select a Collection Filter Set to apply to these machines and click Next.
   This filter set gathers information for all available Windows security bulletins that you can use to patch Windows machines. Select any monthly filter set to filter the bulletins released in a particular month.
5. If no conflicts appear, click Finish to begin the collection.
   If problems occur while collecting data from Windows machines using the VCM Patching Filter Sets while using the default Network Authority Account, either give the account access to the Windows servers or use a separate Network Authority Account for these machines. See Default Network Authority Account for more information.

Assess Windows Machines

Use an assessment template to assess the patching status of Windows machines.

Because the assessment is run only against data in the database, you must collect machine patching data before and after you run an assessment. When run, the template checks data collected from machines to confirm whether the patches referenced by the bulletins must be installed on those machines. For example, a template might contain all bulletins related to Internet Explorer 7 to ensure that all of the instances installed have the latest security fixes.

The assessment checks all of the VCM managed machines in the active machine group. A patch deployment applies only to the machines in the machine group that are managed by VCM Patching.

You can create an assessment template based on bulletins or affected software products, or by importing a text file that lists machines that require a particular patch or that lists machine and patch pairs. The following procedure generates an assessment template based on bulletins.

Prerequisite

Review the collected patching data and determine which machines must be patched.

Procedure

1. Click Patching.
3. Select a bulletin.
4. Click Details and read the technical details about the bulletin, including the affected products and vendor recommendations.
5. Read the Deployment Summary to identify any issues that might interfere with the distribution of the bulletin.
6. Click On the Web to link to vendor information about the bulletin.
7. Review all of the bulletins to include in the assessment template.
8. To create a template that includes all of the bulletins for patches to deploy, select all of the relevant bulletins and click Create Template.
9. Verify that the bulletins are selected and click Finish to create the template.
10. On the VCM toolbar, verify that the correct Machine Group is selected.

11. Click Patching and select Windows > Assessment Templates.

12. Select the template to run and click Assess.

13. When the assessment finishes, click the Refresh button on the toolbar and view the assessment results in the data grid.

**Review VCM Patching Windows Assessment Results**

View the assessed Windows machines. The Assessment Results data grid displays the Windows machines that were assessed, the patch status for each machine, and details about the patches.

**Prerequisites**

Run an assessment template.

**Procedure**

1. Click Patching.

2. Select Windows > Assessment Templates

3. Select the template and view the results in the data grid.

4. View the Patch Status column to determine the state of each machine for the patches listed.

5. If the assessment results provide multiple pages of data, click the Patch Status column heading and drag it up to Column Grouping.

6. In the Column Grouping view, expand the Not Patched status to view all of the machines that are not patched.

7. To display the graphical representation of the patch assessment status, select Enable/Disable Summary in the template data grid view to enable the Summary view.

8. Click the template node.

   The Summary view displays a graph of the patch status for the machines that were assessed and the patch status by asset classification and bulletin severity rating. The Not Patched column displays machines that require a patch or a reboot for a patch that was applied.

   From the Summary view you can navigate to the affected machines.

**Prerequisites for Patch Deployment**

To deploy patches to Windows or UNIX/Linux machines, UNIX machines in single-user mode, or AIX machines, you must understand the actions in the deployment and perform several prerequisites.

VCM Patching runs assessments of UNIX and Linux machines against the patches that VMware knows at the time when VCM Patching performs the assessment.

VCM saves UNIX and Linux patching change actions in the VCM change log. To check the change log, click Console and select Change Management > VCM or Non VCM Initiated Change > By Data Type > Patch Assessment. These change actions are available to Compliance and Reports.

**IMPORTANT** If a failure occurs at any point in the patch deployment job, the System Administrator must check the status of the system, resolve any issues, and then reassess the machines.
VCM Patching Actions

The following actions are available.

- **Agent Install**: VCM Patching installs the Agent component to a machine the first time a patch is deployed to that machine.

- **Agents using HTTP**: If VCM Patching detects that the target machine has an VCM Agent using HTTP, VCM Patching will route the deployment through VCM as a remote command job.

Prerequisites

- Test all patches before you deploy them.

- Back up critical systems. Before you deploy selected patches, you must understand their potential impact and create backups of critical systems.

- Set Administrator privileges. If users who do not have Administrator privileges use VCM Patching to deploy patches, you must modify the File-level permissions of the C:\\collector_\name\\cmfiles\\SUM Downloads share. This default share is shared to Everyone with full control, but the file permissions are more limited and the Everyone group only has read permission on the directory. Make sure that the user, or a group to which the user belongs, has write permission in the download directory.

- Set the timing for multiple patch jobs. When one or more patches are deployed, a job is created for each machine. Click Patching and select Job Management > Windows or UNIX > Job Manager > Scheduled. If a reboot is required, two jobs are created for each machine, each with the same start time. If you have many machines, or if you selected to download the patches at run time, jobs might exceed the defined window before they time out. If jobs time out, you take the following actions.
  - Increase the setting named "How long before a request will be considered stale (minutes)". Click Administration and select Settings > General Settings > Collector.
  - Increase the setting named "Maximum Concurrent Agent Installs". Click Administration, select Settings > General Settings > Patching > Windows > Deployment, and edit the Collector Option.
  - Reschedule jobs in Job Manager. Click Patching and select Job Management > Windows or UNIX > Job Manager > Scheduled.

Acquire the UNIX Patches

After you review the assessment results and determine which patches to deploy, use FTP, HTTP, or another available method to acquire the UNIX patches from the appropriate vendor.

Store the UNIX Patches

Store the UNIX patches in a location that is available locally to the VCM managed machine, such as an NFS mount or a local hard drive. If you store the patches on an NFS mount, you must define the path in machine group mapping. Click Administration and select Settings > General Settings > Patching > Machine Group Mapping. You can use VCM remote commands or another available method to place the patches on the VCM managed machines.

Patch Repository Management

You must manage your own patch repository. A temporary expansion of the patches occurs in the /tmp directory. For single-user mode, patches are extracted to /var/tmp. If you do not use Machine Group Mapping to define an alternate location for the patches, the default location of /tmp is used.
Machine Group Mapping

When you define an alternate patch location for a particular machine group, you must select that machine group in VCM before you deploy the patches. If you do not select this machine group, VCM Patching will not acknowledge the alternate patch location and the patches will not be deployed. The alternate patch location is defined in machine group mapping. Click Administration and select Settings > General Settings > Patching > Machine Group Mapping.

Default Location for UNIX/Linux Patches

If you do not define an alternate location for the patches using machine group mapping, VCM Patching uses the default location of /tmp. A temporary expansion of the patches occurs in the /var/tmp directory. This directory includes the extracted patches and working files that VCM Patching uses for patch deployment. This location must have enough space for these files.

This location must be available in single user mode because some patches on various operating systems require single-user mode.

Location for UNIX/Linux Patches

When you patch UNIX and Linux machines, copy the patches to a shared location and then specify the local patch path location. Click Administration and select Settings > General Settings > Patching > Machine Group Mapping.

To Deploy Patches in Single-User Mode on UNIX Machines

If you will deploy patches in single-user mode on UNIX machines, you must perform several actions.

1. Store or extract the patches in a local location other than /tmp that will be accessible in single user-mode.

2. If you did not manually extract the files in step 1, ensure enough disk space exists to extract the patches in /var/tmp.

3. Set the machine group mapping to the patch path location where you have stored the patches.

4. To successfully deploy UNIX patches in single-user mode, the at daemon must be running on the machines where patches are being deployed.

To Deploy Patches Without Changing the Run Level on UNIX Machines

If you will deploy patches without changing the run level on UNIX machines, you must perform several actions.

1. Store or extract the patches in a local location.

   Do not use /tmp on Solaris machines because this directory will be cleaned out upon reboots that might be initiated by the patches.

2. If you did not manually extract the files in step 1, ensure that enough disk space exists to extract the patches in /tmp, or in /var/tmp on Solaris machines.

3. Set the machine group mapping to the patch path location where you have stored the patches.

4. To successfully deploy UNIX patches where a reboot is required or requested, the at daemon must be running on the machines where patches are being deployed.
You must set the Machine Group mapping for VCM to the location of the patches during deployment. Setting the machine group mapping is especially important when patching in single-user mode because /tmp is not always available, and cannot be relied upon for patching with VCM.

Machine Group mappings are not inherited. For example, if under the machine group called UNIX Machines, you create a machine group called Solaris, the machine group mapping that exists for UNIX Machines will not be applied to the Solaris machine group.

**To Patch AIX machines**

Deploying some patches might fail on AIX machines if the patch prerequisites cannot be resolved by VCM using the downloaded patch bulletin content. This problem can arise with an AIX patch whose status is StatusNotPatched, and where the Bulletin Detail indicates a patch dependency on another set of patches whose dependencies cannot be met.

Although dependencies might not appear the Bulletin Detail, one or more currently irresolvable patch dependencies might actually exist. The missing patch prerequisites can occur when some patch versions do not become applicable until after other patches are installed. In particular, Maintenance Level (ML) or Technology Level (TL) packages and their corresponding bulletins that are intended to upgrade between levels might not show as applicable until the ML/TL upgrade has been met or exceeded. For example, if you are applying a patch that depends on an intermediate ML that has not yet been applied, deploying the patch will fail because the prerequisite patch dependency has not been met.

To resolve the patch interdependencies on AIX machines, you must determine the patch strategy used for the filesets/APARS/MLs/TLs that are being updated.

**Default Location for UNIX/Linux Patches**

If you do not define an alternate location for the patches using machine group mapping, VCM Patching uses the default location of /tmp. A temporary expansion of the patches occurs in the /var/tmp directory.

This directory includes the extracted patches and working files that VCM Patching uses for patch deployment. This location must have enough space for these files.

This location must be available in single user mode because some patches on various operating systems require single-user mode.

**vCenter Software Content Repository Tool**

To help you obtain UNIX patches for deployment, use the Software Content Repository Tool, which is available from the Download VMware vCenter Configuration Manager Web site.

Prerequisites

Ensure you have access to the VCM documentation page at [https://www.vmware.com/support/pubs/vcm_pubs.html](https://www.vmware.com/support/pubs/vcm_pubs.html).

**Procedure**

1. On VCM documentation page, click **Current Product Download**.
2. On the Download VMware vCenter Configuration Manager Web site, click **Drivers & Tools**.
3. Expand **VMware vCenter Configuration Manager Tools**.
4. For your VCM version, click **View Download**.
5. Locate the Software Content Repository Tool and click **Download Manager** or **Manually Download**.
Deploy Patches to Windows Machines

Deploy patches to Windows machines that are managed by VCM Patching. These machines appear in the Licensed Machines node. Click Administration and select Machines Manager > Licensed Machines.

**IMPORTANT** If a failure occurs at any point in the patch deployment job, the System Administrator must check the status of the system, resolve any issues, and then reassess the machines.

**Prerequisites**
- Follow the guidelines. See "Prerequisites for Patch Deployment" on page 159.
- Verify that the Windows Update service is running (set to something other than Disabled) before you patch Windows 2008 servers and Windows 7 machines.

**Procedure**
1. Click Patching.
2. Select Windows > Assessment Templates and select the template used for the assessment.
3. Make sure the data grid view is visible so that you can view the machines and bulletins.
4. Locate the rows that display the StatusNotPatched status.
   - To identify the machines that must be patched, group the Patch Status column.
5. Highlight the row that contains the machine to be patched and select Deploy.
   - With VCM Service Desk Integration installed, the Service Desk Connector dialog box appears before the VCM Patching Deploy wizard. VCM Orchestrator must approve the deployment job before it can run.
6. (Optional) Select additional machine and patch combinations to include.
7. Select the machines and patches to deploy and click Next.
   - To detect the patch, the Deploy checks the Collector first, and uses the downloaded patch, if found. If patches are not found, the Deploy wizard attempts to locate the patch on the Internet.
   - If the patch is found on the Internet, you can choose to download the patch immediately or at run time.
   - If access to the Internet is denied, you must obtain the patches manually and store them in \\collector_name\cmfiles$\SUM Downloads on the Collector.
8. If you selected multiple patches to deploy, confirm the order to deploy the patches or reorder them, and click Next.
9. On the Switches page, do not select any switches for the installatio, and click Next.
10. On the Patch Staging and Deployment Schedule page, select to copy the patches to the VCM Patching machine during deployment.
11. Select to run the deployment immediately or schedule it to run later, and click Next.
12. Click Next to either schedule the deploy job or to instruct VCM Patching to execute the job immediately.
13. On the Reboot Options page, select to not reboot the machine and click Next.
14. On the confirmation page, click Finish to deploy the patch.
   - When the deployment completes, VCM Patching runs a delta collection of the VCM Patching Security Bulletins filter set to update the assessment information.
What to do next

- To view the status of the deployment job, click Patching and select Job Management > Windows > Job Manager > Running.
- If you scheduled the job to run later, to view the status of the scheduled deployment, click Patching and select Job Management > Windows > Job Manager > Scheduled > Deployments.
- In the assessment template data grid view, run another assessment and confirm that the machines you patched are marked as Patched in the assessment results. If a machine is in a pending reboot state, the patch status for the machine is Not Patched.

For more information about scheduled patch deployments for Windows machines, see the online help.

Getting Started with VCM Patching for UNIX and Linux Machines

Use VCM Patching for UNIX/Linux to determine the patch status of UNIX and Linux machines and deploy patches to those machines.

NOTE Assessments of UNIX and Linux machines operate differently from Windows assessments. UNIX and Linux assessments require you to collect new data. Windows assessments are performed against previously collected data.

VCM saves UNIX and Linux patching change actions in the VCM change log. To check the change log, click Console and select Change Management > VCM or Non VCM Initiated Change > By Data Type > Patch Assessment. These change actions are available to Compliance and Reports.

Prerequisites

- Collect patch assessment data from licensed UNIX and Linux machines.
- Verify that your UNIX and Linux machines and operating systems are supported for patch deployment. See the VCM Installation Guide.

Procedure

1. "Check for Updates to Bulletins" on page 164
   Check for updates to VCM Patching bulletins before you assess the patching state of UNIX and Linux machines.

2. "Collect Patch Assessment Data from UNIX and Linux Machines" on page 165
   Collect UNIX and Linux patch assessment data using bulletins, an assessment template, or the Collect wizard.

3. "Explore Assessment Results and Acquire and Store the Patches" on page 166
   View the assessed UNIX and Linux machines. The Assessment Results data grid displays the UNIX and Linux machines that were assessed, the patch status for each machine, and details about the patches.

4. "Deploy Patches to UNIX/Linux Machines" on page 168
   Install the patches on UNIX and Linux machines that are managed by VCM Patching.

Check for Updates to Bulletins

Check for updates to VCM Patching bulletins before you assess the patching state of UNIX and Linux machines.

Prerequisites

Place patch bulletin files on the local machine to load the bulletin updates from a local file.
Procedure
1. Click Patching.
2. Select UNIX/Linux Platform > Bulletins > By Bulletin.
3. Click Check for Update.
4. Select Check for Updates via the Internet and click Next.
   If VCM Patching finds updates, they are downloaded to the local machine. Alternately, you can load
   the updates from patch bulletin files on the local machine.

Collect Patch Assessment Data from UNIX and Linux Machines
Collect UNIX and Linux patch assessment data using bulletins, an assessment template, or the Collect
wizard.

- **Bulletins**: Collect patching data using the Patch Assessment collection filter. Because UNIX and Linux
  assessments are VCM collections, you can schedule these assessments.

- **Assessment template**: Collect patching data using a template that filters the patch assessment results.

- **Collect wizard**: Collect patching data using the Patch Assessment Data Class filter.

**NOTE** Assessments of UNIX and Linux machines operate differently from Windows assessments. UNIX
and Linux assessments require you to collect new data. Windows assessments are performed against
previously collected data.

VCM Patching runs assessments of UNIX and Linux machines against the patches that VMware knows at
the time when VCM Patching performs the assessment.

Patch assessments of UNIX and Linux machines are based on the OS version and machine architecture.
When you collect assessment data using templates, you must match the bulletins, either 32-bit or 64-bit, to
the machine architecture.

If machine data has not been collected, the assessment results might not appear and the machine will not
be available for deployment. A patch-machine mismatch status results. You can display or hide the patch-
machine mismatch status. Click **Administration** and select **Settings > General Settings > Patching >
UNIX > Settings > Bulletin and Update**.

Prerequisites
- Confirm that assessments finished successfully.

- Verify that the patch signature files (.pls files) exist on the Collector.
  The .pls files determine whether required patches are installed on the machine. By default, VCM
  Patching downloads the .pls files every 4 hours.

  Patch files appear in the Console. Click **Console** and select **UNIX > Security > Patches > Assessment or
  Console > Change Management > Non VCM Initiated > By Machine**. During an assessment of the
  machines using the Patch Assessment Data Class, the .pls files are sent from the Collector to the
  machine. A delay might occur during this process.

- Verify that the VCM Agent is installed on the UNIX or Linux machine.

- Verify that you have preconfigured filters if you choose Filters in the following procedure. See "Create
  UNIX and Linux Patch Assessment Filters" on page 166.
The following procedure runs the assessment using patch bulletins.

Procedure
1. On the toolbar, select the **All UNIX Machines** machine group.
2. Click **Patching**
3. Select **UNIX/Linux Platform > Bulletins > By Bulletin**.
4. Select **Assess**.
5. In the UNIX Patch Assessment wizard, select **Default Filter** or **Filters**.
   - If you selected **Filters**, you must select a specific filter.
6. Click **Next** and **Finish** to begin the assessment on all machines in the selected machine group.
7. On the toolbar, click **Jobs** and view the progress of the collection.
   - The assessment on UNIX and Linux machines uses the Patch Assessment collection filter to perform a collection of all machines in the current machine group, and the results are reported in the Assessment Results node.
8. Select **UNIX/Linux Platform > Assessment Results > All Bulletins** and view the results.

Create UNIX and Linux Patch Assessment Filters

Patch assessment filters identify patch bulletins that meet user-defined filtering criteria. These filters limit the bulletins to use in the assessments, which improves the efficiency of the assessment.

Procedure
1. Click **Administration**.
2. Select **Collection Filters > Filters**.
3. In the Collection Filters data grid, select **Add Filter**.
4. On the Name and Description page, name the filter and click **Next**.
5. On the Data Type page, select **UNIX/Linux**.
6. Select **Patch Assessment** and click **Next**.
7. On the **UNIX Patch Assessment Filters** page, to create a subset of the available bulletins, select **Include Bulletin(s) that match this criteria**.
8. Define the filter criteria using the available settings.
   - For example, you can create a filter where **Platform** = **Red Hat** and **Severity** = **Critical**.
9. Click **Next** and **Finish** to create the filter.
10. In the Collection Filters data grid, scroll or page to the Patch Assessment in the Data Type column and locate the new filter in the Name column.

What to do next

Use the new filter when you run an assessment.

Explore Assessment Results and Acquire and Store the Patches

View the assessed UNIX and Linux machines. The Assessment Results data grid displays the UNIX and Linux machines that were assessed, the patch status for each machine, and details about the patches.
Procedure

1. Click **Patching**.

2. Select **UNIX/Linux Platform > Assessment Results > All Bulletins** to display the patch status of all of the machines that were assessed.

3. To display the assessment results for a single bulletin, select **By Specific Bulletin** and select a bulletin in the center pane.

4. Review the patch status for each machine.

<table>
<thead>
<tr>
<th>Icon Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt=" " /></td>
<td>Patched</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Patch-Machine Mismatch</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Patch Not Needed</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Not Patched</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Error Occurred</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Signature Not Found</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Incorrect MD5</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Patch Status Unknown</td>
</tr>
</tbody>
</table>

If machine data has not been collected, the assessment results might not appear and the machine will not be available for deployment. A patch-machine mismatch status results. You can display or hide the patch-machine mismatch status. Click **Administration** and select **Settings > General Settings > Patching > UNIX > Settings > Bulletin and Update**.

