

VMware vCenter Configuration Manager Installation and Getting Started Guide

vCenter Configuration Manager 5.4

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>.

EN-000485-01

vmware[®]

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

© 2006-2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Updated Information	9
About This Book	11
Preparing for Installation	13
Use Installation Manager	14
Understand Installation Configurations	14
Understand Tools Installation	15
Check Prerequisites for Installation	15
Hardware and Software Requirements	15
Administration Rights	15
Default Network Authority Account	15
Collector Services Account	16
VMware Application Services Account	16
VCM Remote Virtual Directory	16
Secure Communications Certificates	16
Server Authentication	17
Understand Use of FIPS Cryptography by VCM	19
VCM Use of Microsoft Cryptographic Service Providers (CSPs) for Windows Machines	19
Cryptography for UNIX/Linux Platforms	19
Cryptography used in VCM Software Components	20
Supported Windows and UNIX Platforms	20
Installing VCM	21
Using Installation Manager	21
Installing and Configuring the OS Provisioning Server and Components	23
Installing the Operating System Provisioning Server	23
Best Practices	23
Install the OS Provisioning Server	23
Preparing Boot Images for Windows Provisioning	28
Create Windows Boot Image	28
Copy the VCM Certificate to the OS Provisioning Server for Linux Provisioning	29
Importing Distributions into the OS Provisioning Server Repository	29
Create Directories for Windows Distributions	29
Import Windows Distributions	30
Import Linux/ESX Distributions	31
basicimport Command Options	32
Configuring the OS Provisioning Server Integration with the VCM Collector	32
Configure Stunnel on the OS Provisioning Server	33
Configure Stunnel on the VCM Collector	34
Confirm Stunnel Configuration	36
Maintaining Operating System Provisioning Servers	37
Backup the OS Provisioning Repository	37
Restore the OS Provisioning Repository From Backup	38
Managing the OS Provisioning Server System Logs	43
Upgrading or Migrating vCenter Configuration Manager	45

Upgrade and Migration Scenarios	45
Prerequisites	46
Back up Your Databases	47
Back up Your Files	47
Back up Your Certificates	47
Software Supported by the VCM Collector	47
Migration Process	48
Prerequisites	48
Foundation Checker Must Run Successfully	48
Use the SQL Migration Helper Tool	48
Migrate Only Your Database	48
Replace your existing 32-Bit Environment with the Supported 64-bit Environment	49
How to Recover Your Machine if the Migration is not Successful	49
Migrate a 32-bit environment running VCM 5.3 or earlier to VCM 5.4	50
Migrate a 64-bit environment running VCM 5.3 or earlier to VCM 5.4	51
Migrate a split installation of VCM 5.3 or earlier to a single-server installation	52
After You Migrate VCM	52
Upgrade Process	52
After You Upgrade VCM	53
Upgrading Existing Windows Agents	53
Upgrading Existing Remote Clients	54
Upgrading Existing UNIX Agents	54
To Upgrade the UNIX Agent(s) with a Local Package	55
To Upgrade the UNIX Agent(s) with a Remote Package	56
Upgrading VCM for Virtualization	56
Upgrading an Agent Proxy Machine	57
Upgrade the vSphere Client VCM Plug-In	59
Getting Started with VCM Components and Tools	61
Understanding User Access	61
Do Not Use the Collector as a Web Console	62
Starting and Logging Onto VCM	62
How to Start VCM and Log On	62
Getting Familiar with the Portal	63
General Information Bar	64
Portal Toolbar	64
Sliders	65
Where to Go Next	67
Getting Started with VCM	69
Discover, License, and Install Windows Machines	69
Verifying Available Domains	69
Checking the Network Authority	70
Assigning Network Authority Accounts	71
Discovering Windows Machines	72
Licensing Windows Machines	75
Installing the VCM Windows Agent on your Windows Machines	77
Performing an Initial Collection	83
Exploring Windows Collection Results	84
Getting Started Collecting Windows Custom Information	88
Discover, License, and Install UNIX/Linux Machines	97
Adding UNIX/Linux Machines	97
Licensing UNIX/Linux Machines	98
Installing the Agent on UNIX/Linux Machines	99
Performing a UNIX/Linux Collection	106
Exploring UNIX/Linux Collection Results	107
Discover, License, and Install Mac OS X Machines	110

Getting Started with VCM for Mac OS X	110
Adding Mac OS X Machines	111
Licensing Mac OS X Machines	112
Installing the Agent on Mac OS X Machines	113
Performing a Mac OS X Collection	119
Exploring Mac OS X Collection Results	121
Discover, License, and Collect Oracle Data from UNIX Machines	123
Adding UNIX Machines Hosting Oracle and Installing the Agent	124
Discovering Oracle Instances	124
Creating the Oracle Collection User Account	125
Performing an Oracle Collection	129
Exploring Oracle Collection Results	129
Reference Information about Oracle	129
Customize VCM for your Environment	130
How to Set Up and Use VCM Auditing	131
Getting Started with VCM for Virtualization	133
Virtual Environments Configuration	133
ESX/ESXi Server Collections	134
vCenter Server Collections	135
Configuring vCenter Server Data Collections	135
vCenter Server Collection Upgrade Considerations	135
vCenter Server Collection Prerequisites	135
Collect vCenter Server Data	137
Reviewing Collected vCenter Server Data	137
Troubleshooting vCenter Server Data Collections	138
Configuring VM Host Collections	138
Configure the Collector as an Agent Proxy	138
License and Configure VM Hosts	139
Copy Files to the ESX/ESXi Servers	141
Perform an Initial Virtualization Collection	142
Reviewing Virtualization Collection Results	143
Configuring the vSphere Client VCM Plug-In	143
Register the vSphere Client VCM Plug-In	143
Configuring the vSphere Client VCM Plug-In Integration Settings	144
Manage Machines from the vSphere Client	145
Upgrade the vSphere Client VCM Plug-In	145
Troubleshooting the vSphere Client VCM Plug-In Registration	146
Getting Started with VCM Remote	149
Getting Started with VCM Remote	149
Installing the VCM Remote Client	150
Installing the Remote Client manually	151
Making VCM Aware of VCM Remote Clients	158
Configuring VCM Remote Settings	158
Creating Custom Collection Filter Sets	158
Specifying Custom Filter Sets in the VCM Remote Settings	158
Performing a Collection Using VCM Remote	159
Exploring VCM Remote Collection Results	159
Getting Started with VCM Patching	161
VCM Patching for Windows and UNIX/Linux	161
VCM Patching for Windows	161
VCM Patching for UNIX/Linux	162
Minimum System Requirements	162
About UNIX Patch Assessment and Deployment	162
Getting Started with VCM Patching	165

Running VCM Patching Reports	174
Customize Your Environment for VCM Patching	175
Getting Started with Operating System Provisioning	177
About OS Provisioning	177
OS Provisioning Components	177
Provision Machines Workflow	178
Collect OS Distributions	179
Discover Provisionable Machines	179
Provision Machines	180
Configure ESX and ESXi Machines	181
Change Agent Communication	182
Working with Provisioned Machines	182
Re-Provision Machines	182
Getting Started with Software Provisioning	185
Introduction to VCM Software Provisioning	185
Using Package Studio to Create Software Packages and Publish to Repositories	185
Software Repository for Windows	185
Package Manager for Windows	185
	186
Installing the Software Provisioning Components	186
Install Software Repository for Windows	187
Install Package Studio	188
Install Package Manager on Managed Machines	190
Using Package Studio to Create Software Packages and Publish to Repositories	190
Creating Packages	191
Using VCM Software Provisioning for Windows	192
Prerequisites	192
Collect Package Manager Information from Machines	193
Collect Software Repository Data	193
Add Repository Sources to Package Managers	194
Install Packages	195
Related Software Provisioning Actions	196
Viewing Provisioning Jobs in the Job Manager	196
Creating Compliance Rules based on Provisioning Data	196
Creating Compliance Rules containing Provisioning Remediation Actions	197
Further Reading	199
Getting Started with VCM Management Extensions for Assets	201
Getting Started with VCM Management Extensions for Assets	201
Review Hardware and Software Configuration Item Fields	201
Modifying Hardware Configuration Item Fields	202
Modifying Software Configuration Item Fields	204
Adding Hardware Configuration Items	205
Editing Values for Devices	205
Modifying Other Devices	206
Adding Software Configuration Items	207
Further Reading	208
Getting Started with VCM Service Desk Integration	209
Getting Started with Service Desk Integration	209
Service Desk Integration in the Console	209
Service Desk Integration in Job Manager	210
Further Reading	211
Getting Started with VCM for Active Directory	213