**Acquire the UNIX Patches**

After you review the assessment results and determine which patches to deploy, use FTP, HTTP, or another available method to acquire the UNIX patches from the appropriate vendor.
**Store the UNIX Patches**

Store the UNIX patches in a location that is available locally to the VCM managed machine, such as an NFS mount or a local hard drive. If you store the patches on an NFS mount, you must define the path in machine group mapping. Click **Administration** and select **Settings > General Settings > Patching > Machine Group Mapping**. You can use VCM remote commands or another available method to place the patches on the VCM managed machines.

**Patch Repository Management**

You must manage your own patch repository. A temporary expansion of the patches occurs in the /tmp directory. For single-user mode, patches are extracted to /var/tmp. If you do not use Machine Group Mapping to define an alternate location for the patches, the default location of /tmp is used.

**Machine Group Mapping**

When you define an alternate patch location for a particular machine group, you must select that machine group in VCM before you deploy the patches. If you do not select this machine group, VCM Patching will not acknowledge the alternate patch location and the patches will not be deployed. The alternate patch location is defined in machine group mapping. Click **Administration** and select **Settings > General Settings > Patching > Machine Group Mapping**.

**Default Location for UNIX/Linux Patches**

If you do not define an alternate location for the patches using machine group mapping, VCM Patching uses the default location of /tmp. A temporary expansion of the patches occurs in the /var/tmp directory. This directory includes the extracted patches and working files that VCM Patching uses for patch deployment. This location must have enough space for these files.

This location must be available in single user mode because some patches on various operating systems require single-user mode.

**Deploy Patches to UNIX/Linux Machines**

Install the patches on UNIX and Linux machines that are managed by VCM Patching.

The deployment assesses whether the patch was installed on the VCM managed machine. The Deploy action exists in the User-created Assessment Template, Imported Template, and Assessment Results for All Bulletins.

---

**IMPORTANT** If a failure occurs at any point in the patch deployment job, the System Administrator must check the status of the system, resolve any issues, and then reassess the machines.

**Prerequisites**

- Verify that your UNIX and Linux machines and operating systems are supported for patch deployment. See the VCM Installation Guide.
- Ensure that patch assessments ran successfully.
- Ensure that patches are available locally to the machine.
- Complete the prerequisites. See "Prerequisites for Patch Deployment" on page 159.

The following procedure deploys the patches using All Bulletins.
Procedure

1. Select **Patching > UNIX/Linux platform > Assessment Results > All Bulletins.**
2. Select the patches to deploy.
3. Select **Deploy.**
4. On the Machines & Bulletins page, review the Recommend Action and Data Age and select the machines and patches to deploy.
5. If you deploy multiple patches, on the Confirm Patch Deployment Order page confirm or reorder the patches in the sequence to be deployed.
6. (Optional) If you need to set the machine run level, on the Run Level for Patch Installation page, set the run level for the patch installation and keep in mind that in single-user mode no network is available.
7. (Optional) If you need to specify commands to deploy the patches, on the Command Line Options page specify the options to use.
8. (Optional) If you need to run remote commands as part of the deployment, on the Pre-Deployment and Post-Deployment Remote Commands page select any of the remote commands to apply during the patch deployment.
9. On the Patch Deployment Schedule page, set the timing for the patch deployment job.
10. On the Reboot Options page, select the options to reboot the machine and send a message or select to avoid a reboot.
11. On the Confirmation page, confirm the patch summary information and complete the wizard to deploy the patch.

After you deploy patches, VCM collects assessment data again to confirm the patches were applied.

VCM saves UNIX and Linux patching change actions in the VCM change log. To check the change log, click **Console** and select **Change Management > VCM or Non VCM Initiated Change > By Data Type > Patch Assessment.** These change actions are available to Compliance and Reports.

**How the Deploy Action Works**

The Deploy action runs a command from the Collector to the VCM managed machines. The VCM job command performs the following actions.

- **Assesses VCM managed machines to determine whether the patch was installed since the last assessment.**
- ** Runs a preinstall script (remote command) if specified.**
- **Installs the patch that already resides on the VCM managed machine’s NFS mounted or local file system.**
- ** Runs a postinstall script (remote command) if specified.**
- **Assesses whether the patch was installed on the VCM managed machine.**

The preinstall and postinstall scripts used in the Deploy actions are remote commands, which differ from using a VCM remote command to install a patch. The patch assessment and deployment process for UNIX and Linux does not use remote commands. If you choose to deploy a patch using a user-created remote command, the patch will not be assessed until you run an assessment.
Running VCM Patching Reports

You can run patch status reports on UNIX and Windows machines based on trends, details, template summary, bulletins, affected software products, and patch deployment history.

With real-time assessment reports you can generate SQL reports for machines assessed against bulletins and affected software products. With the patch deployment history report, you can report on the history of patch deployments using VCM Patching assessment results.

You can generate several reports.

- Create real-time assessment reports by bulletins or products.
- Create real-time assessment reports by affected software products.
- Create real-time assessment reports of bulletins and products.
- Create a patch deployment history report.

When you generate reports, you can take the following actions.

- Manually update VCM Patching Windows content.
- Run reports without Internet access.

Customize Your Environment for VCM Patching

Perform routine maintenance on your VCM configuration management database. With routine maintenance, you can tune the visibility of configuration information so that the policies you develop and the actions you take are appropriate for your IT infrastructure.

To ensure that you retain the correct information for auditing, review the data retention settings and update them appropriately according to your policies.

For more information about VCM Patching, see the online help.
Using the Compliance module, you define a standard configuration for all machines or multiple standards for different machine groups. Then, you compare machines against these configuration rules to see if the machines are in compliance. In some cases, you can enforce certain settings on the machines that are not in compliance.

Preset rules and templates are available that enable you to begin monitoring system compliance to regulatory (Sarbanes-Oxley, HIPAA, GLBA and FISMA) industry and Microsoft standards. You can create and manage rules and rule groups based on Active Directory (AD) objects and configuration data, or on machine data.

**IMPORTANT** Compliance does not query individual systems; it only queries the database. If a machine has not been included in a Collection, or the necessary information has not been included in a Collection, or the last Collection is outdated, the Compliance Monitor will measure incorrect or out-of-date data. Therefore, for accurate Compliance monitoring, you must first collect the necessary data.

**Getting Started with SCAP Compliance**

Security Content Automation Protocol (SCAP) is a suite of standards that enable automated vulnerability management, measurement, and policy compliance evaluation. The VCM SCAP implementation employs or references six open standards that SCAP uses to enumerate, evaluate, and measure the impact of software problems and to report results.

- **Common Configuration Enumeration (CCE).** A standard of unique identifiers for common system configuration issues
- **Common Vulnerabilities and Exposures (CVE).** A dictionary of standard identifiers for security vulnerabilities related to software flaws
- **Open Vulnerability and Assessment Language (OVAL).** An XML standard for security testing procedures and reporting
- **Common Platform Enumeration (CPE).** Standard identifiers and a dictionary for platform and product naming
- **Extensible Configuration Checklist Description Format (XCCDF).** A standard for specifying checklists and reporting results
- **Common Vulnerability Scoring System (CVSS).** A standard for conveying and scoring the impact of vulnerabilities

To calculate CVSS scores that apply to your unique environment, go to the CVSS scoring Web site, fill in the form, and click the Update Scores button.

This release of VCM is compatible with the SCAP 1.0 validation program and is for Windows platforms only.

**Conduct SCAP Compliance Assessments**

You import a benchmark, run an SCAP assessment on the managed machines in your environment, review the results, and have the option to export the results.

**Procedure**

1. "Import an SCAP Benchmark" on page 172
   Add the SCAP benchmark to VCM so that you have the industry-approved set of compliance checks against which to assess your managed machines.
2. "Run an SCAP Assessment" on page 172
   Run an SCAP assessment that compares your managed machine configuration against a profile in a standard SCAP benchmark.
3. "View SCAP Assessment Results" on page 173
   Open and search SCAP assessment results through access in the data grid for the profile against which you measured managed machines.
4. "Export an SCAP Assessment" on page 173
   You can export assessment result output to HTML, XML, CSV, and log files.

**Import an SCAP Benchmark**

Add the SCAP benchmark to VCM so that you have the industry-approved set of compliance checks against which to assess your managed machines.

**Prerequisite**

Obtain a copy of the Tier III or Tier IV benchmark bundle ZIP file that you want. The National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) provides benchmarks for download. [http://web.nvd.nist.gov/view/ncp/repository](http://web.nvd.nist.gov/view/ncp/repository)

**Procedure**

1. Copy the bundle ZIP file to the following folder.
   \{machine-name}\CMFiles$\SCAP\Import
2. Click Compliance.
3. Select SCAP Compliance > Benchmarks.
4. Click Import.
5. Highlight the bundle, and click the right arrow to select it for import.
6. Click Next.
7. Review your selections and click Finish.

**Run an SCAP Assessment**

Run an SCAP assessment that compares your managed machine configuration against a profile in a standard SCAP benchmark.
Prerequisite
Import the benchmark. See “Import an SCAP Benchmark” on page 172.

Procedure
1. Click Compliance.
2. Select SCAP Compliance > Benchmarks > benchmark name > profile name.
3. Click Run Assessment.
4. Highlight the machines to assess, and click the down arrow to select them.
5. Click Next and click Next again.
6. Click Next, review your selections, and click Finish.
   
   A collection job starts, and results are not available until the job finishes. The process differs from the general VCM compliance feature, which looks at existing collection data in the database.

View SCAP Assessment Results
Open and search SCAP assessment results through access in the data grid for the profile against which you measured managed machines.

Where appropriate, VCM includes the corresponding standard identifier in its SCAP assessment results and provides an embedded hyperlink to information about the identifier on Web pages such as those provided by MITRE.

Prerequisite
Generate an assessment. See “Run an SCAP Assessment” on page 172.

Procedure
1. Click Compliance.
2. Select SCAP Compliance > Benchmarks > benchmark name > profile name.
3. In the data grid, find the row for the machine for which you generated an assessment.
4. In the row, click the ellipsis button for the result format that you generated.
   
   The following format options are available on the data grid.
   
   OVAL HTML
   OVAL XML
   XCDDF HTML
   XCDDF XML
5. In the browser window that displays the assessment result, press Ctrl+f to open the search feature, and find the results in which you are interested.

Export an SCAP Assessment
You can export assessment result output to HTML, XML, CSV, and log files. CSV is used for CCE pass/fail results, and log files are for troubleshooting.

Upon successful export, VCM creates a file with a name based on the machine name, output format, and time stamp in the following folder on the Collector.

\\{machine-name\}\CMFiles$\SCAP\Export

You can export the formats that are viewable from the data grid, as well as others.
Prerequisite

Run the assessment. See "Run an SCAP Assessment" on page 172.

Procedure

1. Click Compliance.
2. Select SCAP Compliance > Benchmarks > benchmark name > profile name.
3. Click Export.
4. Highlight the machine for which you want to export assessment results, and click the down arrow to select it.
5. Click Next.
6. Select the output and format for the export file, and click Finish.
Operating system (OS) provisioning is the process of installing operating systems to physical or virtual machines. As part of the provisioning process, you can add newly provisioned machines to VCM.

OS provisioning enables you to quickly deploy one or more physical or virtual machines to meet expanding business needs. Some of these machines may have limited use and lifespan, and may be reprovisioned for other purposes. Other machines are provisioned and distributed for long term use.

The provisioning process installs the supported operating system and the VCM Agent. When the target machines are licensed, you can collect machine data, monitor the machines’ state and status, and manage the security and compliance of the machines.

This chapter includes the following topics:

- Operating System Provisioning Components 175
- Configure Operating System Provisioning Servers 177
- Provision Machines with Operating System Distributions 180
- Provisioned Machines Results 189
- Reprovision Machines 189

**Operating System Provisioning Components**

The OS provisioning components include the VCM Collector, one or more OS Provisioning Servers, and the target physical or virtual machines.

The OS Provisioning Server, when it is installed and configured in your environment, serves as the engine for OS provisioning. However, the process of initiating provisioning actions is managed through the VCM Console. See Figure 12-1, Relationship of OS Provisioning Components.
Patching the Operating System Provisioning Server

Exclude the OS Provisioning Server instances from your automated patching in VCM. Patching the operating system will elevate the minor version and may leave the OS Provisioning Server in an unsupported state.

How Operating System Provisioning Works

The process of provisioning operating systems on physical or virtual machines includes actions that you run in VCM, actions that you perform outside VCM, the underlying processes associated with the actions, and the results.

1. Use VCM to collect the available OS distributions from the OS Provisioning Server.
   
   The collected distributions are displayed in the OS Distributions data grid and are available to install on target machines.

2. Set the BIOS on the target machines to network boot.

3. Connect the target machines to the provisioning network and turn them on.
   
   The OS Provisioning Server discovers the available target machines.
4. Use VCM to collect the discovered target machines from the OS Provisioning Server.
   The discovered target machines appear in the Provisionable Machines data grid by MAC address.

5. Use VCM to send the command that includes the provisioning details to the OS Provisioning Server to
   provision the target machines.
   The OS Provisioning Server creates an installation session for the target machines based on the
   configured OS distribution settings.

6. Reboot the target machines.
   As each target machine requests an IP address from the DHCP server and requests a PXE boot, OS
   Provisioning Server checks the machine’s MAC address to determine if the machine has an installation
   session waiting on the OS Provisioning Server. If an installation session for the machine is found, the
   OS installer boots over TFTP, the OS distribution and VCM Agent are downloaded to the target
   machines using HTTP, and the distribution and Agent are installed on the target machines.
   When the installation completes, the new physical or virtual machines appear in the Provisioned
   Machines data grid. They are licensed or available to license in VCM. If the machine is not licensed, you
   must license it to manage the machine. As each machine is licensed, you manage it in VCM as a
   Windows or Linux machine.

**Configure Operating System Provisioning Servers**

Add OS Provisioning Server instances to VCM so that you can use VCM to submit the install operating
system actions to the OS Provisioning Server. It is the OS Provisioning Server instances that install the
imported operating systems on the target physical or virtual machines.

**Prerequisites**

- Install the OS Provisioning Server and import the OS distributions. See the VCM Installation Guide.

- Install the VCMAgent CMAgent.5.5.0.Linux on your OS Provisioning Server machines using HTTP
  communication protocol and port 26542, the default port. See "Configure Linux and UNIX Machines" on
  page 121.

- Collect the Machines - General data type from the OS Provisioning Server machine. See "Collect
  UNIX/Linux Data" on page 131.

**Procedure**

1. "Add Operating System Provisioning Servers" on page 178
   To register the OS Provisioning Servers, you must add the Red Hat servers that you configured as OS
   Provisioning Servers. When the servers are registered, you select the OS Provisioning Server from
   which to install operating systems when you are configuring the provisioning action.

2. "Set the Trust Status for Operating System Provisioning Servers" on page 178
   You set the trusted status is on Agent machines where you verify that the connection is legitimate.
   When you set the trust status, you are marking the Agent certificate as trusted. When transmitting
   sensitive information, such as credentials, between the Collector and OS Provisioning Servers, the
   machines must be trusted.

3. "Collect Operating System Distributions" on page 179
   Collect the OS Distributions to ensure that you have access to all the operating systems in the OS
   Provisioning Server repository.
4. "Discover Provisionable Machines" on page 179
   The OS Provisioning Server identifies provisionable physical or virtual machines in your environment when the target machines are set to network boot and attempt to PXE boot.

5. "Provision Machines with Operating System Distributions" on page 180
   The OS provisioning process installs one Windows or Linux operating system distribution on one or more physical or virtual machines using OS provisioning.

Continuous provisioned machine management is based on the latest data you collect from the OS Provisioning Server. See "Provisioned Machines Results" on page 189.

Add Operating System Provisioning Servers

To register the OS Provisioning Servers, you must add the Red Hat servers that you configured as OS Provisioning Servers. When the servers are registered, you select the OS Provisioning Server from which to install operating systems when you are configuring the provisioning action.

Prerequisites

- Verify that you installed and configured your OS Provisioning Server instances. See the VCM Installation Guide.
- Ensure that the Red Hat servers that you configured as OS Provisioning Server are added and licensed in VCM. See "Configure Linux and UNIX Machines" on page 121.
- Ensure that you collected Machines - General data from your OS Provisioning Server instances. See "Collect UNIX/Linux Data" on page 131.

Procedure

1. Click Administration.
2. Select Machines Manager > OS Provisioning > Registered Servers.
3. Click Add.
4. On the Select OSP Server page, move the selected servers to the lower pane and click Next.
5. Review the Confirmation information and click Finish.
6. Click Refresh, located on the main toolbar, to update the data grid.

What to do next

- Collect the available distributions from the target OS Provisioning Servers. See "Collect Operating System Distributions" on page 179.

Set the Trust Status for Operating System Provisioning Servers

You set the trusted status is on Agent machines where you verify that the connection is legitimate. When you set the trust status, you are marking the Agent certificate as trusted. When transmitting sensitive information, such as credentials, between the Collector and OS Provisioning Servers, the machines must be trusted.

If you choose not to use this level of security, you can set the Allow sensitive parameters to be passed to agents not verified as Trusted option to Yes in the General Settings for the Collector data grid.
Prerequisites

Verify that your OS Provisioning Server instances are added as registered servers. See "Add Operating System Provisioning Servers" on page 178

Procedure

1. Click Administration.
2. Select Certificates.
3. Select the OS Provisioning Server machines and click Change Trust Status.
4. Add any additional OS Provisioning Server instances to trust to the lower data grid.
5. Select Check to trust or uncheck to untrust the selected machines and click Next.
6. Review the number of machines affected and click Finish.

What to do next

Collect OS distributions from your OS Provisioning Server instances. See "Collect Operating System Distributions" on page 179.

Collect Operating System Distributions

Collect the OS Distributions to ensure that you have access to all the operating systems in the OS Provisioning Server repository. These OS Distributions are operating system images that are available to install on target machines.

Prerequisites

- Ensure that operating system distributions are imported into the OS Provisioning Server repository. To import OS distributions, see See the VCM Installation Guide.
- Verify that the OS Provisioning Integration Enabled setting is configured with a value greater than 0.

Procedure

1. Click Administration.
2. Select Machines Manager > OS Provisioning > OS Distributions.
3. Click Refresh.

This action collects data from the OS Provisioning Server. When the collection finishes, the available operating systems distributions appear in the data grid.

What to do next

Discover target machines. See "Discover Provisionable Machines" on page 179.

Discover Provisionable Machines

The OS Provisioning Server identifies provisionable physical or virtual machines in your environment when the target machines are set to network boot and attempt to PXE boot.
Prerequisites

- Ensure that the target machines have a minimum of 1GB RAM and meet the minimum RAM requirements for the operating system you are installing.

- Configure the primary network interface on the target machines with a connection to the OS Provisioning Server deployment network. If you use a different network as the primary interface, the deployment process appears to start, but you receive communication errors and the process ultimately fails.

Procedure

1. On target machines, configure the BIOS to network boot.
2. Start the machines on your provisioning network.
3. In VCM, click Administration.
4. Select Machines Manager > OS Provisioning > Provisionable Machines.
5. On the data grid toolbar, click Refresh.

   This action collects data from the OS Provisioning Server and the provisioningable machines appear in the data grid when the collection is finished. The machines are identified by MAC address.

What to do next

Provision the target machine. See "Provision Machines with Operating System Distributions" on page 180.

Provision Machines with Operating System Distributions

The OS provisioning process installs one Windows or Linux operating system distribution on one or more physical or virtual machines using OS provisioning.

Depending on the distribution you are installing, use one of the following procedures.

- "Provision Windows Machines" on page 180
  Provisioning physical or virtual machines with a Windows operating system installs the selected operating system and the VCM Agent on one or more of your Windows machines.

- "Provision Linux Machines" on page 183
  Provisioning physical or virtual machines with a Linux operating system installs the selected operating system and the VCM Agent on one or more of your Linux machines.

Provision Windows Machines

Provisioning physical or virtual machines with a Windows operating system installs the selected operating system and the VCM Agent on one or more of your Windows machines.

You can install one OS distribution on one or more target machines. To install a different OS distribution, configure a new OS provisioning action.

Select no more than ten machines per provisioning action.
Prerequisites

- Verify that the operating system you are installing is compatible with the hardware or configuration of the target physical or virtual machines. For example, the operating system must support the drivers required by the hardware.
- Verify that the OS Provisioning Servers are registered. See "Add Operating System Provisioning Servers" on page 178.
- Verify that the OS distributions are collected and appear in the OS Distributions data grid. See "Collect Operating System Distributions" on page 179.
- Verify that the target machines are discovered and appear in the Provisionable Machines data grid. See "Discover Provisionable Machines" on page 179.
- Identify or create any postinstallation scripts that you want to run on the target machine after it is provisioned with the new operating system. The postinstallation scripts are copied to the target machine along with the OS distribution and runs after the operating system is installed.

Procedure

1. Click Administration.
2. Select Machines Manager > OS Provisioning > Provisionable Machines.
3. Select one or more target machines in the data grid on which you are installing the same OS distribution.
4. Click Provision.
5. On the Select OSP Server page, select the OS Provisioning Server that will manage the provisioning action and click Next.
6. On the Select Machines page, add or remove target machines from the selected machine list and click Next.
7. On the Select OS Distribution page, select the Windows operating system that you are installing on the selected machines and click **Next**.

8. On the Settings page, configure the options required for your selected Window OS distribution and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product License Key</td>
<td>(Optional for Windows 2008. Required for Windows 2003 and Windows 7.) Type a license matching the operating system you are installing.</td>
</tr>
<tr>
<td>License Key Type</td>
<td>(Required for Windows 2003 and Windows 7, and for Windows 2008 if Product License Key is provided.) Select the license type, either Retail or MAK (multiple activation key).</td>
</tr>
<tr>
<td>Admin Password</td>
<td>(Required) Type the password for the target machines' local Administrator account.</td>
</tr>
<tr>
<td>Re-enter Admin Password</td>
<td>(Required) Retype the password.</td>
</tr>
<tr>
<td>Domain or Workgroup</td>
<td>(Required) If a Domain and Domain User are specified, Domain details are used. If the domain details are not provided, then the Workgroup is used.</td>
</tr>
<tr>
<td>Add machine(s) to a Domain</td>
<td>Select the check box to add the machines to a Domain rather than a Workgroup. If you select this option, you must configure the domain details.</td>
</tr>
<tr>
<td></td>
<td>The domain controller must be accessible to the deployed machine during the provisioning process.</td>
</tr>
<tr>
<td>Domain Type</td>
<td>Available if you select Add machine(s) to a Domain. Select the type in the drop-down menu.</td>
</tr>
<tr>
<td>Domain User</td>
<td>Available if you select Add machine(s) to a Domain. Type a user name.</td>
</tr>
<tr>
<td>Domain User Password</td>
<td>Available if you select Add machine(s) to a Domain. Type a password for the specified Domain User.</td>
</tr>
<tr>
<td>Re-enter Domain User Password</td>
<td>Available if you select Add machine(s) to a Domain. Retype the password.</td>
</tr>
<tr>
<td>Organization</td>
<td>Name of the licensing organization.</td>
</tr>
<tr>
<td>Windows SKU</td>
<td>(Window 2008 and Windows 7 only) Select the value in the drop-down list. See the online help for possible values.</td>
</tr>
<tr>
<td>Use DHCP to determine IP address</td>
<td>Use your designated DHCP to assign IP address, subnet, default gateway, and DNS. If not selected, you must manually add the information on the Machine-Specific Settings page.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>License these machines for VCM</td>
<td>License the machines for VCM management.</td>
</tr>
</tbody>
</table>

9. On the Machine-Specific Settings page, type the **HostName** and click **Next**.

The HostName is limited to 15 characters.

If you did not select **Use DHCP to determine IP address** on the Settings page, you must configure the IP Address, Subnet, Default Gateway, and DNS.

10. (Optional) On the Post-install Script page, type a **Script Name** and the script, and click **Next**.

11. (Optional) On the Disk Configuration page, select one of the options and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use all available disk space</td>
<td>Creates and formats a single partition using all the available disk space.</td>
</tr>
<tr>
<td>Create partition with <strong>nn</strong> GB</td>
<td>Partitions and formats the specified space. The space you specify must be less than the total available space.</td>
</tr>
</tbody>
</table>

12. On the Confirmation page, click **Finish**.

The OS Provisioning Server starts jobs for each of the selected target machines. Each job creates a configured session for the specified machines. The configured session includes information about the target machine, the OS distribution, the configuration information for the selected combination of target machine and operating system, and the VCM Agent.

13. Reboot the target machines.

You must cycle the power on the machines either manually or using a remote administration mechanism. The machines must be configured to network boot from the OS Provisioning Server, which identifies the configured session that is waiting and the installation begins. If the session does not exist, then the target machine remains provisionable and is not provisioned until a session is created and the target machine is rebooted.

**What to do next**

- Verify that the provisioning process has begun. Click Administration and select **Machines Manager > OS Provisioning > Provisionable Machines**. The machines appear in the appropriate Available Machines or Licensed Machines data grid with an OS provisioning status of OS Provisioning Queued.
- Verify that the provisioning process is finished. Click **Administration** and select **Machines Manager > OS Provisioning > Provisioned Machines**. The OS provisioning status is OS Provisioning Succeeded or OS Provisioning Overwritten.
- Configure the Windows 2008 SP2, and R2, and Windows 7 machines on a public network with access to the Internet and manually complete the Windows license activation on the provisioned machines.
- (Optional) Change the Agent communication protocol. See "Change Agent Communication" on page 188.

**Provision Linux Machines**

Provisioning physical or virtual machines with a Linux operating system installs the selected operating system and the VCM Agent on one or more of your Linux machines.
You can install one OS distribution on one or more target machines. To install a different OS distribution, configure a new OS provisioning action.

**Prerequisites**

- Verify that the operating system you are installing is compatible with the hardware or configuration of the target physical or virtual machines. For example, the operating system must support the drivers required by the hardware.
- Verify that the OS Provisioning Servers are registered. See "Add Operating System Provisioning Servers" on page 178.
- Verify that the OS distributions are collected and appear in the OS Distributions data grid. See "Collect Operating System Distributions" on page 179.
- Verify that the target machines are discovered and appear in the Provisionable Machines data grid. See "Discover Provisionable Machines" on page 179.
- Identify or create any postinstallation scripts that you want to run on the target machine after it is provisioned with the new operating system. The postinstallation scripts are copied to the target machine along with the OS distribution and runs after the operating system is installed.

**Procedure**

1. Click Administration.
2. Select Machines Manager > OS Provisioning > Provisionable Machines.
3. Select one or more target machines in the data grid on which you are installing the same OS distribution.
4. Click Provision.
5. On the Select OSP Server page, select the OS Provisioning Server that will manage the provisioning action and click Next.
6. On the Select Machines page, add or remove target machines from the selected machine list and click Next.
7. On the Select OS Distribution page, select the Linux operating system that you are installing on the selected machines and click Next.

8. On the Settings page, configure the options required for your selected Linux OS distribution and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product License Key</td>
<td>Type the license to use when installing the operating system on the target machines. The license must match the operating system you are installing.</td>
</tr>
<tr>
<td>Root Password</td>
<td>(Required) Type the password you are assigning to the local root.</td>
</tr>
<tr>
<td>Re-enter Root Password</td>
<td>(Required) Retype the password.</td>
</tr>
<tr>
<td>Domain</td>
<td>(Required) Type the domain to which you are assigning the machines.</td>
</tr>
<tr>
<td>Use DHCP to determine IP address</td>
<td>Use your designated DHCP to assign IP address, subnet, default gateway, and DNS. If this option is not selected, you must manually enter the information on the Machine-Specific Settings page.</td>
</tr>
<tr>
<td>License these machines for VCM after deployment</td>
<td>License the target machines for VCM management.</td>
</tr>
</tbody>
</table>

9. On the Machine-Specific Settings page, type the HostName and click Next.

   The HostName is limited to 32 characters.

   If you did not select Use DHCP to determine IP address on the Settings page, you must configure the IP Address, Subnet, Default Gateway, and DNS.

10. (Optional) On the Post-Install Script page, type a Script Name, the script, and click Next.

    Post-install scripts are copied to the machine when the OS distribution is copied and runs after the operating system is installed.

11. (Optional) On the Disk Configuration page, configure the options and click Next.

    You can either install the operating system without partitioning the disk, or you can create partitions and specify the size.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Volume Plan</td>
<td>Select the check box to partition the disk.</td>
</tr>
</tbody>
</table>
| Mount Point         | Type the location of the mount point for the partition. For example, /, /boot, /usr, /var/log. You use the first partition for the operating system and then specify a second mount point for user home directories. The mount points value must meet the specific criteria.

- / and /boot are required mount points.
### Option Description

- Duplicate mount points are not allowed.
- For a swap partition, the mount point and the file system type should be swap.
- When naming mount points, you can use letters, digits, _ and +. Spaces are not allowed.

<table>
<thead>
<tr>
<th>Volume Name</th>
<th>Type the name of the logical partition. For example, LogVol00. The volume names must meet specific criteria. When naming volumes, you can use letters, digits, _ or -. Spaces are not allowed. The name limit 16 characters. If you assign a volume name, you must assign a volume group name. If you assign more than one volume name in a volume group, you cannot use the same name for each volume name.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Volume Size</th>
<th>The the size of the partition in megabytes or gigabytes. For example, 10MB or 1GB. If you select Grow partition to use all remaining space, you can specify a value of 0MB. If Grow is not selected, you must specify a valid partition size.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>File System</th>
<th>Select the type of file system. For a swap partition, the mount point and the file system type should be swap. Supported File System options by operating system.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Supported File System</th>
<th>swap</th>
<th>/boot</th>
<th>/</th>
<th>/home, /tmp, /usr, /var, /usr/local</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 6.0</td>
<td>ext2, ext3, ext4, swap, vfat, xfs</td>
<td>swap</td>
<td>ext2, ext3, ext4</td>
<td>ext2, ext3, ext4, xfs</td>
<td></td>
</tr>
<tr>
<td>RHEL 5.4 and 5.5</td>
<td>ext2, ext3, ext4, swap, vfat</td>
<td>swap</td>
<td>ext2, ext3, ext4</td>
<td>ext2, ext3, ext4</td>
<td></td>
</tr>
<tr>
<td>RHEL 5.0 and 5.2</td>
<td>ext2, ext3, swap, vfat</td>
<td>swap</td>
<td>ext2, ext3, ext4</td>
<td>ext2, ext3</td>
<td></td>
</tr>
<tr>
<td>SLES 10.0 and 11.1</td>
<td>reiser, ext2, ext3, xfs, jfs, swap</td>
<td>swap</td>
<td>reiser, ext2, ext3, ext4</td>
<td>reiser, ext2, ext3, xfs, jfs</td>
<td></td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Supported File System</th>
<th>swapon</th>
<th>/boot</th>
<th>/home, /tmp, /usr, /var, /usr/local</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>xfs, jfs</td>
<td></td>
<td>xfs</td>
<td>jfs</td>
</tr>
</tbody>
</table>

#### Volume Group Name
Type the name of the logical group.

For example, VolGroup00. You can specify only one volume group on the target machines. You may add volume groups after the OS distribution is installed.

The volume names must meet specific criteria.

- When naming volumes, you can use letters, digits, ., or _. Spaces are not allowed.
- The name limit 16 characters.
- If you assign a volume name, you must assign a volume group name.
- (SLES only) You can assign only one volume group when partitioning the disk.
- (RHEL 5.x and 6.0, and SLES 10.3 and 11.1 only) You cannot use /boot as part of the volume group name.

### Add
Click to add the configuration data to the Custom Volume Plan list.

### Custom Volume Plan list
Displays the disk configuration data.

### Grow partition to use all remaining space
Select the option to allow the logical volume to fill available space up to the maximum size specified for the volume.

- You can select the option for only one partition.
- If you select this option, you can specify a Volume Size of 0MB.

### Remove
Click to delete the selected row from the custom volume plan list.

12. On the Confirmation page, click **Finish**.

The OS Provisioning Server starts jobs for each of the selected target machines. Each job creates a configured session for the specified machines. The configured session includes information about the target machine, the OS distribution, the configuration information for the selected combination of target machine and operating system, and the VCM Agent.

13. Reboot the target machines.

You must cycle the power on the machines either manually or using a remote administration mechanism. The machines must be configured to network boot from the OS Provisioning Server, which identifies the configured session that is waiting and the installation begins. If the session does not exist, then the target machine remains provisionable and is not provisioned until a session is created and the target machine is rebooted.
What to do next

- Verify that the provisioning process has begun. Click Administration and select Machines Manager > OS Provisioning > Provisionable Machines. The machines appear in the appropriate Available Machines or Licensed Machines data grid with an OS provisioning status of OS Provisioning Queued.

- Verify that the provisioning process is finished. Click Administration and select Machines Manager > OS Provisioning > Provisioned Machines. The OS provisioning status is OS Provisioning Succeeded or OS Provisioning Overwritten.

- Move the Linux machine to your production network and synchronize the network time. See "Synchronize Time on Installed Linux Operating Systems" on page 188.

- (Optional) Change the Agent communication protocol. See "Change Agent Communication" on page 188.

Synchronize Time on Installed Linux Operating Systems

When Linux machines are provisioned with an operating system, the Network Time Protocol (NTP) service is not running. After moving the newly provisioned Linux machines to a network with access to the NTP server, you must synchronize the time on the machines to network time.

Prerequisites

- Configure the Linux machines on a network with access to the NTP server.

- Identify the NTP servers used in your environment.

Procedure

1. On the Linux machine, log in as root.

2. Run the ntpdate -u <ntpserver> command to update the machine clock.

   For example, ntpdate -u ntp-time.for.mydomain.

3. Open the /etc/ntp.conf file and add the NTP servers used in your environment.

   You can add multiple NTP servers similar to these examples.

   server ntp-time.for.mydomain
   server otherntp.server.org
   server ntp.research.gov

4. Run the service ntpd start command to start the NTP service and implement you configuration changes.

Change Agent Communication

The VCM Agent is installed by the OS Provisioning Server with default settings. After the operating system distribution is installed, you can change the communication setting or install a new Agent.

Prerequisites

Install Windows or Linux operating system distribution. See "Provision Windows Machines" on page 180 or "Provision Linux Machines" on page 183.
Procedure

1. Configure the communication settings for the machines on which you installed one of the following operating using OS provisioning.

   - The Windows Agent is installed with DCOM as the communication protocol. To change the protocol, click Administration and then select Machines Manager > Licensed Windows Machines > Change Protocol.

   - The Linux Agents are installed with inetd or xinetd, as appropriate, with a default communication port of 26542. To change any Agent settings, uninstall the Agent from the machine, and reinstall it with the settings you require. See "Install the Agent on UNIX/Linux Machines" on page 124.

Provisioned Machines Results

Review the OS provisioning data that is specific to the provisioning process.

After you provision the target machines, VCM manages them as Windows or Linux machines. As managed machines, you collect data, add software, run patching assessments, and apply rules to maintain machine compliance in your environment.

The displayed data is only as current as the last time you collected from the OS Provisioning Server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>View administrative details about the OS Provisioning Server.</td>
</tr>
<tr>
<td></td>
<td>- To view all provisioned machines, click Administration and select Machines Manager &gt; OS Provisioning &gt; Provisioned Machines.</td>
</tr>
<tr>
<td></td>
<td>- To view the provisioned Windows machines, click Administration and select Machines Manager &gt; Licensed Machines &gt; Licensed Windows Machines. The OS Provisioning Status column indicates whether the Windows machine was create using OS provisioning.</td>
</tr>
<tr>
<td></td>
<td>- To view the provisioned Linux machines, click Administration and select Machines Manager &gt; Licensed Machines &gt; Licensed UNIX Machines. The OS Provisioning Status column indicates whether the Linux machine was create using OS provisioning.</td>
</tr>
</tbody>
</table>

Reprovision Machines

You can reprovision Windows or Linux machines where the operating system was installed using the OS Provisioning Server and VCM.

When machines are reprovisioned, you may change the machine name.

---

CAUTION Reprovisioning overwrites the existing disk with a new operating system. All existing data is lost.
Prerequisites

- Verify that the machine to be re-provisioned is listed in the Provisioned Machines data grid. Select Administration and click Machines Manager > OS Provisioning > Provisioned Machines.
- Review the provisioning process for the OS distribution you are installing. See "Provision Machines with Operating System Distributions" on page 180.
- On the target machine, set the BIOS to network boot.

Procedure

1. Click Administration.
2. Select Machines Manager > OS Provisioning > Provisioned Machines.
3. Select the machines.
4. Click Re-provision.
5. On the Select OSP Server page, select the OS Provisioning Server that will manage the provisioning action and click Next.
6. On the Select Machines page, add or remove machines and click Next.
7. On the Select OS Distribution page, select the operating system you are installing on the selected machines and click Next.
8. Continue with the provisioning wizard.
   The wizard options vary depending on the OS distribution you are installing.
9. When you are certain that the selected machines are those you want to re-provision, select the Proceed with re-provisioning of the operating system on the selected machines check box.
10. Click Finish.
    The OS Provisioning Server starts jobs for each of the selected machines. Each job creates a configured session for the specified machines. The configured session includes information about the target machine, the OS distribution, the user configuration information for the selected combination of machine and operating system, and the VCM Agent.
11. Reboot the target machines.
    You must cycle the power on the machines either manually or using some remote administration mechanism. The machines must be configured to network boot from the provisioning network. If a session is waiting on the OS Provisioning Server, the installation begins. If the session does not exist, then the machine remains provisioned and will not be re-provisioned until the session is created.

What to do next

- Verify that the provisioning process has begun. Click Administration and select Machines Manager > OS Provisioning > Provisionable Machines. The machines appear in the appropriate Available Machines or Licensed Machines data grid with an OS provisioning status of OS Provisioning Queued.
- Verify that the provisioning process is finished. Click Administration and select Machines Manager > OS Provisioning > Provisioned Machines. The OS provisioning status is OS Provisioning Succeeded or OS Provisioning Overwritten.
- Configure the Windows 2008 SP2, and R2, and Windows 7 machines on a public network with access to the Internet and manually complete the Windows license activation on the provisioned machines.
- (Optional) Change the Agent communication protocol. See "Change Agent Communication" on page 188.
Provisioning Software on Managed Machines

Software provisioning is the process you use to create software packages, publish the packages to repositories, and then install packages on one or more target machines.

To support the provisioning process, the VCM Software Provisioning components consist of VMware vCenter Configuration Manager Package Studio, software package repositories, and Package Manager.

For more information about software provisioning, see VCM online Help, the VCM Software Provisioning Components Installation and User’s Guide, and the Package Studio online Help.