Making VCM Aware of Domain Controllers	213
Confirming the Presence of Domains	214
Adding and Assigning Network Authority Accounts	215
Discovering Domain Controllers	215
Verifying Domain Controller Machines in Available Machines	217
Licensing and Deploying the VCM Agent	217
Performing a Machine Data Type Collection	220
Configuring VCM for Active Directory as an Additional Product	221
Deploying VCM for AD to the Domain Controllers	221
Running the Determine Forest Action	222
Running the Setup DCs Action	223
Performing an Active Directory Data Collection	225
Exploring Active Directory Collection Results	227
Further Reading	230
Accessing Additional Compliance Content	231
Locating the Content Directory	231
Launching the Content Wizard to Import Relevant Content	231
Exploring Imported Content Results in the Portal	231
Installing and Getting Started with VCM Tools	233
Installing the VCM Tools Only	233
Foundation Checker	234
VCM Import/Export and Content Wizard (CW)	234
VCM Import/Export	235
Content Wizard	236
Maintaining VCM After Installation	237
Customize VCM and Component-specific Settings	237
Configure Database File Growth	239
Configure Database Recovery Settings	240
Create a Maintenance Plan for SQL Server 2008 R2	240
Incorporate the VCM CMDB into your Backup and Disaster Recovery Plans	248
Troubleshooting Problems with VCM	249
Evaluating Missing UNIX Patch Assessment Results	249
Resolving Reports and Node Summaries Problems	250
To Resolve the Problem	250
Resolving Protected Storage Errors	250
Resetting the Required Secure Channel (SSL)	251
Updating the VCM Virtual Directory	251
Updating the IIS Settings in VCM	251
Resolving a Report Parameter Error	252
Index	253

Updated Information

VCM Installation and Getting Started Guide is updated with each release of the product or when necessary.

This table provides the update history of the *vCenter Configuration Manager Installation and Getting Started Guide*.

Revision	Description
EN-000485-01	<ul style="list-style-type: none">▪ "Maintaining Operating System Provisioning Servers" on page 37 added to provide information regarding backup and recovery instructions, and file maintenance requirements.▪ "Confirm Stunnel Configuration" on page 42 removed the final confirmation step as it was redundant of the procedure in "Confirm Stunnel Configuration" on page 42.▪ "Provision Machines" on page 180 and "Re-Provision Machines" on page 182 updated to indicate that the step 6 information regarding the use of DHCP and the host name resolving to localhost applies only to ESX and ESXi machines. Additionally, the Post-Provisioning Action at the end of the procedure now includes Windows 2008 SP1 and SP2 as operating systems requiring Internet access to complete the license activation process.
EN-000485-00	Initial Release.

About This Book

The *VMware vCenter Configuration Manager Installation and Getting Started Guide* describes the steps necessary for a successful VCM installation.

This document contains the following information:

- Preparing for the VCM installation.
- Installing VCM.
- Getting started with VCM and its components.
- Maintenance and troubleshooting.

Read this document and complete the associated procedures to prepare for a successful installation.

The *VMware vCenter Configuration Manager Installation and Getting Started Guide* applies to VCM, Foundation Checker, and Service Desk Connector.

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's 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 Hardware and Software Requirements Guide*, *VCM Foundation Checker User's Guide*, *VCM Installation and Getting Started 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>.

Preparing for Installation

Use this information to help you prepare to install VCM components and tools in your enterprise.

- [Use Installation Manager](#): Provides an overview of Installation Manager, which is used to install and activate all VCM components and tools.
- [Understand Installation Configurations](#): Describes the supported installation configurations for VCM.
- [Understand Tools Installation](#): Explains how VCM tools are installed.
- [Check Prerequisites for Installation](#): Lists the prerequisites you should complete prior to using VCM Installation Manager to perform the installation.

For an overview of the security precautions you should take before installing VCM, see the *VCM Security Environment Requirements White Paper* on the Download VMware vCenter Configuration Manager.

This document assumes that your hardware and software configuration meets the requirements described in the *VCM Hardware and Software Requirements Guide*. If you have not already done so, verify that your configuration meets the installation requirements by performing a Tools Only installation of VCM Foundation Checker, and then running it after it is installed. If VCM Foundation Checker does not return any errors, then you are ready to proceed. For more information on performing a Tools only installation, see "[Installing and Getting Started with VCM Tools](#)" on page 233.

Use Installation Manager

Use Installation Manager to perform new installations as well as upgrades. Installation Manager provides a highly simplified process for installing components and tools, and steps you through the entire installation or upgrade process. Installation Manager:

- Performs checks to ensure the machine(s) meets the hardware and software prerequisites necessary for installation.
- Provides confirmation of the license file you apply during installation.
- Installs VCM and all of its components and tools in the appropriate order on your machine(s).
- Tests each progressive step during the installation to ensure that all components are successfully installed and that the licensed components are successfully activated.

Installation Manager operates with minimal user input and provides clear feedback on progress throughout the entire installation process.

Installation Manager installs VCM and all of its components on your machine, even components that you have not purchased. However, only the components that you have purchased are licensed by your license file, which enables you to purchase more licenses later, and thereby activate additional components that are already installed.

To install VCM and all of its components and tools for the first time, follow the procedures in ["Installing VCM" on page 21](#).

IMPORTANT You can use Installation Manager to upgrade from VMware VCM 5.3, EMC Ionix SCM 5.0 or greater, or Configuresoft ECM 4.11.1 or greater to VCM 5.4.

When performing a new installation or a migration, you must have the previous license file available and specify the path to the license file during the installation. Installation Manager will use the license file to activate the components that you have purchased. If you do not have the license file from VCM 4.11.1 or later, contact VMware Customer Support.

Understand Installation Configurations

Before proceeding, you must have already configured your hardware and installed all of the prerequisite software based on the information in the *VCM Hardware and Software Requirements Guide*.

As of VCM 5.4, split installations are not supported. To migrate a split installation of VCM 5.3 or earlier to a single-server installation, see the section on migrating VCM. For more information, contact VMware Customer Support.

For a detailed diagram of a complete installation, see the *VCM Hardware and Software Requirements Guide*.

Understand Tools Installation

Several tools are installed with automatically VCM. These tools include:

- Foundation Checker
- Import/Export Tool and Content Wizard Tool
- Package Studio

You may install VCM tools separately on a non-Collector machine as needed. To install the Tools only, use the installation procedures in ["Installing and Getting Started with VCM Tools" on page 233](#).

Check Prerequisites for Installation

Complete these prerequisites prior to using Installation Manager.

Hardware and Software Requirements

Before you can install VCM, your hardware and software configuration must meet the requirements in the *VCM Hardware and Software Requirements Guide*.

IMPORTANT Installation Manager runs Foundation Checker automatically during the VCM installation, which checks the machine to verify that all of the prerequisites are satisfied for a successful installation of VCM. Running Foundation Checker as part of the Installation Manager process, rather than running it as a standalone tool, captures common issues that are difficult to remediate as well as issues related to specific components and the version of VCM being installed. Because Foundation Checker verifies component-specific issues against VCM, you should use Installation Manager to run Foundation Checker. Foundation Checker must run without producing before you can proceed with the VCM installation. For more information about the standalone Foundation Checker, see ["Installing and Getting Started with VCM Tools" on page 233](#).

If you install the Agent on HP-UX 11.11, you must also install Patch PHSS_30966, which is required. If you need assistance, contact VMware Customer Support.

Administration Rights

The User Account of the person performing your installation or upgrade must be all of the following:

- A system administrator on the machine(s) on which the installation or upgrade is being performed, **and**
- A system administrator on the database instance that will be used, **and**
- A member of a domain.

The installing User Account should **not** be the account used to run the SQL Server Services; nor, after installation, should you create a VCM user with the SQL Server Services account credentials.

Default Network Authority Account

You must specify the default network authority account during the installation. The default network authority account, which is often the system administrator's account (for example, a Domain Admin in the Local Admin Group), must be set up in the Local Administrators group on each machine prior to installation. You should have already completed this step by following the checklist in the *VCM Hardware and Software Requirements Guide*.

The Local System account named NT AUTHORITY\System has unrestricted access to all local system resources. This account is a member of the Windows Administrators group on the local machine, and a member of the SQL Server sysadmin fixed server role. If the NT AUTHORITY\System account does not have access to the VCM installation binary files (possibly because someone removed the account or inherently removed access), the installation will result in an “access denied” error on the first step. Details of this error are not stored in the VCM error log. The solution is to grant access to the NT AUTHORITY\System account from the installation source directory, and then run the installation again (right-click the folder, select the Security tab, and make sure the user or user’s group has Full Control of the file/folder).