This chapter includes the following topics:

- Install the Software Provisioning Components 194
- Using Package Studio to Create Software Packages and Publish to Repositories 199
- Using VCM Software Provisioning for Windows 201
- Related Software Provisioning Actions 205

Using Package Studio to Create Software Packages and Publish to Repositories

Package Studio is the application used to build software packages for installation on target Windows servers and workstations.

Windows packages can include in-house and commercial software installation files, including .msi, .exe, VBScripts, python, PowerShell.

To add a software installer to a package, it must be able to install and uninstall unmanned or quietly using command line options, response files, or other similar methods.

Software Repository for Windows

Software Repository for Windows is the shared location to which packages are published by Package Studio and the location from which Package Manager downloads packages for installation.

Package Manager for Windows

Package Manager is the application installed on each machine to manage the installation and removal of the software contained in packages. Package Manager is configured to use one or more repositories as sources for packages.
If you are using the software provisioning components in conjunction with VMware vCenter Configuration Manager (VCM), you can use VCM to add and remove sources, and to install and remove packages.

**Software Provisioning Component Relationships**

The following diagram displays the general relationship between Package Studio, repositories, and Package Manager in a working environment.

**Figure 13-1. Software Provisioning Diagram**

---

**Install the Software Provisioning Components**

The software provisioning components are installed on the VCM Collector by default. VMware recommends that you install the Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio on a machine other than the Collector.

The software provisioning components should be installed on machines with these relationships:
- **Software Repository for Windows**: Installed on at least one Windows machine in your environment, and installed on the same machine with Package Studio. Install the repository before installing Package Studio.

- **VMware vCenter Configuration Manager Package Studio**: Installed on the same machine as your software repository.

- **Package Manager**: Installed on all Windows machines on which you are managing software provisioning.

To uninstall the applications using a script at a later date, you should save a copy of each of the .msi files in an archive location. To uninstall using the .msi, you must have the same version used to install the application.

**Procedure**

1. **"Install Software Repository for Windows" on page 195**
   
The Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio should be installed on the same machine. Installing the repository installs the Repository folders and subfolders, and configures the virtual directory. The virtual directory is used by Package Manager to access the repository.

2. **"Install Package Studio" on page 196**
   
   You must install the VMware vCenter Configuration Manager Package Studio and the repository on the same machine. The process installs the application files and specifies the repository to which Package Studio will publish packages.

3. **"Install Package Manager on Managed Machines" on page 198**
   
The Package Manager, which installed on the target machines, manages the installation of the software packages. It does not contain the software packages, only pointers to the packages in the repository sources of which it is aware.

**Install Software Repository for Windows**

The Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio should be installed on the same machine. Installing the repository installs the Repository folders and subfolders, and configures the virtual directory. The virtual directory is used by Package Manager to access the repository.

**Prerequisites**

- Verify that the target machine meets the supported hardware, operating system, and software requirements. See VCM Installation Guide for currently supported platforms and requirements.

- Ensure that you have access to the Repository.msi, which is available on the VMware Web site or in the vCenter Configuration Manager application files. The default location in the VCM application files is C:\Program Files (x86)\VMware\VCM\AgentFiles\Products.
Procedure

1. Double-click Repository.msi.
2. On the Welcome page, click Next.
3. Review the license agreement, select the appropriate options to continue, and click Next.
4. On the Installation Folder page, use the default path or click Change to modify the path, and click Next.
5. On the Virtual Directory page, use the default name or type a new name in the text box, and click Next.
6. On the Ready to Install page, click Install.
7. When the Setup Completes page appears, click Finish.

The repository and the virtual directory are added to the locations specified during installation. The default location for the repository is C:\Program Files\VMware\VCM\Tools\Repository (on 32-bit machines) or C:\Program Files (x86)\VMware\VCM\Tools\Repository (on 64-bit machines). The default virtual directory SoftwareRepository is added to Internet Information Services (IIS) > Web Sites > Default Web Site.

Manually Uninstall the Repository

Using the command line syntax, you can run an unattended uninstall the software repository.

Prerequisites

To uninstall the application, use the same version of the Repository.msi that was used to install the application.

Procedure

1. Copy the Repository.msi to the machine on which you are uninstalling the application or point to the file in a shared directory.
2. Run the .msi file using the following command line syntax:

   msiexec /x [path]\Repository.msi /l*v %temp%\Repository.log

Install Package Studio

You must install the VMware vCenter Configuration Manager Package Studio and the repository on the same machine. The process installs the application files and specifies the repository to which Package Studio will publish packages.

Prerequisites

- Verify that the target machine meets the supported hardware, operating system, and software requirements. See VCM Installation Guide for currently supported platforms and requirements.
- Ensure you have access to the PackageStudio.msi, which is available on the VMware Web site or in the vCenter Configuration Manager application files. The default location in the VCM application files is C:\Program Files (x86)\VMware\VCM\AgentFiles\Products.
- Verify that the Software Repository for Windows is installed. Installing the repository before installing Package Studio reduces the manual configuration steps.
Procedure

1. Double-click PackageStudio.msi.
2. On the Welcome page, click Next.
3. Review the license agreement, select the appropriate options to continue, and click Next.
4. On the Installation Folder page, use the default path or click Change to modify the path, and click Next.
5. On the Repository Root Folder page, verify the path is to your installed repository files. If the path is not accurate, click Change. When the path is correct, click Next.
6. On the Ready to Install page, click Install.

The Package Studio is installed to the location specified during installation. The default location is C:\Program Files\VMware\VCM\Tools\Package Studio (on 32-bit machines) or C:\Program Files (x86)\VMware\VCM\Tools\Package Studio (on 64-bit machines).

To start Package Studio, click Start and select All Programs > VMware vCenter Configuration Manager > Tools > Package Studio, or open the Package Studio folder and double-click PackageStudio.exe.

Install Package Studio Using Unattended .MSI

The manual installation process installs the application files and specifies the repository to which Package Studio will publish packages.

Prerequisites

- Verify that the target machine meets the supported hardware, operating system, and software requirements. See VCM Installation Guide for currently supported platforms and requirements.
- Ensure you have access to the PackageStudio.msi, which is available on the VMware Web site or in the vCenter Configuration Manager application files. The default location in the VCM application files is C:\Program Files (x86)\VMware\VCM\AgentFiles\Products.
- Verify that the Software Repository for Windows is installed. Installing the repository before installing Package Studio reduces the manual configuration steps.

Procedure

1. On your Collector, go to C:\Program Files (x86)\VMware\VCM\AgentFiles\Products.
2. Locate the PackageStudio.msi file and copy it to the target machine or a share location.
3. On the target machine, run the .msi file using the following command line syntax.

   msiexec /i [path]\PackageStudio.msi /qn /1*v %temp%\PackageStudio.log

   You can add the following arguments if you want to specify locations other than the default directories:

   REPOSITORY_ROOT=C:\Program Files (x86)\VMware\VCM\Tools\Repository\ (Defaults to this or uses the Repository’s value if it is already installed)

   PACKAGESTUDIO_DIR="C:\Program Files (x86)\VMware\VCM\Tools\Package Studio\"
   (defaults to this path)
The Package Studio is installed to the location specified during installation. The default location is C:\Program Files\VMware\VCM\Tools\Package Studio (on 32-bit machines) or C:\Program Files (x86)\VMware\VCM\Tools\Package Studio (on 64-bit machines).

To start Package Studio, click Start and select All Programs > VMware vCenter Configuration Manager > Tools > Package Studio, or open the Package Studio folder and double-click PackageStudio.exe.

**Manually Uninstall Package Studio**

Use the following script to run an unattended uninstall the Package Manager.

**Prerequisites**

To uninstall the application, you must use the version of the PackageStudio.msi that was used to install the application.

**Procedure**

1. Copy the PackageStudio.msi to the machine on which you are uninstalling the application or a shared location.
2. Run the installation file using the following command line syntax:
   
   ```
   msiexec /x [path]\PackageStudio.msi /i*v %temp%\PackageStudio.log
   ```

   When Package Studio is uninstalled from a machine, the locally saved projects and .crate files remain on the machine, allowing you to copy them to another machine or to delete them manually if they are not needed.

**Install Package Manager on Managed Machines**

The Package Manager, which installed on the target machines, manages the installation of the software packages. It does not contain the software packages, only pointers to the packages in the repository sources of which it is aware. When directed to install, the package is copied from the repository to the cratecache folder on the target machines. Package Manager unzips the files to the %TMP% directory and runs the configured installation.

The Package Manager is installed on target machines when the 5.3 VCM Agent or later is installed from the Collector.

When a Remove Package action is sent to Package Manager, it checks first for the package in the cratecache. If it is not found, it then checks the repository sources for the package, and again copies it to the target machine's cratecache folder where it unzips the files. The configured uninstall files may be run from the zip directory.

**Installing the VCM Agent**

If you are preparing to use software provisioning on machines not previously managed in VCM, you must first install the VCM Agent. See “Install the VCM Windows Agent on Your Windows Machines” on page 91 for complete instructions. When you install the VCM Agent from the Collector, the installation includes the agent extensions for provisioning and the Package Manager for Windows. If you manually install the Agent using the MSI or EXE, you must manually install the Package Manager and the necessary agent extensions. See the online Help.

This default action is based on the settings in Administration > Settings > General Settings > Installer.

**Prerequisites**

Verify that the target machine meets the supported hardware, operating system, and software requirements. See VCM Installation Guide for currently supported platforms and requirements.
Verifying the Installation of the Agent Extensions for Provisioning

If you do not know whether the machines are ready to use provisioning, you can verify the version of the Agent Extensions for Provisioning. The Agent Extensions for Provisioning include the Package Manager.

1. Select Administration > Machines Manager > Licensed Machines > Licensed Windows Machines.

2. In the data grid, locate the machines on which you are verifying the existence of the necessary Agent Extensions and verify that the Agent Ext. For Prov. Version column contains a value of 5.3 or later.

   If it does not, you need to either install or upgrade the VCM Agent.

Upgrading the VCM Agent

If an earlier VCM Agent is installed on your machines, you will need to upgrade to the latest Agent. See Upgrade Agent in the online Help.

Using Package Studio to Create Software Packages and Publish to Repositories

Package Studio is the application used to build software packages for installation on target Windows servers and workstations.

Windows packages can include in-house and commercial software installation files, including .msi, .exe, VBScripts, python, PowerShell.

To add a software installer to a package, it must be able to install and uninstall unmanned or quietly using command line options, response files, or other similar methods.

Creating Packages

You use Package Studio to create packages, including the installation files and the required metadata. When the package is ready for use, you publish it to a repository. The procedure here is only a general process. See the Package Studio online Help or the VCM Software Provisioning Installation and User’s Guide for the detailed procedures.

Procedure

1. Start the VMware vCenter Configuration Manager Package Studio. Select Start > All Programs All > VMware vCenter Configuration Manager > Tools > Package Studio.

   NOTE: If you are running Package Studio on the Collector or a Windows 2008 Server, you must run the application as administrator. See "Run Package Studio as Administrator" on page 200 for more information.

2. Click Manage Packages. Configure the package contents based on the options on the following tabs:
   a. Click Properties and type a Name, Version, Description, and select the Architecture. These fields are required. You have the option to update the other fields, depending on you requirements.
   
      Configuring the package with Depends, Conflicts, Provides, and adding and configuring the installation and removal files.
   b. Click Files and import the installation files, add pre-command files, configure the commands and arguments, and add post-command files.
   c. Click Save to save the setting and files as a Project (*.prj).
   d. Click Generate to save the project as a package (*.crate).
3. Click **Package Signing** and sign the package with a signing certificate.
   a. Click **Open** to select a package (*.crate file).
   b. Click **Sign** and select a certificate from the certificate store or from a file.
4. Click **Manage Repositories** and select the platforms and sections to which you are publishing the package.
   a. Click **Add Platforms** to add a platform.
   b. Select a platform, and then click **Add Sections**.
   c. Select a section, and then click **Publish Package**.
   d. Select the package (.crate) and click **Open**.
   e. (Optional) Select additional platforms and sections to which to publish the package.
   f. Click **Publish**. The package is published to the software repository.
5. Click **External Software** and add externally managed software, especially any packages specified as depends or conflicts in any of your packages.
   a. Click **New External Package** and replace the text with the name you will use as an external software package name.
   b. Type a version number in the Version text box.
   c. Select the **Architecture** in the drop-down menu.
   d. Click **Select Attribute Name** and select a registry property or WMI attribute in the drop-down menu.
   e. Add attributes.
   f. To save a copy locally, click **Save**.
   g. Click **Publish External SW** to publish to the repository.

**Run Package Studio as Administrator**

The enhanced security on Windows 2008 Server requires you to run Package Studio as an administrator. If you do not, you will not be able to publish packages to the repository.

**NOTE**  You do not need to run Package Studio as administrator if your repositories were configured on non-UAC protected paths or when you are running Package Studio and the repositories on machines other than a Windows 2008 Server.

**Procedure**

1. On a Windows 2008 machines, select **Start > All Programs > VMware vCenter Configuration Manager > Tools**.
2. Right-click **Package Studio** and select **Properties**.
3. Click the **Compatibility** tab.
4. In the Privilege Level area, select **Run this program as an administrator** and click **Apply**.
5. Click **OK**.
6. Select **Start > All Programs > VMware vCenter Configuration Manager > Tools > Package Studio**.
7. On the User Account Control dialog box, click **Yes**.
Using VCM Software Provisioning for Windows

Using VCM Software Provisioning, you collect and view Repository and Package Manager data, and then install or remove packages on target machines.

Prerequisites

Software packages are created and published to the repository. See "Creating Packages" on page 199.

Procedure

1. "Collect Package Manager Information from Machines" on page 201
   
   To view information about packages and Package Managers in VCM, you must collect Package Manager data from managed machines.

2. "Collect Software Repository Data" on page 202
   
   Collect the repository data to identify which software packages are in which repositories. From the collected information, you can determine which repositories to assign to machines based on the available packages.

3. "Add Repository Sources to Package Managers" on page 202
   
   Sources are the sections in the repository from which the Package Manager will be able to download and install packages.

4. "Install Packages" on page 203
   
   The process of installing packages includes identifying and processing dependencies and conflicts; running any specified prescripts; running the installation using any specified command arguments; and running any specified post-scripts.

Collect Package Manager Information from Machines

To view information about packages and Package Managers in VCM, you must collect Package Manager data from managed machines.

Regularly collect Package Manager data to determine if your machines are remaining current with the necessary software packages.

Prerequisites

- Package Manager is installed on the target machines. Package Manager is installed when you install the VCM 5.3 Agent or later. See "Install Package Manager on Managed Machines" on page 198.
- Verify that you created software provisioning packages using VMware vCenter Configuration Manager Package Studio and published the packages to the repositories. See "Creating Packages" on page 199.

Procedure

1. Click Collect.

2. Select Machine Data.

3. Click OK.

4. On the Machines page, verify that the Selected pane displays all the machines from which you are collecting package manager data and click Next.

5. On the Data Types page, expand Windows, select Software Provisioning - Package Managers, and click Next.
6. On the Confirmation page, review the information, resolve any conflicts, and click **Finish**.

You can monitor the process in the **Jobs Manager**. See "Viewing Provisioning Jobs in the Job Manager" on page 205.

**What to do next**

- When the collection is finished, view the collected data. Click **Console** and select **Windows tab > Operating System > Software Provisioning > Package Managers**. The data grid displays the packages and their current status.


**Collect Software Repository Data**

Collect the repository data to identify which software packages are in which repositories. From the collected information, you can determine which repositories to assign to machines based on the available packages.

To better manage your repository machines, create a machine group containing all the machines on which the software repository is installed.

**Prerequisites**

Verify that you created software provisioning packages using VMware vCenter Configuration Manager Package Studio and published the packages to the repositories. See "Creating Packages" on page 199.

**Procedure**

1. Click **Collect**.
2. Select **Machine Data**.
3. Click **OK**.
4. On the **Machines** page, verify that the **Selected** pane displays all the machines from which you are collecting repository data and click **Next**.
5. On the **Data Types** page, expand **Windows**, and select **Software Provisioning - Repositories**, and click **Next**.
6. On the Confirmation page, review the information, resolve any conflicts, and click **Finish**.

You can monitor the process in the **Jobs Manager**. See "Viewing Provisioning Jobs in the Job Manager" on page 205.

**What to do next**

- When the collection is finished, view the collected data. Click **Console** and select **Windows tab > Operating System > Software Provisioning > Repositories**. The data grid displays the packages in the repositories.

- Add the repositories to the Package Manager. See "Add Repository Sources to Package Managers" on page 202.

**Add Repository Sources to Package Managers**

Sources are the sections in the repository from which the Package Manager will be able to download and install packages.
Adding a source gives the Package Manager on the selected machines access to the packages available in specified section. The sources are numbered in priority order. When you add a new one, you can specify whether to add it to the beginning or to the end of the list. You can also remove sources.

**Prerequisites**

- Verify that you collected Package Manager data from the target machines. See "Collect Package Manager Information from Machines" on page 201.
- Verify that you collected repository data from software repository. See "Collect Software Repository Data" on page 202.

**Procedure**

1. Click **Console**.
2. Select **Windows tab > Operating System > Software Provisioning > Package Managers**.
3. Select one or more machines, and click **Add Source**.
4. On the Select Machines page, verify that the machines displayed in the lower pane are the machines to which you want to add the source and click **Next**.
5. On the Enter or Select Source page, configure the options, and click **Next**.
   a. Select either **Add source at the beginning of existing source lists** or **Add source at the end of the existing source list**.
   b. Click **Browse Sources**.
   c. On the Browse Sources page, select one of the following in the Show Sources from drop-down menu.
      - **Package Manager Source Lists**: Select this option if you have already added sources to at least one Package Manager and you want to add the source to other Package Managers. When you click **OK**, the selected source populates the Platform and Section on the Enter or Select Source page.
      - **VCM Managed Repositories**: Select this option if the source has not yet been added to a Package Manager. When you return to the Enter or Select Source page, you must type the platform and section names in the appropriate text boxes.
   d. Select the URI and click **OK**.
   e. Verify that the Platform name and the Section name are exactly the names used in the repository.
6. On the Schedule page, select one of the scheduling options and configure as needed.
7. On the Confirmation page, review the information and click **Finish**.

The added source is displayed in the **Package Manager - Sources** data grid.

**What to do next**

Install software packages on target machines. See "Install Packages" on page 203.

**Install Packages**

The process of installing packages includes identifying and processing dependencies and conflicts; running any specified prescripts; running the installation using any specified command arguments; and running any specified post-scripts. You can also remove packages.
Prerequisites

Verify that you added the repository sources to the Package Managers. See "Add Repository Sources to Package Managers" on page 202.

Procedure

1. Click Console.
3. Click Install Package.
4. On the Select Machines page, verify that the machines displayed in the lower pane are the machines to which you want to install the package and click Next.
5. On the Select Package page, select the package to install.
6. Select one of the following version options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Version</td>
<td>Installs the specified version. By default the operator equals the package selected in the list. However, you may select a different operator and type the version number in the text box.</td>
</tr>
<tr>
<td>Install latest available version on all platforms</td>
<td>Installs the latest version of the package available from the sources configured for the Package Manager.</td>
</tr>
</tbody>
</table>

7. Configure the Security Options and click Next.

Determine whether a package is installed or removed based on the state of the signature.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install secure signed package only</td>
<td>The package must be signed and the public key of the signing certificate you used to sign the package is available on all the machines on which you are installing or removing the package.</td>
</tr>
<tr>
<td>Skip signature validation when installing a signed package</td>
<td>(Not Recommended) The package is installed or removed without attempting to verify the signature.</td>
</tr>
<tr>
<td>Allow unsigned package to be installed</td>
<td>(Not recommended) The package is installed or removed even if it is unsigned.</td>
</tr>
</tbody>
</table>

8. On the Schedule page, select one of the scheduling options and configure as needed.
9. On the Confirmation page, review the information, resolve any conflicts, and click Finish.

You can monitor the process in the Jobs Manager. See "Viewing Provisioning Jobs in the Job Manager" on page 205.

The package is displayed as Installed in the Package Manager - Packages data grid.
Related Software Provisioning Actions

You can use the following management options in VCM when working with software provisioning.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>All Software Provisioning are available for auditing as part of Change Management. Click Console and select <strong>Change Management &gt; VCM Initiated or Non VCM Initiated</strong> to view the data. Software Provisioning actions are not eligible for rollback through Change Management. Undo unwanted changes using Compliance enforcement remediation actions. See &quot;Create Compliance Rules Containing Software Provisioning Remediation Actions&quot; on page 207. Non VCM Initiated changes related to Software Provisioning include publishing packages to repositories from Package Studio and manually running command-line actions in Package Manager.</td>
</tr>
<tr>
<td>Compliance</td>
<td>You can create compliance rules based on software provisioning data types, and you can add provisioning remediation actions to rules. See &quot;Create Compliance Rules Based on Software Provisioning Data&quot; on page 206 and &quot;Create Compliance Rules Containing Software Provisioning Remediation Actions&quot; on page 207.</td>
</tr>
<tr>
<td>Reports</td>
<td>You can run reports on collected Software Provisioning data. Click Reports and select <strong>Machine Group Reports &gt; Software Provisioning</strong> to run the default reports, or you can create your own.</td>
</tr>
<tr>
<td>Administration</td>
<td>Displays current jobs running, and job history. Use the job history when troubleshooting the processing of a job. See &quot;Viewing Provisioning Jobs in the Job Manager&quot; on page 205. Define user access rules and roles to specify what level of access users have to the Software Provisioning data and actions in VCM. Click Administration and select <strong>User Rules and Roles &gt; User Manager &gt; VCM Access</strong> to configure the Access Rules and Roles.</td>
</tr>
</tbody>
</table>

Viewing Provisioning Jobs in the Job Manager

The Jobs Manager tells you the state of a currently running Provisioning job, including the success or failure of a job, either collecting data from machines or installing, updating, or removing packages from machines.

The currently running provisioning jobs are visible in the following locations:

- Jobs button. Located on the portal toolbar.
- Administration slider. Select **Administration > Job Manager > Running**.

Job history is available in **Administration > Job Manager > Other Jobs**. The provisioning related job names include the following types of jobs:

- Change Request: Add Source
- Change Request: Remove Source
- Change Request: Install Package
- Change Request: Remove Package
Create Compliance Rules Based on Software Provisioning Data

A Compliance rule based on software provisioning data detects any packages or sources that are out of compliance. You can configure remediation actions to bring the machines back into compliance.

In this example the Compliance rule checks whether the source, where the values are platform=Any and section=Release, was added to selected Package Managers as a source. If not, then add the repository source to the machines where the rule fails.

Procedure

1. Click Compliance.
2. Select Machine Group Compliance > Rule Groups.
3. Expand your rule group and select Rules.
5. Type a Name and Description for your rule and click Next.
6. On the Data Type page, expand Windows and select the data type on which you are basing the rule and click Next.
   In this example, select Software Provisioning - Package Managers - Sources.
7. On the Rule Type page, select Conditional (if/then) and click Next.
8. On the Conditional Data page, configure the options.
   a. In the IF area, click Add.
   b. Select Source Repository URI = YourRepository.
   c. Select Must Exist.
   d. In the THEN area, click Add and select Platform = Any and Section = Release.
   e. Click Next.
9. On the Options page, configure the settings.
   a. Select a Severity in the drop-down menu.
   b. Select Make available for enforcement where possible.
   c. Select Software Provisioning action.
   d. Select Add Source in the drop-down menu and click Define Action.
   e. On the Software Provisioning Compliance Remediation page, select Add source to the beginning of existing source list.
   f. Click Browse Sources and select the repository URI where the Platform=Any and Section=Release exist, and click OK.
      The Platform and Section update with Any and Release respectively.
   g. Click OK.
   h. Click Next.
10. On the Collection filters page, select the Provisioning - Package Managers collection filter and click Next.
11. On the Important page, review the information and click Finish to save your rule.
What to do next
Add the rule to your template. When the Compliance Template is run, it checks the target machines to determine if the repository source is added as a source. If it is not, the source is added to the machines Package Manager.

Create Compliance Rules Containing Software Provisioning Remediation Actions
When configuring a Compliance rule, you can configure the rule to perform a remediation based on a software provisioning action such as Install Package, Remove Package, Add Source, or Remove Source.

In this procedure, the example is to determine whether a software application named XSoftware is installed. If the software is installed correctly, a service named XService should be running. Configure a Compliance rule to determine if XService service is running. If it is not running, install the XSoftware package.

Procedure
1. Click Compliance.
2. Select Machine Group Compliance > Rule Groups.
3. Expand your rule group and select Rules.
5. On the Rule and Name page, type a Name and Description for your rule and click Next.
6. On the Data Type page, expand Windows, select the data type on which you are basing the rule, and click Next.
   The data type does not need to be software based. In this example, select Services.
7. On the Rule Type for Services page, select Conditional (if/then) and click Next.
8. On the Conditional Data properties page, configure the options and click Next.
   a. In the IF section, click Add.
   b. Select Services Name = XService.
   c. Select Must Exist.
   d. In the THEN section, click Add.
   e. Select State = Running.
9. On the Options page, configure the options.
   a. Select a Severity in the drop-down menu.
   b. Select Make available for enforcement where possible.
   c. Select Software Provisioning action.
   d. Select Install Package in the drop-down menu, and click Define Action.
   e. On the Software Provisioning Compliance Remediation page select the XSoftware package to install if the rule you are configuring fails.
   f. Configure the version options to use the selected version, specify a different version, or install the
g. Specify the Security Options.

Determine whether a package is installed or removed based on the state of the signature.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install secure signed package only</td>
<td>The package must be signed and the public key of the signing certificate you used to sign the package is available on all the machines on which you are installing or removing the package.</td>
</tr>
<tr>
<td>Skip signature validation when installing a signed package</td>
<td>(Not Recommended) The package is installed or removed without attempting to verify the signature.</td>
</tr>
<tr>
<td>Allow unsigned package to be installed</td>
<td>(Not recommended) The package is installed or removed even if it is unsigned.</td>
</tr>
</tbody>
</table>

h. Click OK and click Next.

10. On the Collection filters page, select the Services collection filter and click Next.

11. On the Important page, review the information and click Finish to save your rule.

What to do next

Add the rule to your compliance template. When the template is run, if the check for XService running fails, the XSoftware package is installed.
VCM for Active Directory collects Active Directory objects across domains and forests, and displays them through a single console. The information is consolidated and organized under the Active Directory slider, allowing you to view your Active Directory structure, troubleshoot issues, detect change, and ensure compliance.

You can filter, sort, and group Active Directory data to pinpoint the specific area of interest. You can also view a subset of your Active Directory (a forest, domain, or specific organizational unit branch) by setting the Active Directory location in the AD Location field near the top of VCM. Dashboards display high level information in graphical form, alerts notify you about problems or misconfigurations, and change management tracks changes to the Active Directory objects or configuration by data type.

This chapter includes the following topics:

- Configure Domain Controllers
- Collect Active Directory Data
- Active Directory Collection Results

Configure Domain Controllers

To manage your Active Directory environment, you must verify domains and accounts, discover and license domain controllers, install the VCM Agent, and collect data from the domain controllers.

Procedure

1. "Verify Available Domains" on page 210
   - Allow VCM access to each domain so that the VCM Collector can interact with the domain controllers in your environment.

2. "Check the Network Authority Account" on page 210
   - Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

3. "Assign Network Authority Accounts" on page 211
   - Select and assign the network authority account that you identified for VCM access to the domain controllers.

4. "Discover Domain Controllers" on page 211
   - In your network, identify the domain controllers that you are managing with VCM.
5. "License Domain Controllers" on page 212
   To manage domain controllers, you must license them in VCM.

6. "Install the VCM Windows Agent on Your Domain Controllers" on page 213
   Install the VCM Windows Agent on each domain controller so that you can collect data and manage the virtual or physical machines.

7. Collect Domain Controller Data
   Start managing the domain controllers by performing an initial collection, which adds domain controller data to VCM.

   Continuous domain controller management is based on the latest data that you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data. See "Windows Collection Results" on page 98.

Verify Available Domains

   Allow VCM access to each domain so that the VCM Collector can interact with the domain controllers in your environment.

   During installation, VCM discovered all domains to which the network authority account had access. If the domain controllers belong to a domain that is not listed, you must add that domain manually.

   Prerequisites
   Verify that you have the fully-qualified names of the domains to manage.

   Procedure
   1. Click Administration.
   2. Select Settings > Network Authority > Available Domains.
   3. If the domain does not appear Available Domains view and have a Domain Type of Active Directory, add the domain.
      a. Click Add.
      b. Type the domain name and select the domain type as AD.
      c. Click OK.
   4. Verify that the domain appears in the data grid.

   What to do next
   Verify that a network authority account is available and create other necessary domain accounts. See "Check the Network Authority Account" on page 210.

Check the Network Authority Account

   Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

   VCM network authority accounts must have administrator privileges on each domain to be managed in the organization. Although you specified an initial default network authority account when you installed VCM, you can add different administrator accounts if you do not assign the default account.

   Prerequisites
   Verify the presence of domains. See "Verify Available Domains" on page 210.
Procedure

1. Click Administration.
2. Select Settings > Network Authority > Available Accounts.
3. To add a new domain account, click Add.
4. Type the domain name, user name, and password, and click Next.
5. Click Finish to add the account.

What to do next

Assign the network authority account to the domain so that VCM can access the domain controllers in the domain. See “Assign Network Authority Accounts” on page 211.

Assign Network Authority Accounts

Select and assign the network authority account that you identified for VCM access to the domain controllers.

Assign an account with administrator privileges on the domain.

Prerequisites

Verify or add the necessary network authority account. See “Check the Network Authority Account” on page 210.

Procedure

You must perform the following steps twice, once for NetBios and once for Active Directory.

1. Click Administration.
2. Select Settings > Network Authority > Assigned Accounts > By Domain > NetBios.
3. Select an assigned account.
4. Click Edit Assigned Accounts.
5. Select the account to receive authority to the domain and click Next.
6. Confirm the accounts to include in the authority list for the domain and click Finish.

What to do next

- Repeat the preceding assignment steps, and select Active Directory in step 2.
- Discover the domain controllers in your environment. See “Discover Domain Controllers” on page 211.

Discover Domain Controllers

In your network, identify the domain controllers that you are managing with VCM.

To discover the available domain controllers, VCM uses general discovery rules to identify many Windows machines or uses specific discovery rules to identify particular Windows machines.

The time required to perform an initial discovery depends on the size and composition of your network. If all domain controllers are not available during initial discovery, such as systems that are disconnected from the network, the first discovery will not find all domain controllers. If the discovery does not identify all domain controllers, you might need to run additional discoveries after the other domain controllers become available.
You can use the Discovered Machines Import Tool (DMIT), which imports machines discovered by the Network Mapper (Nmap), to import many physical and virtual machines at one time into the VCM database. Download DMIT from the VMware Web site.

**Prerequisites**

Assign a Network Authority Account that VCM can use for access. See "Assign Network Authority Accounts" on page 211.

**Procedure**

1. Click Administration.
2. Select Machines Manager > Discovery Rules.
3. Click Add to create a discovery rule.
4. Type a name and description and click Next.
5. Select By Browse List and click Next.
6. Select Only discover machines in the Browse List that match these criteria.
7. Select and type the following filter parameters.
   - Where Domain Controller Type <> " (two single quotes, no space)
8. Click Next.
9. Click Yes and click Finish.
10. On the toolbar, click Jobs to track current discovery job status.

**What to do next**

- Verify that jobs have finished running. Click Administration and select Job Manager > History > Other Jobs > Past 24 Hours.
- Verify that the domain controllers are available. Click Administration and select Machines Manager > Available Machines.
- License the domain controllers in your environment. See "License Domain Controllers" on page 212.

**License Domain Controllers**

To manage domain controllers, you must license them in VCM.

The number of discovered domain controllers might exceed the number of your available licenses. If that happens, the number available goes negative and appears in red to indicate that you do not have enough licenses.

For servers and workstations, exceeding the limit on your license key produces warnings but does not restrict VCM operation. License key counts that are over the limit are recorded and maintained for auditing purposes. Suite license keys support unlimited licenses, provided that the suite edition includes VCM and the component that you are managing is part of the suite. If a component is not part of the suite, it counts against the nonsuite server or workstation key.

**Prerequisites**

Verify that the domain controllers you license are listed with a machine type of workstation or server in the Available Machines node. If the discovered or added type is not workstation or server, VCM cannot license the machines.
Procedure

1. Click Administration.
2. Select Machines Manager > Available Machines.
3. Select the domain controllers to license.
4. Click License.
5. Verify that the domain controllers to license appear in the Selected list.
   Use the arrows to move the domain controllers.
6. Click Next to view your Product License Details.
   The licensed domain controller count increases by the number of licensed machines.
7. Click Next.
   VCM confirms that the licenses you requested will be applied to the selected domain controllers.
8. Click Finish.

What to do next

Install the VCM Windows Agent. See "Install the VCM Windows Agent on Your Domain Controllers" on page 213.

Install the VCM Windows Agent on Your Domain Controllers

Install the VCM Windows Agent on each domain controller so that you can collect data and manage the virtual or physical machines.

Before you can collect data from domain controllers, you must install the VCM Windows Agent on the licensed domain controllers in your environment to enable communication between the Collector and the target machines.

Standardized Windows configurations such as Federal Desktop Core Configuration (FDCC) or United States Government Configuration Baseline (USGCB) include strict security group policy settings. The Windows Firewall: Do not Allow Exceptions group policy configures Windows Firewall to block all unsolicited incoming messages, including configured exceptions. This setting overrides all configured exceptions. For VCM to communicate properly with the VCM Agent on managed machines in strict, secure environments, disable the Windows Firewall: Do not Allow Exceptions group policy on the managed machines. For more information, see support.microsoft.com.

Prerequisites

- License the domain controllers on which you install the Agent. See "License Domain Controllers" on page 212.
- Verify that you know the communication protocols and ports that are used by the Collector and the Agents.
Procedure

1. Click Administration.
2. Select Machines Manager > Licensed Machines > Licensed Windows Machines.
3. In the data grid, select one or more domain controllers on which to install the Agent and click Install.
4. On the Machines page, verify that the target machines appear in the Selected list and click Next.
5. On the Install Options page, select the default installation options and click Next.
   You can schedule subsequent Agent installations to run later.
6. On the Schedule page, select Run Action now and click Next.

What to do next

- Verify that jobs have finished running. Click Administration and select Job Manager > History > Other Jobs > Past 24 Hours.
- Collect Windows data from VCM managed domain controllers in your environment. See "Collect Domain Controller Data" on page 214.

Collect Domain Controller Data

Start managing the domain controllers by performing an initial collection, which adds domain controller data to VCM.

Use the default filter set to collect a general view of the domain controllers in your environment. The first time that you use the default filter to collect data, the Windows Agent returns all of the data specified in the filter and stores the data in the VCM database. All subsequent collections will return a delta against the data previously collected.

A delta collection includes only the differences between the data on the target machine and the data stored in the VCM database. If you need a full collection, you can specify that VCM collect all data again. A full collection can take a significant amount of time depending on the number of VCM managed domain controllers from which you are collecting.

When you perform a full collection from your entire environment, run the collection during nonworking hours so that users do not notice any performance impact on managed machines. After the initial collection is finished, subsequent delta collections will most likely not impact performance.

Prerequisites

- To collect data from Windows XP SP2 or Vista machines that use DCOM communication, you must enable ICMP pings in the firewall settings or disable ICMP pings in VCM.
- Verify that DCOM is enabled on the managed machine. Run dcomcnfg and select Enable Distributed COM on this computer.
Procedure
1. On the VCM toolbar, click Collect.
2. On the Collection Type page, select Machine Data and click OK.
3. On the Machines page, select the domain controllers from which to collect data and click Next.
   To move all visible domain controllers to the selection window, use the double arrow.
4. Select the Do not limit collection to deltas check box.
   This option ensures that a full collection occurs during the initial set up of VCM for Active Directory.
5. On the Data Types page, select Machines.
6. Select Use default filters and click Next.
7. On the Important page, resolve any conflicts and click Finish.

What to do next

Configure VCM for Active Directory as an Additional Product
After VCM has discovered, licensed, and installed the Windows Agent on your domain controllers, configure VCM for Active Directory as an additional product. Configuring VCM for Active Directory provides the mechanism that allows VCM to manage the Active Directory forests and collect detailed schema information.

Procedure
1. "Install VCM for Active Directory on the Domain Controllers" on page 215
   To use VCM to collect Active Directory data from your environment, install VCM for Active Directory on your domain controllers.
2. "Run the Determine Forest Action" on page 216
   VCM for Active Directory requires a forest determination for all domain controllers so that it can proceed with schema and structure collection.
3. "Run the Domain Controller Setup Action" on page 217
   VCM for Active Directory collects your Active Directory schema and structure as part of the domain controller setup action.

Install VCM for Active Directory on the Domain Controllers
To use VCM to collect Active Directory data from your environment, install VCM for Active Directory on your domain controllers.

VCM for Active Directory will operate with only a single domain controller configured with VCM for Active Directory, which will serve as both the forest data source (FDS) and replication data source (RDS). However, to collect important nonreplicated attributes such as Last Logon, install VCM for Active Directory on as many domain controllers as possible.
Prerequisites

- Discover, license, and install the VCM Windows Agent on your domain controllers. See "Configure Domain Controllers" on page 209.
- Verify that jobs have finished running. Click Administration and select Job Manager > History > Other Jobs > Past 24 Hours.

Procedure

1. Click Administration.
2. Select Machines Manager > Additional Components > VCM for Active Directory.
3. Click Install.
4. Move the domain controllers on which to install VCM for Active Directory to the lower pane.
5. Click Next.
6. Verify that Run Action now is selected and click Finish.

If you add future Active Directory machines to your environment, configure them with VCM for Active Directory by running the following installer.

Program Files (x86)\VMware\VCM\AgentFiles\ADProductInstall.exe

What to do next

Determine the Active Directory forest in your environment. See "Run the Determine Forest Action" on page 216.

Run the Determine Forest Action

VCM for Active Directory requires a forest determination for all domain controllers so that it can proceed with schema and structure collection.

Prerequisites

- Install VCM for Active Directory on your domain controllers. See "Install VCM for Active Directory on the Domain Controllers" on page 215.
- Verify that jobs have finished running. Click Administration and select Job Manager > History > Other Jobs > Past 24 Hours.

Procedure

1. Click Administration.
2. Select Machines Manager > Additional Components > VCM for Active Directory.
3. Click Determine Forest.
4. Move the domain controllers on which to determine the forest to the lower pane.
   Determine the forest for all available domain controllers.
5. Click Next.
6. Click Finish.

What to do next

Run the domain controller setup action and identify your FDS and RDS. See "Run the Domain Controller Setup Action" on page 217.
Run the Domain Controller Setup Action

VCM for Active Directory collects your Active Directory schema and structure as part of the domain controller setup action.

During setup, you select a Forest Data Source (FDS) and Replication Data Source (RDS). Select machines that have reliable connections and availability. The same domain controller is allowed to serve as both FDS and RDS.