NOTE The network authority account can be changed later in VCM at **Administration > Settings > Network Authority**.

Collector Services Account

The Collector Services Account must be specified during the installation process. This account, which may not necessarily be the system administrator’s, must exist in the Local Administrators group on the Collector machine. In addition, this account must not be the LocalSystem account.

IMPORTANT If the password for your services account changes, you must also change the password in both the Services Management and Component Services DCOM Config consoles.

To change your services password in the Services Management console, click **Administrative Tools > Services**. Locate all of the services that use the services account to log on. Right-click each of these services and select **Properties**. Click the **Log On** tab and update the password field to reflect your new password.

To change your services password in the Component Services DCOM Config console, click **Administrative Tools > Component Services**. Expand the Component Services node and select **Computers > My Computer > DCOM Config**. Right click the **LicenseDcom** file and select **Properties**. Click the **Identity** tab and update the password field to reflect your new password.

VMware Application Services Account

The VMware Application Services Account must be a domain user. Because this account will have full administrative authority for the CSI_Domain database, you should never use it as a VCM login or for any other purpose.

VCM Remote Virtual Directory

You must specify the VCM Remote Virtual Directory account during the installation. To reduce the chances of a security risk to accounts, this account should not be the same account that you used for your Default Network Authority Account and/or your Services Account.

NOTE If necessary, you can change the service account later using the IIS Management console.

Secure Communications Certificates

VCM uses Transport Layer Security (TLS) to secure all HTTP communication with Windows and UNIX Agents in HTTP mode (includes all UNIX Agents and Windows Agents in HTTP mode). TLS uses certificates to authenticate the Collector and Agents to each other. You must specify certificates for the Collector and for the Enterprise during the installation. If you plan to use your own certificates, familiarize yourself with the certificate names so that you can select them during installation.

To be valid, a Collector certificate must be:

- Located in the local machine personal certificate store.
- Valid for Server Authentication. If any Enhanced Key Usage extension or property is present, it must include the Server Authentication OID 1.3.6.1.5.5.7.3.1. If the Key Usage extension is present, it must include DIGITAL_SIGNATURE.
- Active, and not expired.

Alternatively, Installation Manager can generate the Collector and Enterprise certificates for you; select the **Generate** option during installation.

NOTE If you will install more than one Collector that will communicate with the same Agent(s), or plan to replace/renew your certificates later, special considerations are required to generate and select certificates in VCM Installation Manager. For details about VCM and Transport Layer Security (TLS), see Transport Layer Security Implementation for VCM.

Server Authentication

Server Authentication is a method of authenticating the server to the client. VCM supports server authentication. In VCM environments where TLS is employed, VCM Agents verify the identity of the Collector(s) through the use and verification of certificates (over HTTP).

Typically, the server authenticates a client/user by requiring information such as a user name and password. When server authentication is used, the client/user verifies that the server is valid. To accomplish this verification using TLS, the server provides a certificate issued by a trusted authority, such as Verisign®. If your client web browser has the Verisign® Certified Authority certificate in its trusted store, it can trust that the server is actually the Web site you access.

TLS uses certificates managed by a public key infrastructure (PKI) to guarantee the identity of servers and clients. A certificate is a package containing a public key and information that identifies the owner and source of that key, and one or more certifications (signatures) to verify that the package is authentic. To sign a certificate, an issuer adds information about itself to the information already in the certificate request. The public key and identifying information are hashed and signed using the private key of the issuer's certificate.

Certificates are defined by the X.509 RFC standard, which includes fields that form a contract between the creator and consumer. The Enhanced Key Usage extension specifies the use for which the certificate is valid, including Server Authentication.

Enterprise and Collector Certificates

An Enterprise Certificate and one or more Collector Certificates enable secure HTTP Collector-Agent communication in VCM. The Enterprise Certificate enables VCM to operate in a multi-Collector environment. Agents have the Enterprise Certificate in their trusted certificate stores, which they use implicitly to validate any certificate issued by the Enterprise Certificate. All Collector Certificates are expected to be issued by the Enterprise Certificate, which is critical in environments where a single Agent is shared between two collectors.

Server Authentication is required to establish a TLS connection with an Agent. All Collectors should have a common Enterprise Certificate. Each Collector Certificate is issued by the Enterprise Certificate, and is capable of Server Authentication.

- The Collector Certificate is used to initiate and secure a TLS communication channel with an HTTP Agent. The Agent must be able to establish that the Collector Certificate can be trusted, which means that the Collector Certificate is valid and the certification path starting with the Collector Certificate ends with a trusted certificate. By design, the Enterprise Certificate is installed in the Agent's trusted store, and the chain ends with the Enterprise Certificate.
- A Collector Certificate can also be used to issue Agent certificates. As long as all Collector Certificates are issued by the same Enterprise Certificate, any Agent Certificate may be issued by any Collector Certificate, and all Agents will be able to trust all Collectors. Similarly, all collectors will be able to validate all Agent Certificates. Agent Certificates are used for Mutual Authentication only. Mutual authentication is supported, but requires interaction with VMware Customer Support and a Collector Certificate that also has certificate signing capability.
- The Collector Certificate and associated private key must be available to the Collector. This certificate is stored in the (local machine) personal system store.

Collector Certificates in VCM must adhere to the requirements specified above in Secure Communications Certificates.

Delivering Initial Certificates to Agents

VCM Agents use the Enterprise Certificate to validate Collector Certificates. Therefore, the Agent must have access to the Enterprise Certificate as a trusted certificate. In most cases, VCM will deliver and install the Enterprise Certificate as needed.

- Installing the Agent from a Disk (Windows only): The VCM Installation DVD does not contain customer-specific certificates. If HTTP is specified, the manual VCM Installer requests the location of the Enterprise Certificate file during the installation. You must have this file available at installation time. The certificate file (with a .pem extension) can be copied from the CollectorData folder of the Collector. This will be the case whether you run the manual installer directly (CMAgentInstall.exe) or use the "Agent Only" option from the DVD auto-run program.
- Using CMAgentInstall.exe to Install the Agent (Windows only): CMAgentInstall.exe or CMAgent[version].msi is the manual Agent installer program. The manual installer will request the location of the Enterprise Certificate file, if HTTP is specified. You must have this file available at installation time. The certificate file can be copied from the CollectorData folder of the Collector.
- MSI Install Package: If HTTP is specified, the MSI agent install package also requires access to the .pem file.
- Installing the Agent for UNIX/Linux: See [Installing the VCM Agent on UNIX/Linux Machines](#) in this document.

Installing the Agent Using a Provisioning System

For Windows®, the manual installation program is available in .exe and .msi formats. Both versions allow the Enterprise Certificate file to be specified with a command line switch. You may also omit the certificate installation step by use of a command line switch. When these programs are run through a provisioning system, you must ensure that the Enterprise Certificate is available (and still secure), and configure the program options appropriately. Alternatively, you may choose to push the Enterprise Certificate to Agents by some other means and configure the provisioning system to omit certificate installation.

For UNIX/Linux, each UNIX/Linux installation package is targeted for one or more supported platforms. To install the UNIX/Linux Agent using a provisioning system, extract the installation package as appropriate and then deploy the extracted file with the provisioning system. The Enterprise Certificate is embedded in the installation package on the Collector.

For more information about Installing the Agent on UNIX/Linux Machines and UNIX/Linux packages and platforms, refer to section [Installing the VCM Agent on UNIX/Linux Machines](#).

Understand Use of FIPS Cryptography by VCM

Federal Information Processing Standards (FIPS) are developed by the US National Institute of Standards (NIST) and the Canadian Communications Security Establishment (CSE). VCM incorporates cryptographic service providers that conform to these FIPS standards:

- FIPS 140-2: Security Requirements for Cryptographic Modules
- FIPS 46-3: Data Encryption Standard (DES)
- FIPS 81: DES Modes of Operation
- FIPS 113: Computer Data Authentication
- FIPS 171: Key Management
- FIPS 180-1: Secure Hash Standard (SHA-1)
- FIPS 186-2: Digital Signature Standard (DSA) and Random Number Generation (RNG)
- FIPS 198: Message Authentication Codes (MACs) using SHA-1
- FIPS 197: Advanced Encryption Standard (AES) Cipher
- FIPS 200: Federal Information Security Management Act (FISMA)
- SP 800-2: Public Key Cryptography (including RSA)
- SP 800-20: Triple DES Encryption (3DES) Cipher

VCM Use of Microsoft Cryptographic Service Providers (CSPs) for Windows Machines

On Windows machines, VCM uses cryptography by way of the Microsoft CryptoAPI, which is a framework that dispatches to Microsoft Cryptographic Service Providers (CSPs). CSPs are not shipped with VCM or installed by VCM, but instead are part of the security environment included with Microsoft Windows. In the configurations supported by VCM, these CSPs are FIPS 140-2 validated. An up-to-date table of FIPS certificate numbers is at: <http://technet.microsoft.com/en-us/library/cc750357.aspx>.