- **FDS:** VCM for Active Directory uses the FDS as a resource for all Forest-level information. You identify one FDS for each Forest.

- **RDS:** The RDS supplies all replicated data to VCM for Active Directory. You identify only one RDS for each domain so that collections on replicated attributes are performed only on a single domain controller. Other domain controllers that have VCM for Active Directory installed are accessed only during collection of nonreplicated attributes.

If you change your RDS, VCM for Active Directory does not purge data collected from the old RDS. The data is refreshed when you run a new collection using the new RDS.

**Prerequisites**

- Use VCM for Active Directory to determine the Forest. See "Run the Determine Forest Action" on page 216.

- Verify that jobs have finished running. Click Administration and select Job Manager > History > Other Jobs > Past 24 Hours.

**Procedure**

1. Click Administration.
2. Select Machines Manager > Additional Components > VCM for Active Directory.
3. Click Setup DCs.
4. Select an FDS for each forest and click Next.
5. Select an RDS for each domain and click Next.
6. Click Finish.

When the Setup DCs action finishes, VCM for Active Directory initiates the following jobs.

- Active Directory schema collection
- Active Directory specifier collection
- Active Directory structure collection

The information obtained from the third collection identifies the organizational unit (OU) structure that supports the use of VCM for Active Directory. To view information, click Administration, and select Machines Manager > Additional Components > VCM for Active Directory.

**What to do next**

Collect Active Directory data. See "Collect Active Directory Data " on page 217.

Collect Active Directory Data

Perform your first collection of Active Directory objects by launching the same collection wizard that you use for Windows and UNIX/Linux collections. The first time you run an Active Directory collection, the Agent returns all objects and attributes from your selected Active Directory environment.
Prerequisites

- Verify that jobs have finished by clicking Administration and selecting Job Manager > History > Other Jobs > Past 24 Hours.

Procedure

1. From the toolbar, click Collect.
2. On the Collection Type page, select Active Directory and click OK.
3. On the AD Collection Options page, click Select Data Types to collect from these machines.
4. To ensure that a full collection occurs, select the Do not limit collection to deltas check box and click Next.
5. On the Data Types page, click Select All.
6. Select the Use default filters option and click Next.
7. On the Location page, click the ellipsis button (...).
8. On the Select an AD Location page, expand the Enterprise tree, select an Active Directory Location, and click OK.
10. Click Finish.

What to do next

Explore initial Active Directory collection results. See "Active Directory Collection Results" on page 218.

Active Directory Collection Results

After you collect the initial Active Directory data, explore the results under Active Directory, Reports, and Compliance.

Displayed information is only as current as the last time that you collected Active Directory data.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Provides summary and day-to-day information about your Active Directory</td>
</tr>
<tr>
<td>Dashboard</td>
<td>environment in a graphical format.</td>
</tr>
<tr>
<td></td>
<td>To view the dashboard, click Active Directory and select Dashboards &gt;</td>
</tr>
<tr>
<td></td>
<td>Managed Objects.</td>
</tr>
<tr>
<td></td>
<td>Several Active Directory Dashboards are available.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Provides summary information about your Active Directory environment</td>
</tr>
<tr>
<td>Object Summary</td>
<td>in a textual format.</td>
</tr>
<tr>
<td></td>
<td>To view the summary reports, click Active Directory and select Objects</td>
</tr>
<tr>
<td></td>
<td>&gt; object-type.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Provides the detailed information behind the summary for your Active</td>
</tr>
<tr>
<td>Object Detail</td>
<td>Directory environment.</td>
</tr>
<tr>
<td></td>
<td>To view the detailed information, click Active Directory and select Objects</td>
</tr>
<tr>
<td></td>
<td>&gt; object-type. Click the View data grid button.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>From the data grid view, you can enable or disable the summary to view the details immediately.</td>
<td></td>
</tr>
</tbody>
</table>

**Reports**

- Provides Active Directory information by running preconfigured or custom reports against the latest collected data. The time needed for a report to generate depends on the volume or complexity of the data requested.
  - To use the reporting options, click **Reports** and expand **Active Directory Reports**.

**Compliance**

- Provides preconfigured Active Directory compliance rules and templates, which allow you to check the collected data against specific values.
  - To view Active Directory compliance rules, click **Compliance** and select **Active Directory Compliance > Rule Groups**.
  - To view Active Directory compliance templates, click **Compliance** and select **Active Directory Compliance > Templates**.
The VCM Remote client is the communication and management mechanism that you use to manage mobile Windows machines as they connect to and disconnect from the network.

For Windows machines that are not continuously connected to the network, the VCM Remote client listens for network events indicating it has access to the VCM Remote-related components on the VCM Internet Information Services (IIS) server. Based on the configured settings, the Collector creates requests, such as a collection request, for the remote machine that has just become available online.

**VCM Remote Management Workflow**

To indicate the presence of the mobile Windows machine on your network, the VCM Remote client sends an HTML POST file over HTTP to a server-side component residing on the VCM Internet Information Services (IIS) server. Based on user-defined settings, the Collector auto-licenses the remote machine, installs or upgrades the VCM Windows Agent, and determines whether it should submit a collection job for that remote machine.

The Collector batches the requests and processes them at periodic intervals. This batch processing manages the problem of having 15,000 clients come online within a short time of one another and creating 15,000 individual requests.

**Configuring VCM Remote Connection Types**

The VCM Remote client accommodates three connection methods, including broadband, dial-up, and LAN, for Windows machines that do not have a continuous connection to the network.

To optimize the collection of the Windows machine data, you configure different collection filters for different connection types based on general bandwidth for each connection type.

- **Broadband:** DSL and cable connections can be 156Kb to more than 1Mb.
- **Dial-up:** A dial-up connection can be 56Kb or less.
- **LAN:** A local area connection to the network equal to or greater than 1Mb. A VPN connection might be available at LAN speeds but connected over the Internet.

For each connection type, you assign a customized collection filter set. For example, when a remote machine connects using a dial-up connection, you use a collection filter set that collects only key data compared to a filter set for LAN connections that collects more data from the target machines.
Using Certificates With VCM Remote

The use of certificates with VCM Remote ensures secure communication between VCM and the VCM Remote client when they are communicating outside your internal network.

The communication between the Collector and the VCM Remote client is secured using Transport Layer Security (TLS) certificates. You can use the VCM certificate or you can use an existing Enterprise certificate.

- **VCM Certificate**: A certificate generated during the installation of VCM. The VCM certificate is located on the Collector at [install path]\VMware\VCM\CollectorData. You must copy the .pem file to each target machine.

- **Enterprise Certificate**: A certificate already in the certificate store in your environment.

Determine the certificate that you are using to validate communication, either a VCM-generated or a Enterprise certificate in certificate store. By default, the installation of a Windows VCM Agent in HTTP mode adds the Collector’s Enterprise Certificate to the certificate store of the client system. The VCM Remote client can also use this certificate.

After you install the VCM Remote client, the first time the remote machine connects the Collector network, it requests a Collector certificate. If the Collector certificate is trusted by the Enterprise certificate on the client, the Collector certificate is added to the client's certificate store.

Configure and Install the VCM Remote Client

You configure the VCM Remote client server-side communication settings and then install the client on target Windows machines. After it is installed, the VCM Remote client manages the communication with VCM when the remote machine is connected to the network.

**Procedure**

1. "Configure the VCM Remote Settings" on page 222
   You create custom filter sets for each communication method and configure the settings to ensure efficient on-going management of the mobile Windows machines managed using the VCM Remote client.

2. "Install the VCM Remote Client" on page 225
   You install the VCM Remote client on the target Windows machines that are not continuously connected to the network.

3. "Connect VCM Remote Client Machines to the Network" on page 232
   Connect your remote machine to the VCM-managed network to begin managing the machine. The VCM Remote client notifies VCM that the remote machine is on the network and it is processed based on VCM Remote settings and requires no user interaction.

When you configure Windows machines with the VCM Remote client, the client handles the communication when the remote machine connects to the network, but the machines are managed as Windows machines. See "VCM Remote Collection Results" on page 232.

Configure the VCM Remote Settings

You create custom filter sets for each communication method and configure the settings to ensure efficient on-going management of the mobile Windows machines managed using the VCM Remote client.
Create Custom Collection Filter Sets

You create custom collection filter sets for Dial-up, Broadband, or LAN connections to efficiently manage mobile machines using the VCM Remote client. To optimize results, create a different filter set for each connection type.

With filter sets based on connection type rather than using the default filter set, you can optimize collections based on the stability and speed of the connection. For example, an all encompassing collection is difficult to complete over a dial-up connection. To optimize the collection performance, create a dial-up filter set that is limited to a few high-importance data types and does not include the File System Uploads or Emergency Repair Disk data types.

Prerequisites

Review the purpose of the different connection types to understand what to include or exclude from your collection filter sets. See "Configuring VCM Remote Connection Types" on page 221.

Procedure

1. Click Administration.
2. Select Collection Filters > Filter Sets.
3. On the Collection Filter Sets data grid, click Add Filter Set.
4. On the Name and Description page, type a Name and Description.
   For example, use names similar to Remote Client - Broadband, Remote Client - LAN, and Remote Client - Dial-up.
5. Select Filter Set and click Next.
6. On the Filters page, select Machine Based Filter Set.
7. Select the filters to include in the filter set and click Next.
8. On the Conflicts page, resolve any data type conflicts and click Next.
9. On the Important page, review the summary information and click Finish.
What to do next

- Repeat the procedure for all the connection types for which you configure filter sets.
- Assign the filter sets to the appropriate VCM Remote settings. See "Specify Custom Filter Sets in the VCM Remote Settings" on page 224.

Specify Custom Filter Sets in the VCM Remote Settings

VCM Remote supports three connection types: broadband, dial-up, and LAN. To optimize the collection of data, you must specify the collection filter set for each connection used in your environment.

When a mobile Windows machine connects to the network using one of three connection types and the VCM Remote client indicates the presence of the machine, VCM determines the connection type and uses the collection filter specified for the connection when collecting data from the target machine. This method enables mobile VCM Remote client machines to connect using any of the connection types and to collect data using a filter set optimized for the connection type.

Prerequisites

Create VCM Remote collection filter sets, one for each connection type. See "Create Custom Collection Filter Sets" on page 223.

Procedure

1. Click Administration.
2. Select Settings > General Settings > VCM Remote.
3. On the VCM Remote Settings data grid, select each setting separately and click Edit Settings.
   - Name of the Collection Filter Set Remote will use for Broadband connections
   - Name of the Collection Filter Set Remote will use for Dialup connections
   - Name of the Collection Filter Set Remote will use for LAN connections
4. On the Edit Settings page, select the related filter set in the drop-down menu and click Next.
5. On the Important page, review the summary and click Finish.

What to do next

- Repeat the procedure for the other settings.
- Configure the Agent and host file settings. See "Specify Agent and Host File Settings" on page 224.

Specify Agent and Host File Settings

To ensure the VCM Remote client efficiently installs or upgrades the Agent and manages communication, you must configure the server settings on the Collector.
Procedure

1. Click Administration.
2. Select Settings > General Settings > VCM Remote.
3. On the VCM Remote Settings data grid, select each setting separately and click Edit Settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should Remote automatically install an Agent to the client (if required)?</td>
<td>Click Yes. Allows VCM to install the Agent when contacted by the VCM Remote client the first time.</td>
</tr>
<tr>
<td>Should Remote automatically upgrade an Agent to the client (if required)?</td>
<td>Click Yes. Allows VCM to upgrade the Agent when contacted by the VCM Remote client.</td>
</tr>
<tr>
<td>Will IP Address of calling client be added to local host file?</td>
<td>Click Yes. Adds the IP address of the VCM Remote client to the host file to ensure that the remote client name is resolved and updated so that communication can begin.</td>
</tr>
<tr>
<td>Minutes to retain host File Entry</td>
<td>Type 30 or greater to specify 30 minutes or longer. Retains the IP address of the VCM Remote client in the host file for the set time to ensure that the remote client name is quickly resolved and updated during that time.</td>
</tr>
</tbody>
</table>

4. Configure the setting and click Next.
5. On the Important page, review the summary and click Finish.

What to do next

- Repeat procedure for the other settings on the VCM Remote Settings data grid.
- Install the VCM Remote client. See “Install the VCM Remote Client” on page 225.

Install the VCM Remote Client

You install the VCM Remote client on the target Windows machines that are not continuously connected to the network.

To install the VCM Remote client, use the method easiest to implement depending on your access to the target machines and the number of remote machines on which you are installing the client.
"Install the VCM Remote Client Manually" on page 226

The manual installation of the VCM Remote client is a wizard-based process that you use when you have direct access to the target machines. This process is a useful way to install the client if you are creating an image to install on other machines.

"Install the VCM Remote Client Using a Command Line" on page 227

You use the command line to install the VCM Remote client when you want to run an unattended installation using Group Policy or software provisioning.

"Install the VCM Remote Client Using Windows Remote Commands" on page 229

You use the Windows remote commands to deploy the VCM Remote client to multiple machines in your environment. The VCM Agent must be installed on the target machines.

Install the VCM Remote Client Manually

The manual installation of the VCM Remote client is a wizard-based process that you use when you have direct access to the target machines. This process is a useful way to install the client if you are creating an image to install on other machines.

Prerequisites

Determine the certificate that you are using to validate communication between the client and the Collector. See "Using Certificates With VCM Remote" on page 222.

Procedure

1. On the target machine, create a folder and copy the files from the Collector to the target folder.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM Remote Client.msi</td>
<td>Located on the Collector at [install path] \VMware\VCM\AgentFiles.</td>
</tr>
<tr>
<td>CM_Enterprise_Certificate_</td>
<td>(Optional) Located on the Collector at [install path] \VMware\VCM\CollectorData.</td>
</tr>
<tr>
<td>xxx.pem</td>
<td>Copy the file if you do not have or are not using the Enterprise certificate located in the remote machine's certificate store.</td>
</tr>
</tbody>
</table>

2. On the target machine, double-click the CM Remote Client.msi file.

3. On the VCM Remote Client Setup page, click Next.

4. On the Installation Folder page, accept the default installation location or click Change to enter a different location, and click Next.
5. On the VCM Remote Client Information page, configure the options and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Machine Name</td>
<td>Name of the Windows machine on which the VCM Collector and Microsoft IIS are installed.</td>
</tr>
<tr>
<td>Path to ASP Page</td>
<td>Path for the IIS default VCM Remote Web site. The <code>&lt;virtual directory name&gt;</code> must match the virtual directory name as it appears in the Collector's IIS. The default value is VCMRemote.</td>
</tr>
</tbody>
</table>

6. On the Select Certificates page, configure the certificate option that supports your environment and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate File</td>
<td>Browse to the location of the VCM-generated .pem file you copied from the Collector.</td>
</tr>
<tr>
<td>Skip Certificate Deployment</td>
<td>Select the option to use the existing Enterprise certificate in the client certificate store.</td>
</tr>
</tbody>
</table>

7. On the Ready to install CM Remote Client page, click **Install**.

8. Click **Finish** when the installation is completed.

**What to do next**

Connect the remote machine to the network to ensure that VCM completes the installation process. See “Connect VCM Remote Client Machines to the Network” on page 232

**Install the VCM Remote Client Using a Command Line**

You use the command line to install the VCM Remote client when you want to run an unattended installation using Group Policy or software provisioning.

**Prerequisites**

Determine the certificate that you are using to validate communication between the client and the Collector. See “Using Certificates With VCM Remote” on page 222.
Procedure

1. On the target machine, create a folder and copy the files from the Collector to the target folder.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM Remote Client.msi</td>
<td>Located on the Collector at [install path] \VMware\VCM\AgentFiles.</td>
</tr>
<tr>
<td>CM_Enterprise_Certificate_***.pem</td>
<td>(Optional) Located on the Collector at [install path] \VMware\VCM\CollectorData. Copy the file if you do not have or are not using the Enterprise certificate located in the remote machine's certificate store.</td>
</tr>
</tbody>
</table>

2. At a command prompt, edit the installation command for your environment, and run the command.

   If the names and paths contain spaces, you must use double quotation marks.

   msiexec.exe /qn /i "[path]\cm remote client.msi" COLLECTOR="YourCollectorName" PATHTOASP="VCMRemote/ecmremotehttp.asp" INSTALLDIR="c:\Program Files (x86) \VMware\VCM Remote Client" CERTIFICATE_FILE="[path]\YourEnterpriseCertificateName.pem" /l*v "[path]\filename.log"

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/qn</td>
<td>No error messages appear during installation.</td>
</tr>
<tr>
<td>[path]\cm remote client.msi</td>
<td>Path to the CM Remote Client.msi on the target machine.</td>
</tr>
<tr>
<td>COLLECTOR=YourCollectorName</td>
<td>Replace &lt;YourCollectorName&gt; with the name of your VCM Collector.</td>
</tr>
<tr>
<td>PATHTOASP=VCMRemote/ecmremotehttp.asp</td>
<td>Path to the IIS Default Web Site virtual directory containing ecmremotehttp.asp.</td>
</tr>
<tr>
<td>INSTALLDIR=c:\Program Files (x86) \VMware\CM Remote Client</td>
<td>Path where you want the VCM Remote client files installed. The directory is created by the command.</td>
</tr>
<tr>
<td>CERTIFICATE_FILE=[path]\YourEnterpriseCertificateName.pem</td>
<td>Certificate path and name on the target machine. If you are using an existing Enterprise certificate in the client certificate store, you use SKIP_CERTIFICATE_FILE=1 instead of CERTIFICATE_FILE=[path]\YourEnterpriseCertificateName.pem. If the certificate does not exist in the store, any communication between the client and the Collector will fail.</td>
</tr>
<tr>
<td>/l*v [path]\filename.log</td>
<td>Error messages added to the log file in the specified path. If the path is not specified, the log file is saved in the directory from which the msiexec.exe was run.</td>
</tr>
</tbody>
</table>
**What to do next**

Connect the remote machine to the network to ensure that VCM completes the installation process. See "Connect VCM Remote Client Machines to the Network" on page 232.

**Install the VCM Remote Client Using Windows Remote Commands**

You use the Windows remote commands to deploy the VCM Remote client to multiple machines in your environment. The VCM Agent must be installed on the target machines.

The script installs the VCM Remote client under the Windows directory rather than the Program Files directory. It is not necessary to create the install directory on the target machine before you run the script.

**Prerequisites**

- Verify that the Agent is installed on target machines. See "Configure Windows Machines" on page 87.
- Identify the certificate you are using to validate communication between the client and the Collector. See "Using Certificates With VCM Remote" on page 222.

**Procedure**

1. On your Collector, copy [install path]\Enterprise Configuration Manager\AgentFiles\CM Remote Client.msi to [install path]\Enterprise Configuration Manager\WebConsole\L1033\Files\Remote_Command_Files.

2. On your Collector, copy [install path]\Enterprise Configuration Manager\CollectorData\<YourEnterpriseCertificate>.pem to [install path]\Enterprise Configuration Manager\WebConsole\L1033\Files\Remote_Command_Files.

3. In VCM, select Console > Windows Remote Commands.

4. On the data grid toolbar, click Add.

5. On the Name and Description page, type a unique name and description for the command, and click Next.


   a. In the Type drop-down menu, select VBScript.

   b. In Command Text text box, copy and paste the script and modify it as specified in the script comments.