Cryptography for UNIX/Linux Platforms

On UNIX/Linux platforms, the VCM Agent uses the cryptography of the OpenSSL v0.9.7 module. This cryptographic library is installed with the VCM Agent.

Cryptography used in VCM Software Components

VCM uses various software components that also use cryptography. Microsoft IIS, Internet Explorer, and SChannel (SSL/TLS) systems call the CryptoAPI, and thus use the Windows FIPS-validated modules. VCM for Virtualization uses ActiveX COM components from WeOnlyDo! Software (WOD) for SSH and SFTP services. WOD utilizes the FIPS 140-2 compliant OpenSSL library.

Table 1-1. Installed or Used Cryptography Modules

System	Platform	OpenSSLFIPS 1.1.2	OpenSSLFIPS 1.1.1	OpenSSLCrypt 0.9.7	Crypto++	CryptoAPI
UI	Windows					Used
VCMServer	Windows				Installed	Used
Virt Proxy	Windows	Installed				Used
AD Agent	Windows					Used
Win Agent	Windows					Used
UNIX Agent	HP/UX			Installed		Installed
	AIX			Installed		Installed
	Solaris			Installed		Installed
	Debian		Installed			Installed
	Red Hat		Installed			Installed
	SUSE		Installed			Installed
ESX Server	All	No cryptography modules are used or installed on ESX.				

Supported Windows and UNIX Platforms

Supported Windows and UNIX platforms, and their architectures, are listed in the *VCM Hardware and Software Requirements Guide*. For information about TLS, see *Transport Layer Security (TLS) Implementation for VCM* on the Download VMware vCenter Configuration Manager.

Installing VCM

Use Installation Manager to install VCM and all of its components and tools.

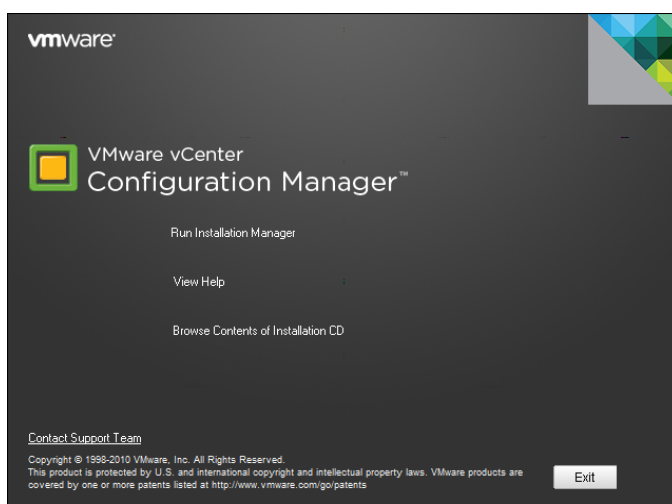
To install only the VCM tools, follow the installation procedures in ["Installing and Getting Started with VCM Tools" on page 233](#).

IMPORTANT Before you migrate VCM to VCM 5.4, read [Migrating VCM and Related Components](#).

VMware vCenter Configuration Manager (VCM) Installation Manager is a standalone application that checks your machine to ensure it is properly configured and configures licensed components during the installation process.

When you install VCM and related components, read about each configurable component to ensure you supply the appropriate information. The default settings may not fit your configuration exactly. If you migrate VCM or SQL Server, or migrate to a 64-bit system, see ["Upgrading or Migrating vCenter Configuration Manager" on page 45](#).

When you insert the installation CD into the machine to install VCM, the initial installation screen appears and displays several options.



If the installation screen does not appear automatically, or if you begin the installation from a network location, navigate to the CD root directory or the file share and double-click `setup.exe`.

1. Select one of these options:
 - **Run Installation Manager.** Starts Installation Manager and begins the installation.
 - **View Help.** Displays the Installation Manager Help, which describes the selections that appear during the installation.
 - **Browse Contents of Installation CD.** Starts Windows Explorer and displays the content of the installation CD, which includes documentation.
 - **Contact Support Team.** Displays instructions to contact VMware Customer Support.
 - **Exit.** Closes Installation Manager.
2. Click **Run Installation Manager** to begin the installation process.
3. Follow the steps through the wizard to complete the installation. For details about the installation options, see the Installation Manager Help.

After the installation completes, configure SQL Server settings to configure the database file growth and database recovery settings to fine-tune your VCM Database. See the instructions in ["Maintaining VCM After Installation" on page 237](#).

CAUTION During the installation, a folder containing VCM-related MSI files is added to %windir%\Installer\. If you move or delete the contents of this folder, you will not be able to use Installation Manager to upgrade, repair, or uninstall VCM successfully.

Installing and Configuring the OS Provisioning Server and Components

3

The Operating System (OS) Provisioning server installs OS distributions on target machines. The OS Provisioning server is installed and configured on a Red Hat server, and then operating systems are imported into the OS Provisioning Server repository. After the distributions are imported, the server manages the installation process.

When the OS Provisioning server is installed, configured, and OS distributions have been imported, you then use VCM to provision target machines with an operating system. See ["About OS Provisioning" on page 177](#) for more information.

Installing the Operating System Provisioning Server

VCM OS provisioning supports one instance of VCM with one instance of the Operating System (OS) Provisioning Server.

You must first configure the server to meet the prerequisites specified in the *VCM Hardware and Software Requirements Guide*, install the OS Provisioning Server application, and then perform post-install configurations.

Best Practices

Configure your OS Provisioning Server in a private or restricted network. When provisioning machines, connect the machines to the private network. This practice maintains security during the provisioning process.

For additional security information, see *VMware vCenter Configuration Manager Security Environment Requirements White Paper*.

Install the OS Provisioning Server

The OS Provisioning Server manages the installation of operating system distributions on target machines. You install the OS Provisioning Server using supplied media or media images. The installation must be run as the root user for the installation to complete correctly.

Prerequisites

- Ensure the machine meets all the prerequisites to installation specified in the *VCM Hardware and Software Requirements Guide*.
- Disable SELinux to allow the loading of shared libraries.

Procedure

1. Mount the VCM-OS-Provisioning-Server-<version number>.iso by either attaching to the media image or mounting the image.

When mounting the image, do not use the no-exec option.

2. Change the directory to where the image is located.

```
cd /<OS Provisioning Server ISO>
```

where <OS Provisioning Server ISO> is the path to the mounted file.

3. Run the # ./INSTALL-ME-FIRST command to install the database package.

When completed, "The installation completed successfully" message is displayed.

For more information about the process if it fails, see the DB2 installation log at /tmp/db2setup.log.

4. Run the # ./INSTALL-ME-SECOND command to install the OS Provisioning Server software.

The `autoinstall -d -a y` utility can be used for unattended installation of OS Provisioning Server.

5. In the Nixstaller window, click **Next**.
6. On the dialog box, click **Continue**.
7. When the installation is completed, click **Close**.
8. Click **Finish**.
9. Run the # `service FastScale status` command to verify that the installation has completed successfully.

A successful installation displays results similar to the following (pid values vary):

```
FSrepository does not implement a status command
rsyslogd (pid 3335) is running...
fsmesgd (pid 3517) is running...
fsrepod (pid 3683) is running...
fsadmin (pid 12618 12617 12614 3785 3784 3783 3782 3781 3778 3777 3776 3753)
is running...
dhcpd (pid 3786) is running...
Checking Basic Server: EMC HomeBase Server (Database) is running (PID: 3951).
Checking Basic Server: EMC HomeBase Server is running (PID: 4143).
fsjobd (pid 4237) is running...
fshinvd (pid 4249) is stopped...
stunnel (pid 4262 4261 4260 4259 4258 4257) is running...
```

An unsuccessful installation either displays the following error message:

```
"FastScale: unrecognized service"
```

or a few of the above mentioned services might not be running. If so, review the logs to determine possible problems.

10. Run the commands to create the repository database.

This action destroys any existing repository information.


```
# su - fsrepo
[fsrepo@<machine name>~]$ create-repository
```

11. When the action completes, run the `[fsrepo@<machine name>~]$ exit` command.

If necessary you can review the `/opt/FastScale/home/fsrepo/fscreate-repo.log`.

The OS Provisioning Server maintenance commands can also be added to the root user's path. The default shell profiles are modified by OS Provisioning Server to add `/opt/FastScale/sbin` to the root account. When the user is root, the maintenance commands in `/opt/FastScale/sbin` are available in the default path and are available when the profile is reloaded.

12. Reboot the OS Provisioning Server to ensure that all related services are started in the correct order.
13. Run the `# service FastScale status` command to verify the OS Provisioning Server services after reboot.

A successful installation displays the same results as above.

What to do next

When you install the OS Provisioning Server, specific OS Provisioning users were created.

- `fsrepo`: Used to create the repository.
- `vcuser`: Used to run `basicimport` of distributions and for communication with VCM.

To ensure proper security, you must set the password for the `vcuser`. See ["Set the vcuser Password" on page 25](#).

Set the vcuser Password

The `vcuser` is used when importing distributions into the OS Provisioning repository and for communication between VCM and the OS Provisioning Server. You must not delete the user or change the permissions, but you should set the `vcuser` password based on your corporate standards.

Prerequisites

The OS Provisioning Server is installed.

Procedure

1. Log on to the OS Provisioning Server as root.
2. Run the `passwd vcuser` command.
3. Type the new password, and then confirm the password.

Configure DHCP

The recommended configuration for OS provisioning is to use a private isolated network set up specifically for OS provisioning. When using a private provisioning network, the best practice is to configure the DHCP server included with the OS Provisioning Server to provide addresses and network boot information to nodes connected to this isolated network. If, however, you are provisioning systems on a network shared for other uses, you will likely already have a DHCP server on the network. In this case, you must disable the OS Provisioning Server's DHCP server and configure your regular DHCP server to provide network boot information for machines to be provisioned. See ["Configure a DHCP Server other than the OS Provisioning Server" on page 26](#) for more information.

Whether you use a private provisioning network or a shared network you can use either the OS Provisioning Server DHCP server or a separate DHCP server; however, only one DHCP server should be active on any network, and the DHCP server will need to be able to “point” new systems to the OS Provisioning Server for discovery and provisioning.

The OS Provisioning Server provides DHCP services on the provisioning network by default. The DHCP server must be configured to listen on the private provisioning network interface.

Procedure

1. Open the `/opt/FastScale/etc/dhcpd.conf` file and configure the settings as necessary for your environment.

Option	Description
subnet	The IP address subnet of the private network interface. Default value: 10.11.12.0
netmask	The netmask of the subnet. Default value: 255.255.255.0
address range	The range of allocated IP addresses for the provisioned nodes. Default value: 10.11.12.100 – 10.11.12.200
broadcast-address	The broadcast address on the subnet. Default value: 10.11.12.255
next-server	The IP address of the private network interface. Default value: 10.11.12.1

Configure a DHCP Server other than the OS Provisioning Server

If you are provisioning using an external DHCP server, you must modify your regular DHCP network using this procedure.

Configuring the corporate DHCP server to use the IP address of the OS Provisioning Server for PXE Boot allows the nodes to connect to the OS Provisioning Server after DHCP had completed. When the nodes are set to NetBoot (PXE) on startup, the nodes download the boot kernel through TFTP from the OS Provisioning Server. For this process to work, you must turn off DHCP on the OS Provisioning Server.

Prerequisite

Turn off DHCP on the OS Provisioning Server.

Procedure

1. On the OS Provisioning Server, log in as root and edit `/etc/sysconfig/FSdhcpd` to prevent the DHCP resetting after a reboot.

```
Change DHCPD_CONF=/opt/FastScale/etc/dhcpd.conf
to DHCPD_CONF=/opt/FastScale/etc/dhcpd.conf.none
```

2. On the OS Provisioning Server, run the following command:

```
/opt/FastScale/etc/init.d/FSdhcpd stop
```

3. On the corporate DHCP server, update the `dhcpd.conf` file with the following options:

```
allow bootp;
allow booting;

next-server <IP address of the OS Provisioning Server>; where <IP address of the OS
Provisioning Server> is replaced with the specified IP address.
```

Configure TFTP

The OS Provisioning Server provides TFTP services on the provisioning network, which, by default, has a private IP address. The TFTP server must be configured to listen on this private network interface.

Procedure

1. Open the `/opt/FastScale/homebase-server/etc/channels/TFTP.xml` file and configure the settings as necessary for your environment.

Option	Description
<code>connectionActive</code>	Enables or disables TFTP server. A value of <code>true</code> enables the server, and a value of <code>false</code> disables the server. The default value is <code>true</code> .
<code>localHost</code>	The IP address of the private network interface. The default value is <code>10.11.12.1</code> .

The utility `fstftp_conf`, located in `/opt/FastScale/sbin`, can also be used to update the file.

2. If you make changes, restart the basic service using the `service FastScale FSbasic restart` command.

Uninstall the OS Provisioning Server

Uninstall the OS Provisioning Server by first mounting the OS Provisioning Server media, and then running the `uninstall` command. These programs must be run as the root user for the uninstall process to complete correctly.

CAUTION The uninstall process removes the application and deletes all the data stored in the database.

Procedure

1. Mount the OS Provisioning Server ISO by either attaching to the media image or mounting the image.
2. Change the directory to where the image is located.

```
cd /<OS Provisioning Server ISO Location>
```

where `<OS Provisioning Server ISO Location>` is the path to the mounted media.

3. Run the following command to uninstall the application:

```
./UNINSTALL-ME
```

4. Type **Yes**.

The following is a sample of the uninstall log:

```
[Thu Jul 22 08:57:06 IST 2010] UNINSTALL-ME: Starting uninstallation of
Application Stack Manager...

[Thu Jul 22 08:57:08 IST 2010] UNINSTALL-ME: FastScale service is running

[Thu Jul 22 08:57:08 IST 2010] UNINSTALL-ME: Stopping FastScale service
```

```
[Thu Jul 22 08:57:08 IST 2010] UNINSTALL-ME: Command : /sbin/service FastScale
stop
Shutting down FSnetfs: [ OK ]
Shutting down FSSyslog: [ OK ]
Shutting down FSmesgd: [ OK ]
Shutting down FSDhcpd: [ OK ]
.....
[Thu Jul 22 09:00:44 IST 2010] UNINSTALL-ME: Uninstallation complete!
```

Preparing Boot Images for Windows Provisioning

It is necessary to prepare a Windows boot image to successfully provision target Windows machines. The boot image, created once on a Windows machine and applied to the OS Provisioning Server, is used to meet the booting needs of the Windows distribution installations on target machines.

Create Windows Boot Image

You must create a Windows boot image and add it the OS Provisioning Server. The image is created on a Windows machine and deployed to the OS Provisioning Server.

Prerequisites

- Verify that the Windows Automated Install Kit (WAIK) is installed.
- Verify that Java Virtual Machine (JVM), version 1.6.0 or later, is installed.
- Verify that the OS Provisioning Server is accessible on the network to the Windows machine, usually the Collector, on which you are creating the image.

Procedure

1. Copy `/opt/FastScale/homebase-server` from the OS Provisioning Server to a directory on the Windows machines. For example, `c:\Program Files (x86)\VMware\VCM\Tools\homebase-server`.
2. On the OS Provisioning Server, import a supported Windows operating system using the `basicimport` command.
See ["Import Windows Distributions" on page 30](#) for more information.
3. On the Windows machine, change the directory to the `bin` directory in the `homebase-server` directory. For example, `c:\Program Files (x86)\VMware\VCM\Tools\homebase-server\bin`.
4. Run the create command.

```
hbd create windows --waik <Path to WAIK> -l <OS Provisioning Server Public IP>
--deploymenturl <OS Provisioning Server Private IP Address> -u <HB User> -p
<HB password>
```

Option	Description
<Path to WAIK>	Path to the WAIK installation. For example, "c:\Program Files (x86)\Windows AIK".
<OS	OS Provisioning Server's Public Interface IP Address.

Option	Description
Provisioning Server Public IP>	
<OS Provisioning Server Private IP>	OS Provisioning Server's Private Interface IP Address. The default configuration is 10.11.12.1. If provisioning the Windows AIK machine is connected to OS Provisioning Server using the deployment network, then the '--deploymenturl' option is not necessary. Instead, you should specify the deployment IP address as the argument to the '-l' option.
<HB User>	HomeBaseServer configured username. The default username is "admin".
<HB password>	HomeBaseServer configured password. The default password is "admin".