   ```vbscript
   Call DoWork
   'Copyright 1999-2010 VMware, Inc.
   'Coded by Ryan L.
   'Description: Installs VCM Remote ver. 2
   'Modified 4/27/2008 - Stephen S. Included Certificate file options
   'Modified 7/7/2010 - VCM
   Dim sCollName, sInstallDir, sVirDir, sAddRemove, sCertFile, bInstallCert
   Sub DoWork()
   Set WshShell = CreateObject("WScript.Shell")
   sCollName = "YourCollectorName" 'Name of your VCM Collector machine in quotes
   ```

   ```vbscript
   Call DoWork()
   ```
bInstallCert = 1 'If the value is 1, the Enterprise Certificate is installed. If the value is set to 0, the installation of the certificate is skipped and it is assumed that the certificate is already present. The Remote Client will NOT function until the Enterprise Certificate is installed as specified in Step 2

cCertFile = "EnterpriseCert" 'The filename of your enterprise certificate (.pem file) as identified in Step 2

sVirDir = "VCMRemote/EcmRemoteHttp.asp" 'Where you replace CMRemote with the IIS Default Web Site virtual directory containing the ECMRemoteHTTP.asp file

sInstallDir = WshShell.ExpandEnvironmentStrings("%windir%") & "\VMware\VCM Remote Client" 'The installation directory on the TARGET machine

sAddRemove = 1 'Whether or not VCM remote should appear in the Add/Remove programs List, should be 0 = hide, 1 = show

sMSIPackageName = "CM Remote Client.msi" 'Name of the MSI package that installs VCM Remote Agent

CheckVars

If sAddRemove = 0 Then

    AppToRun = "msiexec.exe /qn /i " & Chr(34) &
    EcmAgtContext.JobDownloadDirectory & "\" & sMSIPackageName & Chr(34) & " ALLUSERS=1 COLLECTOR=" & Chr(34) & sCollName & Chr(34) & " PATHTOASP=" & Chr(34) & sVirDir & Chr(34) & " ARPSYSTEMCOMPONENT=" & sAddRemove & " INSTALLDIR=" & Chr(34) & sInstallDir & Chr(34)

Else

    AppToRun = "msiexec.exe /qn /i " & Chr(34) &
    EcmAgtContext.JobDownloadDirectory & "\" & sMSIPackageName & Chr(34) & " ALLUSERS=1 COLLECTOR=" & Chr(34) & sCollName & Chr(34) & " PATHTOASP=" & Chr(34) & sVirDir & Chr(34) & " INSTALLDIR=" & Chr(34) & sInstallDir & Chr(34)

End If

If bInstallCert = 1 Then

    AppToRun = AppToRun & " CERTIFICATE_FILE=" & Chr(34) &
    EcmAgtContext.JobDownloadDirectory & "\" & sCertFile & Chr(34)

Else

    AppToRun = AppToRun & "SKIP_CERTIFICATE_FILE=1"

End If

EcmScriptRuntime.CmdExecute Chr(34) & AppToRun & Chr(34), 10000

End Sub
Sub CheckVars()
If sCollName = "" Then
  WScript.Quit
Else
  sCollName = Trim(sCollName)
End If

If sVirDir = "" Then
  sVirDir = "vcmremote/ecmremotehttp.asp"
Else
  sVirDir = Trim(sVirDir)
End If

If sInstallDir = "" Then
  sInstallDir = "c:\vcm remote client"
Else
  sInstallDir = Trim(sInstallDir)
End If

If sAddRemove <> 0 And sAddRemove <> 1 Then
  sAddRemove = 1 'Set whether or not VCM Remote appears in the Add/Remove programs list. 1=display, 0=do not display
End If

If sAddRemove = "" Then
  sAddRemove = 1
End If

If IsNumeric(sAddRemove) = False Then
  sAddRemove = 1
End If

sAddRemove = Trim(sAddRemove)
End Sub
c. Select the Certain file(s) are required to be on the target machine for this remote command check box.
d. Click Next.

7. On the Files page, move the CM Remote Client.msi file and the .pem file to the list on the right, and click Next.

8. On the Important page, review and summary and click Finish.

   VCM saves and adds the command to Windows Remote Commands list.


10. On the Machines page, select the Windows machines on which you are installing VCM Remote.

11. On the Schedule page, select when to run the installation and click Next.

   If you are running the installation command on many Windows machines at one time, schedule the installation for nonpeak network hours.

12. On the Important page, review the summary to verify the number of target machines and click Finish.

What to do next

- Verify that the installation is finished. To view the status of the Install CM Remote Client job, click Administration and select Job Manager > History > Instant Collections.

- Connect the remote machine to the network to ensure that VCM completes the installation process. See "Connect VCM Remote Client Machines to the Network" on page 232

**Connect VCM Remote Client Machines to the Network**

Connect your remote machine to the VCM-managed network to begin managing the machine. The VCM Remote client notifies VCM that the remote machine is on the network and it is processed based on VCM Remote settings and requires no user interaction.

**Prerequisites**

- Configure the VCM Remote server settings. See "Configure the VCM Remote Settings" on page 222.

- Install the VCM Remote client on target machines. See "Install the VCM Remote Client" on page 225.

**Procedure**

1. Connect the remote machines to the VCM managed network.

   VCM Remote client sends a POST request to the VCM IIS server indicating its presence on the network. The Collector processes the request, auto-licenses the remote machine, installs or upgrades the VCM Windows Agent, and determines whether it should submit a collection job for that remote machine.

What to do next

Review the collected data. See "VCM Remote Collection Results" on page 232.

**VCM Remote Collection Results**

The VCM Remote client-specific data is limited to administrative details. All other data collected from the remote machine appears in VCM as Windows machine data. See "Windows Collection Results" on page 98.

The displayed data is only as current as the last time you collected from the remote machines.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>View administrative details about the VCM Remote client.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>-</td>
<td>To view the installed Remote client version, click <strong>Administration</strong> and select <strong>Machines Manager &gt; Licensed Machines &gt; Licensed Windows Machines</strong>. The Remote Client Version appears in the data grid.</td>
</tr>
<tr>
<td>-</td>
<td>To view the status of remote collection jobs, click <strong>Administration</strong> and select <strong>Job Manager &gt; History &gt; VCM Remote</strong>.</td>
</tr>
</tbody>
</table>
VCM management extensions for assets integrates and manages hardware and software asset data that is not gathered through the automated managed machine collection processes of VCM.

- **Hardware**: VCM for assets stores supplemental information (data that is not automatically collected) about physical and virtual machines that are managed by VCM. In addition, VCM for assets stores data about non-managed enterprise equipment such as printers, mobile devices, routers, and so on.

- **Software**: VCM for assets can collect and store information about the software that is installed on physical and virtual machines managed by VCM.

VCM users view the asset data in the VCM Console, where, depending on assigned role, users might also have edit permission.

This chapter includes the following topics:

- Configure Asset Data Fields
- Configure Asset Data Values for VCM Machines
- Configure Asset Data for Other Hardware Devices
- Configure Asset Data for Software

**Configure Asset Data Fields**

An administrator must configure VCM for assets so that it includes the columns of data that apply to the hardware and software assets in your environment.

**Procedure**

1. "Review Available Asset Data Fields" on page 236
   
   VCM for assets is populated with a short list of data fields to get you started.

2. "Add an Asset Data Field" on page 236
   
   You can add any data that you want to store and manage about your hardware or software.

3. "Edit an Asset Data Field" on page 237
   
   Change VCM for assets data fields to keep up with your tracking and management needs for hardware or software.

4. "Delete a VCM for Assets Data Field" on page 238
   
   Remove asset data fields that do not serve a purpose in your environment.

5. "Change the Order of Asset Data Columns" on page 238
Changing the order of the VCM for assets data field list changes the order of columns when you view asset data in the VCM Console.

6. "Refresh Dynamic Asset Data Fields” on page 239

You can force VCM for assets to refresh the values in all fields that are configured to populate dynamically.

**Review Available Asset Data Fields**

VCM for assets is populated with a short list of data fields to get you started. Examples include hardware data such as location or contact person, and software data such as license expiration date or number of copies.

VCM for assets is configurable, so review the data fields and the order in which they appear. You have the opportunity to add, modify, remove, and rearrange fields.

**Prerequisites**

- Log in to VCM using an account with the Administrator role.
- Identify the asset data that you want to store about your hardware or software.

**Procedure**

1. Click Administration.
2. Select Settings > Asset Extensions Settings.
3. Select one of the following nodes.
   - Hardware Configuration Items > Other Devices
   - Hardware Configuration Items > VCM Devices
   - Software Configuration Items
4. In the data grid, review the names and descriptions.
   
   Each row, in order, becomes a column in the asset data display in the VCM Web Console.

**What to do next**

Supplement the populated data fields by adding more. See "Add an Asset Data Field” on page 236.

**Add an Asset Data Field**

You can add any data that you want to store and manage about your hardware or software.

**Prerequisites**

- Log in to VCM using an account with the Administrator role.
- Identify the asset data that you want to store about your hardware or software.

**Procedure**

1. Click Administration.
2. Select Settings > Asset Extensions Settings.
3. Select one of the following nodes.
   - Hardware Configuration Items > Other Devices
   - Hardware Configuration Items > VCM Devices
   - Software Configuration Items
4. Click Add.

5. Type a name and description for the new asset data field and click Next.

   The name is the column heading that appears when users view the data in the VCM Console.

6. Specify properties about the new data.
   a. Select the way to populate the data.
      - Manually: type free-form text
      - Lookup: select from a fixed or query-based list of values
      - Dynamically: query from other data
   b. Select the data type.

      For string data, also enter the maximum number of characters to allow.

7. Click Next.

8. Configure the way to populate the data based on your earlier selection.
   - Manually: No configuration steps are needed. The user types the data at runtime.
   - Lookup, fixed: Create the fixed list by typing values and clicking Add. When finished, click Next.
   - Lookup, query-based: Type the SQL query that populates the list from which to select values, and click Next.
   - Dynamically: Type the SQL query that pulls the value from another data source, and click Next.

9. Select the roles that are allowed to edit the data.

   Only users assigned to these roles can edit the data using the VCM Console.

10. Review the settings and click Finish.

What to do next

Modify fields that need to be adapted for your site. See "Edit an Asset Data Field" on page 237.

Edit an Asset Data Field

Change VCM for assets data fields to keep up with your tracking and management needs for hardware or software.

Prerequisites
   - Log in to VCM using an account with the Administrator role.
   - Identify the asset data that you want to store about your hardware or software.

Procedure
   1. Click Administration.
   2. Select Settings > Asset Extensions Settings.
   3. Select one of the following nodes.
      - Hardware Configuration Items > Other Devices
      - Hardware Configuration Items > VCM Devices
      - Software Configuration Items
   4. In the data grid, select the row.
   5. Click Edit.
6. Change the name or description for the data field and click Next.
   The name is the column heading that appears when users view the data in the VCM Console.

7. Click Next.
   You cannot change the data properties.

8. Click Next.

9. Select the roles that are allowed to edit the data.
   Only users assigned to these roles can edit the data using the VCM Console.

10. Review the settings and click Finish.

**What to do next**
Remove unwanted fields. See "Delete a VCM for Assets Data Field" on page 238.

**Delete a VCM for Assets Data Field**
Remove asset data fields that do not serve a purpose in your environment.

**Prerequisites**
- Log in to VCM using an account with the Administrator role.
- Identify the asset data that you want to store about your hardware or software.

**Procedure**
1. Click Administration.
2. Select Settings > Asset Extensions Settings.
3. Select one of the following nodes.
   - Hardware Configuration Items > Other Devices
   - Hardware Configuration Items > VCM Devices
   - Software Configuration Items
4. In the data grid, select the row.
5. Click Delete.
   You cannot delete entries that are marked with a lock icon.
6. Click OK.

**What to do next**
Rearrange asset data fields so that the order of columns shown in the VCM Console meets your requirements. See "Change the Order of Asset Data Columns" on page 238.

**Change the Order of Asset Data Columns**
Changing the order of the VCM for assets data field list changes the order of columns when you view asset data in the VCM Console.

**Prerequisites**
- Log in to VCM using an account with the Administrator role.
- Identify the asset data that you want to store about your hardware or software.
Procedure
1. Click Administration.
2. Select Settings > Asset Extensions Settings.
3. Select one of the following nodes.
   - Hardware Configuration Items > Other Devices
   - Hardware Configuration Items > VCM Devices
   - Software Configuration Items
   In the data grid, each row, in order, becomes a column in the asset data display in the VCM Console.
4. Click Column Order.
5. Select entries, use the arrow buttons to move rows up or down, and click Next.
6. Review the rearranged order and click Finish.

What to do next
Refresh the values in dynamically generated fields. See "Refresh Dynamic Asset Data Fields" on page 239.

Refresh Dynamic Asset Data Fields
You can force VCM for assets to refresh the values in all fields that are configured to populate dynamically.

Prerequisites
Log in to VCM using an account with the Administrator role.

Procedure
1. Click Administration.
2. Select Settings > Asset Extensions Settings.
3. Select one of the following nodes.
   - Hardware Configuration Items > Other Devices
   - Hardware Configuration Items > VCM Devices
   - Software Configuration Items
4. Click Refresh Dynamic Fields.
   The option recalculates and overwrites all dynamic data fields listed and might take time to finish.
5. Click OK.

What to do next
Enter data for machines that are managed by VCM. See "Configure Asset Data Values for VCM Machines" on page 239.

Configure Asset Data Values for VCM Machines
Although the asset data for machines that are managed by VCM is collected, you can customize some data through VCM for assets.

Prerequisites
Log in to VCM with a role that has edit permission for asset configuration data.
Procedure
1. Click Console.
2. Select Asset Extensions > Hardware Configuration Items > VCM Devices.
3. In the data grid, select the VCM machine.
4. Click Edit Values.
5. Verify that the machine you want is in the Selected list and click Next.
   Use the arrow buttons to move entries to or from the Selected list.
6. Move the data fields that you want to edit into the Selected list and click Next.
   Use the arrow buttons to move entries to or from the Selected list.
7. Select or type the new values and click Next.
8. Review the new values and click Finish.

What to do next
Enter data for hardware that is not managed by VCM, such as printers, mobile devices, routers, and so on.
See "Configure Asset Data for Other Hardware Devices" on page 240.

Configure Asset Data for Other Hardware Devices
A user with a role that has permission to edit asset data can populate VCM for assets with the hardware devices in your environment that are not discovered and managed by VCM.

Procedure
- "Add Other Hardware Devices" on page 240
  Use VCM for assets to keep track of your non-VCM managed hardware by adding information about the hardware devices directly to VCM.
- "Add Multiple Similar Other Hardware Devices" on page 241
  If your site has many nearly identical devices, you can use VCM for assets to clone one copy as a way to quickly add records for the other devices.
- "Edit Asset Data for Other Hardware Devices" on page 241
  Use VCM for assets to change your hardware asset records as your enterprise changes.
- "Edit Asset Data Values for Other Hardware Devices" on page 242
  You can change only the details about a given piece of equipment when the long term information, such as the model name or number, is going to remain the same.
- "Delete Other Hardware Devices" on page 242
  Use VCM for assets to delete the records of hardware devices that are no longer a part of your site.

Add Other Hardware Devices
Use VCM for assets to keep track of your non-VCM managed hardware by adding information about the hardware devices directly to VCM.
Prerequisites

- Have an administrator configure the asset data fields that you need. See "Configure Asset Data Fields" on page 235.
- Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click Console.
2. Select Asset Extensions > Hardware Configuration Items > Other Devices.
3. Click Add.
4. Select or type the details that identify the device, such as its name and model, and click Next.
5. Select or type the values for the asset data associated with the device and click Next.
   The fields can vary depending on how the administrator configured your data for other hardware devices.
6. Click Finish.

Add Multiple Similar Other Hardware Devices

If your site has many nearly identical devices, you can use VCM for assets to clone one copy as a way to quickly add records for the other devices.

Prerequisites

- Log in to VCM with a role that has edit permission for asset configuration data.
- Create at least one copy of the device to serve as a baseline. See "Add Other Hardware Devices" on page 240.

Procedure

1. Click Console.
2. Select Asset Extensions > Hardware Configuration Items > Other Devices.
3. In the data grid, select the original, baseline asset.
4. Click Clone.
5. Modify the details to reflect the new copy of the asset and click Next.
   You must change at least the name.
6. Modify the values to reflect the asset data associated with the new device and click Next.
7. Click Finish.

Edit Asset Data for Other Hardware Devices

Use VCM for assets to change your hardware asset records as your enterprise changes.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.
Procedure

1. Click Console.
2. Select Asset Extensions > Hardware Configuration Items > Other Devices.
3. In the data grid, select the asset.
4. Click Edit.
5. Change the details that identify the device, such as its name and model, and click Next.
6. Change the values for the asset data associated with the device and click Next.
   The fields can vary depending on how the administrator configured your data for other hardware devices.
7. Click Finish.

Edit Asset Data Values for Other Hardware Devices

You can change only the details about a given piece of equipment when the long term information, such as the model name or number, is going to remain the same.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click Console.
2. Select Asset Extensions > Hardware Configuration Items > Other Devices.
3. In the data grid, select the asset.
4. Click Edit Values.
5. Move the data fields that you want to edit into the Selected list and click Next.
   Use the arrow buttons to move entries to or from the Selected list.
6. Select or type the new values and click Next.
7. Review the new values and click Finish.

Delete Other Hardware Devices

Use VCM for assets to delete the records of hardware devices that are no longer a part of your site.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click Console.
2. Select Asset Extensions > Hardware Configuration Items > Other Devices.
3. In the data grid, select the asset.
4. Click Delete.
5. Click OK.
Configure Asset Data for Software

A user with a role that has permission to edit asset data can use VCM for assets to gather information about the software on machines that are discovered and managed by VCM.

Procedure

- **"Add Software Assets" on page 243**
  
  Manage your software assets by having VCM for assets detect what is installed on the physical and virtual machines in your environment.

- **"Add Multiple Similar Software Assets" on page 244**
  
  If your environment has many nearly identical copies of software, such as the same application with a different license number, you can use VCM for assets to clone one copy as a way to quickly add records for the others.

- **"Edit Asset Data for Software" on page 245**
  
  Use VCM for assets to change your software asset records as your enterprise changes.

- **"Edit Asset Data Values for Software" on page 245**
  
  You can change the details about a specific copy of software when the long term information, such as the application name or version, is going to remain the same.

- **"Delete Software Data" on page 246**
  
  Use VCM for assets to delete entries for software that is no longer installed at your site.

Add Software Assets

Manage your software assets by having VCM for assets detect what is installed on the physical and virtual machines in your environment.

**Prerequisites**

- Have an administrator configure the asset data fields that you need. See **"Configure Asset Data Fields" on page 235**.

- Log in to VCM with a role that has edit permission for asset configuration data.

**Procedure**

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. Click **Add Software**.
4. Type a name and description and click **Next**.
5. Select the data type that VCM for assets will look for to detect the installed software and click **Next**.

   The options take you to custom wizard pages where you type or select what VCM for assets will look for in the database.
- **Software Inventory (Windows)**: Select a product from the software inventory (SI) list.
- **Registry (Windows)**: Type or select a Windows Registry path, key, and value.
- **File System - Known Files (Windows)**: Type or select a filename and version.
- **Software Inventory - Packages (UNIX)**: Select a product from the SI list.
- **Software Inventory - Utilities (UNIX)**: Select a product from the SI list.
- **File System - Known Files (UNIX)**: Type or select a filename.

6. Click Next.

7. Select or type the values for the asset data associated with the software and click **Next**.
   The fields can vary depending on how the administrator configured your data for software.

8. Click **Finish**.

**Add Multiple Similar Software Assets**

If your environment has many nearly identical copies of software, such as the same application with a different license number, you can use VCM for assets to clone one copy as a way to quickly add records for the others.

**Prerequisites**
- Log in to VCM with a role that has edit permission for asset configuration data.
- Create at least one copy of the software to serve as a baseline. See “Add Software Assets” on page 243.

**Procedure**

1. Click **Console**.

2. Select **Asset Extensions > Software Configuration Items**.

3. In the data grid, select the original, baseline software asset.

4. Click **Clone**.

5. Modify the details to reflect the new copy of the software asset and click **Next**.
   You must change at least the name.

6. Change the data type that VCM for assets will look for to detect the installed software and click **Next**.
   The options take you to custom wizard pages where you type or select what VCM for assets will look for in the database.

   - **Software Inventory (Windows)**: Select a product from the software inventory (SI) list.
   - **Registry (Windows)**: Type or select a Windows Registry path, key, and value.
   - **File System - Known Files (Windows)**: Type or select a filename and version.
   - **Software Inventory - Packages (UNIX)**: Select a product from the SI list.
   - **Software Inventory - Utilities (UNIX)**: Select a product from the SI list.
   - **File System - Known Files (UNIX)**: Type or select a filename.

7. Click **Next**.

8. Modify the asset data values to reflect the new software and click **Next**.

9. Click **Finish**.
Edit Asset Data for Software

Use VCM for assets to change your software asset records as your enterprise changes.

Prerequisites
Log in to VCM with a role that has edit permission for asset configuration data.

Procedure
1. Click Console.
2. Select Asset Extensions > Software Configuration Items.
3. In the data grid, select the software asset.
4. Click Edit.
5. Change the name or description and click Next.
6. Change the data type that VCM for assets will look for to detect the installed software and click Next.
   The options take you to custom wizard pages where you type or select what VCM for assets will look for in the database.
   - Software Inventory (Windows): Select a product from the software inventory (SI) list.
   - Registry (Windows): Type or select a Windows Registry path, key, and value.
   - File System - Known Files (Windows): Type or select a filename and version.
   - Software Inventory - Packages (UNIX): Select a product from the SI list.
   - Software Inventory - Utilities (UNIX): Select a product from the SI list.
   - File System - Known Files (UNIX): Type or select a filename.
7. Click Next.
8. Change the values for the asset data associated with the software and click Next.
   The fields can vary depending on how the administrator configured your data for software.
9. Click Finish.

Edit Asset Data Values for Software

You can change the details about a specific copy of software when the long term information, such as the application name or version, is going to remain the same.

Prerequisites
Log in to VCM with a role that has edit permission for asset configuration data.
Procedure
1. Click Console.
2. Select Asset Extensions > Software Configuration Items.
3. In the data grid, select the software asset.
4. Click Edit Values.
5. Move the data fields that you want to edit into the Selected list and click Next.
   Use the arrow buttons to move entries to or from the Selected list.
6. Select or type the new values and click Next.
7. Review the new values and click Finish.

Delete Software Data
Use VCM for assets to delete entries for software that is no longer installed at your site.

Prerequisites
Log in to VCM with a role that has edit permission for asset configuration data.

Procedure
1. Click Console.
2. Select Asset Extensions > Software Configuration Items.
3. In the data grid, select the software asset.
4. Click Delete.
5. Click OK.
Managing Changes with Service Desk Integration

VCM Service Desk Integration tracks planned and unplanned changes to managed machines in your organization, and integrates change requests with your change management process.

Service Desk Integration works by temporarily holding requested changes to managed machines while VCM integrates with your service desk application in order to pass the requests through your change management process or workflow. After the changes are approved, VCM resumes changing the managed machines, in order of criticality.

VCM Service Desk Connector links VCM with the service desk application in order to track and manage the VCM initiated changes. Change management process and workflow definitions vary by customer and depend on the configuration implemented during your VMware services engagement.

This chapter includes the following topics:

- **Configure Service Desk Integration**
- **View Service Desk Integration in the Console**
- **View Service Desk Integration in Job Manager**

### Configure Service Desk Integration

To add the Service Desk Integration feature to VCM, you must complete the following high-level tasks.

**Procedure**

1. Contact VMware Customer Support to determine the requirements for your integration and arrange for a VMware services engagement.
2. License Service Desk Integration.
3. Activate Service Desk Integration

After VMware Customer Support assists you with licensing and the integration of VCM with your service desk application, additional nodes that are unique to the service desk feature appear in VCM.

**What to do next**

Look at your service desk data. See "View Service Desk Integration in the Console" on page 247.

### View Service Desk Integration in the Console

When service desk integration is enabled, the Service Desk data grids provide a detailed view of VCM-related service desk events.
Procedure

1. Click Console.
2. Select Service Desk.
3. Under the Service Desk node, select any subnode.
   
   For example, click By RFC to view the data according to request for change (RFC). Under the By RFC sub-node, select an RFC to view the data for that item.

Your subnodes and data views might differ from the defaults or from other organizations based on your requirements and specific implementation.

What to do next

Look at the status of change jobs. See "View Service Desk Integration in Job Manager" on page 248.

View Service Desk Integration in Job Manager

VCM Service Desk Integration pauses requested changes to managed machines while VCM integrates with your service desk application to pass the request through your change management process.

Procedure

1. Click Administration.
2. Select Job Manager > Pending Response.
   
   After the job is approved, it is released to run immediately or at a scheduled time.
3. Select Job Manager > Running.
   
   Alternately, select Job Manager > Scheduled.

NOTE Patching jobs are in a different location. Locate patching jobs by clicking Patching and selecting VCM Patching Administration > {operating-system} > Job Manager.
Index

% Systemroot% environment variable 94, 96
A
About Patching 153
about this book 9
access by user 11
accessing
  compliance content 21
active directory
  (AD) 209
  collection results 218
  configuration 215
  data collection 217
  getting started 209
  installing VCM for active directory 215
  run determine forest action 216
  run domain controller setup action 217
AD (active directory) 209
add
  vCenter Server 30
  vCloud Director 37
  vShield Manager 47
add servers
  provisioning, operating system 178
adding
  asset data field 236
  hardware asset data 240
  Mac OS X 142
  multiple hardware asset data 241
  multiple software asset data 244
  Oracle Instances 134-135
  repository sources 202
  service desk integration 247
  software asset data 243
  UNIX/Linux machines 122
ADProductInstall.exe for Windows 94-95
agent
  ADProductInstall.exe for Windows AD 94-95
  CMAgentInstall.exe for Windows 94-95
  install, manual 93
  install, Windows 91
  installation 91
  installing Mac OS X 143
  Linux and UNIX 124
  remote client 224
  uninstall, Mac OS X 149
  uninstall, UNIX/Linux 131
  uninstalling 97
agent communication
  changing after OS provisioning 188
agent proxy
  collector 51
assessment
  SCAP 172-173
assets
  adding data field 236
  adding hardware data 240
  adding multiple hardware data 241
  adding multiple software data 244
  adding software data 243
  configuring data fields 235
  configuring hardware data 240
  configuring software data 243
  deleting data field 238
  deleting hardware data 242
  deleting software data 246
  editing hardware data 241
  editing software data values 242
  editing software data values 245
  editing data field 237
  getting started 235
  rearranging data fields 238
  refreshing dynamic data field 239
  reviewing data field 236
  VCM asset data 239
assigning
  network authority account 89
auditing 85
available domains
  domain controllers 210
B
badge score
  vCenter Operations Manager 74, 76-79
binary mode, use for ftp 124, 144
C
certificates
  remote client 222
change
  vCenter Operations Manager 73
change management
  WCI 111
check
  for UNIX/Linux updates 164
  for Windows updates 157
checking
  network authority account 88, 210
CMAgentInstall.exe
  for Windows 94-95
uninstalling agent 97
collect
domain controllers 214
ESX logs 50, 55
ESX service console operating system 50
hosts, virtual machine 51
package managers 201
repositories 202
vCenter Server 32
vCenter Server virtual machines 35
vCloud Director 37, 39
vCloud Director vApp 41
virtual machine hosts 51
vShield Manager 46, 49
collect distributions
provisioning, operating system 179
collecting
WCI data 112
collection filter for WCI 116
collection results
active directory 218
Oracle 139
Remote 232
UNIX/Linux 132
WCI 117
collection scripts
custom for WCI 113
collection user account
creating, Config User Action 137
collections
active directory 217
domain controllers 214
Mac OS X 149
Oracle 138
patching 157
results, Mac OS X 151
UNIX/Linux 131
vCenter Server data 30, 33
virtualization 55
WCI 115
Windows machines 97
collector
agent proxy 51
aware of Remote client 222, 232
install before agents 124, 143
lock request 94
compliance
checking, UNIX/Linux 132
content, accessing 21
Mac OS X 151
software provisioning 206-207
compliance exceptions
vCenter Server 68
vCloud Director 68
virtual objects 68
compliance filters
vCenter Server 64
vCloud Director 64
virtual objects 64
collection rule groups
preview 64
vCenter Server 62
vCloud Director 62
virtual objects 62
collection rules
vCenter Server 63
vCloud Director 63
virtual objects 63
collection templates
vCenter Server 61, 65
vCloud Director 61, 65
virtual objects 61, 65
configuration
Active Directory 215
configuring
asset data field 235
hardware data 240
software data 243
vSphere Client Plug-in 57
console
service desk integration 247
content for compliance 21
wizard 20
copying
files to ESX/vSphere servers 53
create packages
software provisioning 199
creating
Oracle collection user account 137
CSI_AGENT_RUN_OPTION 124, 143
custom filter sets
for Remote 223
remote client 224
D
deleting
asset data field 238
hardware asset data 242
software asset data 246
deploy
patching 168
deploying
patches, UNIX/Linux 168
patches, Windows machines 163
determine forest action
running for active directory 216
develop
custom collection scripts 113
discover
domain controllers 211
vCloud Director vApp 43
discovering
domain controllers 209, 211
Oracle Instances 133
Windows machines 87, 89
discovery
provisioning, operating system 179
domain controllers
add network authority 210
assign network authority 211
available domains 210
collect 214
collecting 214
discover 211
discover, license, install 209
discovering 211
domain discovery 210
license 212
licensing 212
run setup action 217
domain discovery
domain controllers 210
Windows machines 88
domains
active directory 209
download settings
patch assessment content 156
E
editing
asset data field 237
hardware asset data 241
hardware asset data values 242
software asset data 245
software asset data values 245
VCM asset data 239
environment variable, %Systemroot% 94, 96
ESX
collect 51
service console operating system collection 50
ESX files
copy 53
ESX logs
collect 50, 55
example PowerShell script 106
exploring
assessment results, UNIX 166
assessment results, Windows 159
Remote collection results 232
exporting
SCAP assessment 173
F
filter for WCI collections 116
filter sets
Remote 223
remove client 223
forest
run determine forest action 216
forests
active directory 209
foundation checker 19
installation 22
ftp, use binary mode 124, 144
G
getting started
active directory 209
assets 235
auditing 85
deploy patches, UNIX/Linux 168
deploy patches, Windows 163
explore assessment results, UNIX 166
explore assessment results, Windows 159
launch assessment 158
launching 12
logging on 12
patching collection 157
remote client 221
tools 19
Using Patching 156
virtualization 23
vSphere Client Plug-in 58
WCI 99
WCI PowerShell scripts 101
H
host files
remote client 224
hosts
collect 51
HTTP agent, port number 94
I
import/export wizard 20
importing
SCAP benchmark 172
information bar in portal 13
install package manager
software provisioning 198
install package studio
software provisioning 196
install repository
software provisioning 195
installation
agent on Mac OS X machines 143
agent on Red Hat, SUSE 124
agent on UNIX/Linux machines 124
agent on Windows machines 91, 93
agent, UNIX 125, 144
foundation checker 22
tools 19
Windows machines 87, 209
InstallCMAgent 126, 145
installing
Package Studio 196
packages 203
PowerShell 114
remote client 226-227, 229
repositories 195
software provisioning 194
VCM for active directory 215
integration
service desk 247
invalid certificate in vSphere Client
troubleshooting 59
job manager 19
  service desk integration 248
job status reporting
  WCI 116
jobs history
  provisioning 205
launch an assessment 158
license
  domain controllers 212
licensing
  domain controllers 209, 212
  Mac OS X 143
  UNIX/Linux machines 123
Linux and UNIX
  install agent 124
  patching 164-165
  patching filters 166
  upgrade 122
lock request, submit from collector 94
logs
  ESX 55
Mac OS X
  adding 142
  agent installation 143
  agent, uninstall 149
  collection 149
  collection results 151
  licensing 143
managing agent
  virtual environments 26
managing agent collection
  virtual environments 27
managing agent enabled
  virtual environments 28
managing agent HTTPS bypass
  virtual environments 28
managing agent trust status
  virtual environments 27
managing agent; SSL thumbprint 29
mapping
  create 76
  dashboard 78
  schedule 78
  vCenter Operations Manager 73-74, 77-79
NAT
  see network address translation 41
network address translation
  vCloud Director vApp 41
network authority account
  assigning 89
  checking 88, 210
  domain controllers 210
network authority, assign
  domain controllers 211
operating system
  virtual machine 36
operating system provisioning 175
Oracle
  10g installations 137
  Add/Edit Instance 133
  adding instances 134-135
  collection results 139
  collection user account 137
  collections 138
  Config User Action 137
  discovering instances 133
  permissions 137
Oracle 10g
  user account 137
overview
  SCAP 171
vSphere Client Plug-in 56
package managers
  collect 201
Package Studio
  installing 196
packages
  installing 203
patch assessment content architecture
  download settings 156
  repository 156
patching 156
  check for updates, UNIX/Linux 164
  check for updates, Windows 157
  collect, Linux and UNIX 165
  collection 157
  deploy 168
  filters, Linux and UNIX 166
  new UNIX patch assessment content 155
  prerequisites 159
  reports 170
  UNIX and Linux 164
permissions
  Oracle 137
port number for HTTP agent install 94
port number for UNIX agent install 127, 146
portal
  familiarizing 13
  information bar 13
  sliders 15
  toolbar 14
PowerShell
  example script 106
  executing for WCI 106
installation 114
references 106
script signing policies 105
scripts, troubleshooting 119
signing scripts for WCI 106
WCI getting started 101
Windows Custom Info 115
PowerShell script
  verifying 113
prerequisites
  patching deployment 159
preview
  compliance rule groups 64
Product Overview 153
provision machines
  operating systems 180, 183
provisioning
  compliance 207
  compliance rule 206
  jobs History 205
provisioning, operating system 175
  add servers 178
  agent communication 188
  collect distributions 179
  components 175
  discovery 179
  provision machines 180, 183
  re-provision machines 189
results 189
  servers 177
  set server trust status 178
  time, Linux 188
workflow 176
provisioning, software 193, 201
  create packages 199
  install package manager 198
  install package studio 196
  install repository 195
  installation 194
purge
  for WCI 115
R
re-provisioning machines
  operating systems 189
rearranging
  asset data fields 238
Red Hat
  install UNIX agent 124
refreshing
  dynamic asset data field 239
registering
  vSphere Client Plug-in 56
remediation
  compliance rule 207
Remote
  collection results 232
  filter sets 223
  settings 222
remote client
  certificates 222
  collector aware 222, 232
  configure VCM remote 221
getting started 221
installation 225
  installation, command line 227
  installation, manual 226
  installation, remote commands 229
network 232
  settings 222
  settings, custom filter sets 224
  settings, filter sets 223
  settings, host files 224
reports
  patching 170
  WCI 118
repositories
  collect 202
  installing 195
repository for patch assessment content 156
repository sources
  adding 202
results
  collection, active directory 218
  collection, Mac OS X 151
  ESX logs 55
  provisioning, operating system 189
  SCAP 173
  vCloud Director 40
  virtualization 55
  vShield Manager 49
reviewing
  asset data field 236
run compliance
  vCenter Server 66
  vCloud Director 66
  virtual objects 66
running
  determine forest action 216
  domain controller setup 217
S
SCAP
  assessment 172-173
  benchmark 172
  exporting assessment 173
  importing benchmark 172
  overview 171
  results 173
score
  vCenter Operations Manager 73-74, 76-79
script
  verify validity 113
script-based collection filter 116
script signing
  policies 105
  references 106
scripts
  PowerShell 101
service desk integration 247
  adding 247
  console 247
job manager 248
set server trust status
  provisioning, operating system 178
settings
  remote 222
  vCloud Director 38
  vShield Manager 47
setup action
  running for active directory 217
signing
  policies, PowerShell scripts 105
  PowerShell scripts 106
sliders
  in portal 15
software provisioning 193, 201
  create packages 199
  install package manager 198
  install package studio 196
  install repository 195
  installation 194
sources
  repository sources 202
SQL*Plus
  Oracle 137
SSL thumbprint
  managing agent 29
standards compliance
  create 76
  dashboard 78
  run 77
  schedule 78
  vCenter Operations Manager 73-74, 76-79
SUSE
  install UNIX agent 124
T
time
  provisioning, Linux operating system
  Linux 188
ToCMBase64String 102
toolbar
  in portal 14
tools
  foundation checker 19
  getting started 19
  import/export, content 19
  installation 19
  job manager 19
troubleshooting
  PowerShell scripts 119
  vSphere client integration 59
U
uninstall
  agent 97
  agent, Mac OS X 149
  agent, UNIX/Linux 131
UNIX agent
  port number 127, 146
UNIX and Linux
  install agent 124
  patching 164-165
  patching filters 166
  upgrade 122
UNIX patch assessment content 155
UNIX patch assessment content repository 156
UNIX patch content download 156
UNIX/Linux
  agent uninstall 131
  check for updates 164
  collections 131
  machines, adding 122
  machines, licensing 123
updates
  check for UNIX/Linux 164
  check for Windows 157
upgrade
  Linux and UNIX 122
user access 11
V
vCenter Operations Manager 73
  badge score 74, 76-79
  change 73
  compliance standards 73
  mapping 73-74, 77-79
vCenter Server 23
  add 30
  collect 32
  compliance exceptions 68
  compliance filters 64
  compliance rule groups 62
  compliance rules 63
  compliance templates 61, 65
  data collections 30
  run compliance 66
vCenter Server virtual machines
  collect 35
vCloud Director
  add 37
  collect 37, 39
  collection results 40
  compliance exceptions 68
  compliance filters 64
  compliance rule groups 62
  compliance rules 63
  compliance templates 61, 65
  run compliance 66
  settings 38
vApp collection 41
vApp network address translation 41
vCloud Director vApp
discover 43
VCM actions tab; troubleshooting 59
VCM asset data
  editing 239
VCM Summary and VCM Action
  troubleshooting 59
VCM summary tab troubleshooting 59
verify PowerShell script 113
virtual environments managing agent 29
virtual environments managing agent 26
managing agent collection 27
managing agent enabled 28
managing agent HTTPS bypass 28
managing agent trust status 27
virtual machine manage operating system 36
virtual machines vCloud Director vApp 41
virtual objects compliance exceptions 68
compliance filters 64
compliance rule groups 62
compliance rules 63
compliance templates 61, 65
run compliance 66
virtualization collecting results 55
collections 55
getting started 23
vShield Manager add 47
collect 46, 49
collection results 49
settings 47
vSphere Client Plug-in configuring 57
getting started 58
overview 56
registering 56

W
WCI challenges CDATA 105
challenges in column names 104
challenges in scripting 102
challenges in task entries 104
change management 111
collecting data 112
collection 115
collection filter 116
collection results 117
custom collection scripts 113
executing PowerShell scripts 106
getting started 99
guidelines in scripting 102
job status reporting 116
prerequisites to collect 100
purge 115
running reports 118
verify PowerShell script 113
Windows check for updates 157
Windows Custom Information (WCI) 99
Windows machines collecting 97
discover, license, install 87
discovering 89
domain discovery 88
install agent 91
licensing 90
uninstalling agent 97
wizards content 20
import/export 20