5. Verify that the boot image files are created on the OS Provisioning Server in `/opt/FastScale/homebase-server/deployment`.

Copy the VCM Certificate to the OS Provisioning Server for Linux Provisioning

If you are using the OS Provisioning Server to install Linux distributions, you must copy the VCM certificate file to the OS Provisioning Server to ensure the certificate is included with the VCM Agent when the configured session is created prior to provisioning.

Procedure

1. Copy the VCM certificate, `VMware_VCM_Enterprise_Certificate_*.pem`, located on the VCM Collector in `\Program Files (x86)\VMware\VCMAgent\CollectorData`, to the OS Provisioning Server `/opt/FastScale/var/fsadmin/basic/directory`.

Importing Distributions into the OS Provisioning Server Repository

Operating system distributions must be imported into the OS Provisioning Server repository before you can use VCM to install them on target machines. The `basicimport` command uses an `-i` option to specify an `.iso` and a `-d` option to specify directories.

The supported operating systems are listed in *VCM Hardware and Software Requirements Guide*.

Create Directories for Windows Distributions

Some Windows operating systems distribution files are issued on multiple CDs. Due to the dependencies within the packages, multiple CDs cannot be loaded using separate `basicimport` commands for each CD. You must create a single directory out of multiple Windows operating system CDs before importing.

Procedure

1. On the OS Provisioning Server, create a directory to contain the files from both CDs by typing:

```
# mkdir -p /tmp/<directory name>
```

For example, `# mkdir -p /tmp/Win2003-R2-SP2-Standard`

2. Insert the first CD in the drive and type:

```
# cp -R /media/cdrom/<source directory name> /tmp/<directory name>
```

For example, # cp -R /media/cdrom/Win2003-R2-SP2-Standard /tmp/Win2003-R2-SP2-Standard

3. Replace the first CD with the second CD and type:

```
# cp -R /media/cdrom/<source directory name> /tmp/<directory name>
```

For example, # cp -R /media/cdrom/Win2003-R2-SP2-Standard /tmp/Win2003-R2-SP2-Standard

When importing the second CD, do not replace any files if prompted during the copy operation.

Import Windows Distributions

Distributions are the operating system installation files. You must import each OS distribution into the OS Provisioning repository before you can use VCM to install it on target machines.

NOTE Importing distributions with spaces in the file name is not supported. Before importing, remove the spaces or replace the spaces with underscores.

Procedure

1. Mount the ISO by either attaching to the media image or mounting the image. For Windows 2008 and Windows 7, use -t udf mount type and do not include any spaces in the path. For all other Windows, use loopback. For example, \$ mount -oloop /<iso_file.iso> /<mount point>

NOTE Do not use -t iso9660 when mounting the image. Some automounted media will not import. If you receive a fingerprint error message during basicimport, unmount the directory and manually mount it without the -t iso9660 option.

2. Log in as vcmuser.
3. For your first import, type the command:

```
# basicimport -d /mnt/<directory name> -l <OS Provisioning Server IP address>
```

NOTE Changing the OS Provisioning Server IP address at a later time is not currently supported. If the initial IP address of the OS Provisioning Server after install is not the address you intend for it to have when it is put into production, you must change its address, and related DHCP and TFTP configurations, before you import any OS distributions.

For subsequent imports, the -l option is not necessary:

```
# basicimport -d /mnt/<directory name>/
```

Where the <directory name> is the file name. For example, Win2k3SE-R2-SP2-i386. If you created a /tmp/ directory for a multi-CD distribution, include the path. For example /tmp/<directory name>, or /tmp/Win2003-R2-SP2-Standard.

4. Type the **Family Name**.

For example, Windows. You must provide a unique family name to perform the basicimport of different operating systems in the same family. No other family can exist with the same combination of name, version, and architecture values.

5. Type the **Family Version**.

For example, 2008R2.

6. Type the **Family Architecture**, either i386 or x86_64

7. Type the **Provenance**.

For example, CD, hotfix, or SP.

8. The script runs as follows with a specific example:

```
Importing data into repository...
Importing source data...
No recipes are accessible.
Adding new recipe WINSERVER2003_std_r2_sp2BasicRecipe-2
Creating UCI WINSERVER2003_std_r2_sp2-BasicUCI.
Attaching UCI WINSERVER2003_std_r2_sp2-BasicUCI to recipe 2.
UCI WINSERVER2003_std_r2_sp2-BasicUCI is attached to recipe 2.
Updating the Summary data...
```

Import Linux/ESX Distributions

Distributions are the operating system installation files. You must import each OS distribution into the OS Provisioning repository before you can use VCM to install it on target machines.

NOTE Importing distributions with spaces in the file name is not supported. Before importing, remove the spaces or replace the spaces with underscores.

Linux, or ESX distributions use the following procedure. The SUSE distribution is issued on multiple DVDs; however, only the first disk is required and must be imported using the following procedure.

Procedure

1. On the OS Provisioning Server, log in as vcmuser.
2. For your first import, type the command:

```
# basicimport -i <distribution name>.iso -l <OS Provisioning Server IP
address>
```

NOTE Changing the OS Provisioning Server IP address at a later time is not currently supported. If the initial IP address of the OS Provisioning Server after install is not the address you intend for it to have when it is put into production, you must change its address, and related DHCP and TFTP configurations, before you import any OS distributions.

For subsequent imports, the -l option is not necessary:

```
# basicimport -i <distribution name>.iso
```

Where the <distribution name> is the iso file name. For example, ESX-4.0.0-update01-208167.

3. Type the **Family Name**.

For example, ESX. You must provide a unique family name to perform the basicimport of different operating systems in the same family. No other family can exist with the same combination of name, version, and architecture values.

4. Type the **Family Version**.

For example, 4.0ul.

5. Type the **Family Architecture**, either i386 or x86_64.

6. Type the **Provenance**.

For example, CD, hotfix, or SP.

7. The script runs as follows:

```

Importing data into repository...
Importing source data...
No recipes are accessible.
Adding new recipe ESX4.0ulBasicRecipe-2
Creating UCI ESX4.0ul-BasicUCI.
Attaching UCI ESX4.0ul-BasicUCI to recipe 2.
UCI ESX4.0ul-BasicUCI is attached to recipe 2.
Updating the Summary data...
#

```

basicimport Command Options

Use the `basicimport` command line options to import UNIX, Linux, ESX, or Windows distributions into the OS Provisioning repository.

Table 3-1. basicimport Command Options

Option	Description
-h	Help. Displays the basicimport options.
-d	Directory. Path to the media source directory. A required option when importing OS distributions issued on more than one media item, such as multiple DVDs.
-i	ISO file. Path and image name for the distribution. Used with importing distributions issued on one media source, such as a Red Hat distribution on a single DVD.
-l	IP address of the OS Provisioning Server.
-n	Family name. For example, ESX or Windows.
-V	Family version. For example, 4.0u1 or 2008r2sp2.
-a	Family Architecture. For example, i386 or x86_64.
-p	Provenance. Distribution source. For example, CD, hotfix, or SP.

Configuring the OS Provisioning Server Integration with the VCM Collector

Stunnel is used to establish secure communication between VCM and the OS Provisioning Server SOAP services. Use the following procedures, which include configuration information, to securely set up the Stunnel channel. These procedures assume the following:

- All private keys are RSA keys.

Certificates are created or obtained, and copied to the required locations using industry best practices.

- **On the VCM Collector:**

Copy certificate to c:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\vcm_stunnel_cert.pem.

Copy private key to c:\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\vcm_stunnel_pk.pem.

- **On the OS Provisioning Server:** Copy certificate to /opt/FastScale/var/certs/vcm_stunnel_cert.pem
- All directories where these keys and certificates are stored are appropriately secured.

Configure Stunnel on the OS Provisioning Server

Stunnel is used to establish secure communication between VCM and the OS Provisioning Server SOAP services. On the OS Provisioning Server, you copy the certificates to the locations specified in the `stunnel.conf` file.

Procedure

1. Log into the OS Provisioning Server as root.
2. Place the VCM stunnel certificate validation chain in /opt/FastScale/var/certs as described in /opt/FastScale/etc/stunnel.conf.

All of the files in this directory are owned by root and have permissions of -rw-r--r--.

The stunnel configuration file on the OS Provisioning Server is /opt/FastScale/etc/stunnel.conf.

```
; stunnel configuration file for server proxy
; Some performance tunings
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
; debug = 7
cert = /opt/FastScale/var/certs/service.pem
key = /opt/FastScale/var/certs/private/service.key
; Either CAfile or CAPath, but not both, should be defined
; CAfile = /opt/FastScale/var/certs/ca-cert.pem
; Certificate Authority directory
; This is the directory in which stunnel will look for certificates
when using the verify.
; Note that the certificates in this directory should be named
; XXXXXXXX.0 where XXXXXXXX is the hash value of the DER encoded
subject of the
; cert (the first 4 bytes of the MD5 hash in least significant byte
order).
```

```

; The hash can be obtained with the command: openssl x509 -noout -in
cert.pem -hash
CApath = /opt/FastScale/var/certs
client = no
foreground = no
output = /opt/FastScale/logs/stunnel.log
pid = /opt/FastScale/logs/stunnel.pid
[fsmesgds]
accept = 40610
connect = localhost:21310
; Authentication stuff
verify = 3
[fsre pods]
accept = 40607
connect = 127.0.0.1:21307
; Authentication stuff
verify = 3

```

3. Restart stunnel.

```
service FastScale restart
```

What to do next

After configuring the Stunnel on the OS Provisioning server, you must configure the communication on the VCM Collector. See ["Configure Stunnel on the VCM Collector" on page 40](#).

Configure Stunnel on the VCM Collector

The VCM Collector installation installs Stunnel files to establish secure communication between VCM and the OS Provisioning Server SOAP services. You perform this configure Stunnel to ensure the connection on the Collector is operational.

Prerequisites

- Before placing the VCM Stunnel certificate and the VCM Stunnel private key, you must ensure the files are secured according to your corporate best practices.
- Verify that you have a [C:] \Program Files (x86) \VMware \VCM \Tools \sTunnel \certs \ directory. If the directory does not exist, create it.
- Verify that you have a [C:] \Program Files (x86) \VMware \VCM \Tools \sTunnel \key \ directory. If the directory does not exist, create it.

Procedure

1. Place the VCM Stunnel certificate in
[C:]\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\vcml_stunnel_cert.pem.
2. Place the VCM Stunnel RSA private key in
[C:]\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\vcml_stunnel_pk.pem.
3. Place the OS Provisioning Server Stunnel CA certificate validation chain in the file(s) and directory specified in the stunnel.conf file.

The VCM Stunnel configuration file on the VCM application server is [C:]\Program Files (x86)\VMware\VCM\Tools\stunnel.conf.

In Stunnel.conf, you should update the path for cert, key, CAfile or CApath, depending on where you installed VCM.

```
cert = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\vcml_stunnel_
cert.pem

key = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\vcml_stunnel_pk.pem

;; Use stunnel in client mode

client = yes

;; FIPS mode can be enabled as desired

fips = no

;; Some performance tunings

socket = l:TCP_NODELAY=1

socket = r:TCP_NODELAY=1

;; Either CAfile or CApath, but not both, should be defined

;; CAfile contains the certificate chains needed to verify the certificates of
remote connections

;CAfile = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\ca-cert.pem

;; CApath = directory

;; Certificate Authority directory

;; This is the directory in which stunnel will look for certificates when
using the verify.

;; Note that the certificates in this directory should be named

;; XXXXXXXX.0 where XXXXXXXX is the hash value of the DER encoded subject of
the

;; cert (the first 4 bytes of the MD5 hash in least significant byte order).

;; The hash can be obtained with the command: openssl x509 -noout -in cert.pem
-hash

CApath = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs

;; Some debugging stuff useful for troubleshooting

;debug = 7

;output = stunnel.log
```

```

;; verify = level
;; level 1 - verify peer certificate if present
;; level 2 - verify peer certificate
;; level 3 - verify peer with locally installed certificate
;; default - no verify
verify = 3

;; limit connections to certain ciphers
ciphers = AES128-SHA:DES-CBC3-SHA :@STRENGTH

;; asm_hostname_or_ip_address must be replaced with the correct value for the
OS Provisioning Server

[fsrepo]
accept = 127.0.0.1:21307
connect = asm_hostname_or_ip_address:40607

```

4. Update the accept and connect values in the [fsrepo] section.

Value	Action
accept = 21307	Update to accept = 127.0.0.1:21307
connect = asm_hostname_or_ip_address:40607	Update to the hostname or the IP address of the OS Provisioning Server

5. Run the commands from the Stunnel directory to register and start the Stunnel service.

```

cd c:\Program Files (x86)\VMware\VCM\Tools\sTunnel
stunnel -install
net start stunnel

```

What to do next

Verify that the communication between the OS Provisioning server and the VCM Collector is properly configured. See ["Confirm Stunnel Configuration" on page 42](#).

Confirm Stunnel Configuration

You must confirm that Stunnel communication between the OS Provisioning server and the VCM Collector is configured and active before provisioning machines.

Prerequisites

- Configure Stunnel on the OS Provisioning Server as described in ["Configure Stunnel on the OS Provisioning Server" on page 39](#).
- Configure Stunnel on the VCM Collector as described in ["Configure Stunnel on the VCM Collector" on page 40](#).

Procedure

1. From the VCM Collector, start Internet Explorer and go to `http://localhost:21307/`.

If the connection is properly configured, the following message is displayed.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:t="urn:types.fastscale.com"
xmlns:dos="urn:bobdos.fastscale.com" xmlns:wsns="http://tempuri.org/wsns.xsd"
xmlns:fst="urn:bob.fastscale.com">
- <SOAP-ENV:Body>
- <SOAP-ENV:Fault>
<faultcode>SOAP-ENV:Client</faultcode>
<faultstring>HTTP GET method not implemented</faultstring>
</SOAP-ENV:Fault>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

If the connection is not working, the page displays `Web page not found`. Review your Stunnel configuration files and make any necessary corrections.

Maintaining Operating System Provisioning Servers

The maintenance of the OS Provisioning server includes backing up the repository, restoring the repository after a disaster or machine failure, and managing system logs.

Backup the OS Provisioning Repository

The OS Provisioning server includes a repository containing your imported OS distributions. To avoid recreating the distributions if the server fails, you should back up the repository as part of your recovery plan.

Prerequisites

- Ensure that you have sufficient disk space available on your machine for the backed up files. Use the `du -sk /opt/FastScale` command to check the amount of space used by the OS Provisioning Server files.
- Make certain no OS Provisioning actions are currently in progress. The backup process forces all applications to exit, including OS Provisioning daemons, FSadmin, and FSrepod.

Procedure

1. Log in as the fsrepo user.

```
# su - fsrepo
```

2. Run the backup command to backup the repository files to /tmp/fs-backup.

```
[fsrepo@localhost~]$ mkdir /tmp/fs-backup
[fsrepo@localhost~]$ db2 CONNECT TO FSREPO;
[fsrepo@localhost~]$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
[fsrepo@localhost~]$ db2 CONNECT RESET;
[fsrepo@localhost~]$ db2 BACKUP DATABASE FSREPO TO /tmp/fs-backup WITH 2
BUFFERS BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
[fsrepo@localhost~]$ db2 CONNECT TO FSREPO;
[fsrepo@localhost~]$ db2 UNQUIESCE DATABASE;
[fsrepo@localhost~]$ db2 CONNECT RESET;
[fsrepo@localhost~]$ exit

# service FastScale restart
```

3. Using a backup manager, one that preserves siblings, permissions, and ownership of files, create backup copies of the required files and directories.

- /opt/FastScale/homebase-server/deployment
- /opt/FastScale/homebase-server/etc/
- /opt/FastScale/homebase-server/keys/
- /opt/FastScale/homebase-server/packages
- /opt/FastScale/homebase-server/profiles
- /opt/FastScale/var/fsadmin/basic

4. Go to /opt/FastScale/homebase-server/bin and run the command to make a snapshot of the database contents.

```
./hbs.sh db dump -u admin -p admin <zip file>
```

Restore the OS Provisioning Repository From Backup

To recover from a OS Provisioning server failure, you reload the databases and restore the files you back up as part of your recovery plan.

Prerequisites

Verify that the OS Provisioning Server is installed.

Procedure

1. Log in as the fsrepo user.

```
# su - fsrepo
```

2. Run the command to restore the database from the backup directory.

```
[fsrepo@localhost~]$ db2 CONNECT TO FSREPO;
[fsrepo@localhost~]$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
```

```
[fsrepo@localhost~]$ db2 CONNECT RESET;

[fsrepo@localhost~]$ db2 RESTORE DATABASE FSREPO FROM /tmp/fs-backup TAKEN AT
<timestamp> WITH 2 BUFFERS BUFFER 1024 PARALLELISM 1 WITHOUT PROMPTING;

[fsrepo@localhost~]$ db2 CONNECT TO FSREPO;

[fsrepo@localhost~]$ db2 UNQUIESCE DATABASE;

[fsrepo@localhost~]$ db2 CONNECT RESET;

[fsrepo@localhost~]$ exit
```

3. Restore the required files from the backup location to the OS Provisioning server.
 - /opt/FastScale/homebase-server/deployment
 - /opt/FastScale/homebase-server/etc/
 - /opt/FastScale/homebase-server/keys/
 - /opt/FastScale/homebase-server/packages
 - /opt/FastScale/homebase-server/profiles
 - /opt/FastScale/var/fsadmin/basic
4. Go to /opt/FastScale/homebase-server/bin and run the command to restore the database snapshot.


```
./hbs.sh db load -u admin -p admin <zip file>
```
5. Reboot the OS Provisioning server.

What to do next

After restoring the repository, you must configure the communications. See "[Configure Stunnel on the OS Provisioning Server](#)" on page 39.

Configure Stunnel on the OS Provisioning Server

Stunnel is used to establish secure communication between VCM and the OS Provisioning Server SOAP services. On the OS Provisioning Server, you copy the certificates to the locations specified in the `stunnel.conf` file.

Procedure

1. Log into the OS Provisioning Server as root.
2. Place the VCM stunnel certificate validation chain in /opt/FastScale/var/certs as described in /opt/FastScale/etc/stunnel.conf.

All of the files in this directory are owned by root and have permissions of -rw-r--r--.

The stunnel configuration file on the OS Provisioning Server is

/opt/FastScale/etc/stunnel.conf.

```
; stunnel configuration file for server proxy
```

```
; Some performance tunings
```

```
socket = l:TCP_NODELAY=1
```

```
socket = r:TCP_NODELAY=1
```

```
; debug = 7
```

```
cert = /opt/FastScale/var/certs/service.pem
```

```

key = /opt/FastScale/var/certs/private/service.key
; Either CAfile or CAPath, but not both, should be defined
; CAfile = /opt/FastScale/var/certs/ca-cert.pem
; Certificate Authority directory
; This is the directory in which stunnel will look for certificates
when using the verify.
; Note that the certificates in this directory should be named
; XXXXXXXX.0 where XXXXXXXX is the hash value of the DER encoded
subject of the
; cert (the first 4 bytes of the MD5 hash in least significant byte
order).
; The hash can be obtained with the command: openssl x509 -noout -in
cert.pem -hash
CApath = /opt/FastScale/var/certs
client = no
foreground = no
output = /opt/FastScale/logs/stunnel.log
pid = /opt/FastScale/logs/stunnel.pid
[fsmsgds]
accept = 40610
connect = localhost:21310
; Authentication stuff
verify = 3
[fsrepods]
accept = 40607
connect = 127.0.0.1:21307
; Authentication stuff
verify = 3

```

3. Restart stunnel.

```
service FastScale restart
```

What to do next

After configuring the Stunnel on the OS Provisioning server, you must configure the communication on the VCM Collector. See ["Configure Stunnel on the VCM Collector" on page 40](#).

Configure Stunnel on the VCM Collector

The VCM Collector installation installs Stunnel files to establish secure communication between VCM and the OS Provisioning Server SOAP services. You perform this configure Stunnel to ensure the connection on the Collector is operational.

Prerequisites

- Before placing the VCM Stunnel certificate and the VCM Stunnel private key, you must ensure the files are secured according to your corporate best practices.
- Verify that you have a [C:]\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\ directory. If the directory does not exist, create it.
- Verify that you have a [C:]\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\ directory. If the directory does not exist, create it.

Procedure

1. Place the VCM Stunnel certificate in
[C:]\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\vcml_stunnel_cert.pem.
2. Place the VCM Stunnel RSA private key in
[C:]\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\vcml_stunnel_pk.pem.
3. Place the OS Provisioning Server Stunnel CA certificate validation chain in the file(s) and directory specified in the stunnel.conf file.

The VCM Stunnel configuration file on the VCM application server is [C:]\Program Files (x86)\VMware\VCM\Tools\stunnel.conf.

In stunnel.conf, you should update the path for cert, key, CAfile or CAPath, depending on where you installed VCM.

```
cert = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\vcml_stunnel_
cert.pem

key = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\vcml_stunnel_pk.pem

;; Use stunnel in client mode

client = yes

;; FIPS mode can be enabled as desired

fips = no

;; Some performance tunings

socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1

;; Either CAfile or CAPath, but not both, should be defined

;; CAfile contains the certificate chains needed to verify the certificates of
remote connections

;CAfile = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\ca-cert.pem

;; CAPath = directory

;; Certificate Authority directory

;; This is the directory in which stunnel will look for certificates when
using the verify.

;; Note that the certificates in this directory should be named

;; XXXXXXXXX.0 where XXXXXXXXX is the hash value of the DER encoded subject of
the
```

```

;; cert (the first 4 bytes of the MD5 hash in least significant byte order).
;; The hash can be obtained with the command: openssl x509 -noout -in cert.pem
-hash
CApath = C:\Program Files (x86)\VMware\VC\Tools\sTunnel\certs
;; Some debugging stuff useful for troubleshooting
;debug = 7
;output = stunnel.log
;; verify = level
;; level 1 - verify peer certificate if present
;; level 2 - verify peer certificate
;; level 3 - verify peer with locally installed certificate
;; default - no verify
verify = 3
;; limit connections to certain ciphers
ciphers = AES128-SHA:DES-CBC3-SHA :@STRENGTH
;; asm_hostname_or_ip_address must be replaced with the correct value for the
OS Provisioning Server

[fsrepo]
accept = 127.0.0.1:21307
connect = asm_hostname_or_ip_address:40607

```

4. Update the accept and connect values in the [fsrepo] section.

Value	Action
accept = 21307	Update to accept = 127.0.0.1:21307
connect = asm_hostname_or_ip_address:40607	Update to the hostname or the IP address of the OS Provisioning Server

5. Run the commands from the Stunnel directory to register and start the Stunnel service.

```

cd c:\Program Files (x86)\VMware\VC\Tools\sTunnel
stunnel -install
net start stunnel

```

What to do next

Verify that the communication between the OS Provisioning server and the VCM Collector is properly configured. See ["Confirm Stunnel Configuration" on page 42](#).

Confirm Stunnel Configuration

You must confirm that Stunnel communication between the OS Provisioning server and the VCM Collector is configured and active before provisioning machines.

Prerequisites

- Configure Stunnel on the OS Provisioning Server as described in ["Configure Stunnel on the OS Provisioning Server" on page 39.](#)
- Configure Stunnel on the VCM Collector as described in ["Configure Stunnel on the VCM Collector" on page 40.](#)

Procedure

1. From the VCM Collector, start Internet Explorer and go to `http://localhost:21307/`.

If the connection is properly configured, the following message is displayed.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:t="urn:types.fastscale.com"
xmlns:dos="urn:bobdos.fastscale.com" xmlns:wsns="http://tempuri.org/wsns.xsd"
xmlns:fst="urn:bob.fastscale.com">
- <SOAP-ENV:Body>
- <SOAP-ENV:Fault>
<faultcode>SOAP-ENV:Client</faultcode>
<faultstring>HTTP GET method not implemented</faultstring>
</SOAP-ENV:Fault>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

If the connection is not working, the page displays `Web page not found`. Review your Stunnel configuration files and make any necessary corrections.

Managing the OS Provisioning Server System Logs

The OS Provisioning server generates the log files in the `/opt/FastScale/log` directory. You should monitor the space used and truncate the files if they begin to consume too much disk space on the server.

- `fsadmin.err`: Contains messages from the Apache web server.
- `fsadmin.log`: Lists internal commands from the Apache web server.
- `FSjobd.log`: Contains messages generated during the job build process.
- `FSmesgd.log`: Contains messages generated by the message daemon.
- `FSnetfs.log`: Contains messages from the FSnetfs service.
- `FSrepod.log`: Contains messages generated by the repository database server.
- `php.log`: Contains messages from the php interpreter used by the web server and the jobs build program.

Upgrading or Migrating vCenter Configuration Manager

4

When you migrate vCenter Configuration Manager (VCM), you must consider all aspects of your environment. Before you install VCM 5.4 and the related components and tools in your enterprise, you must make sure the Collector machine meets the requirements for the new version.

Upgrade and Migration Scenarios

A migration to VCM 5.4 means you will install a new 64-bit environment, including the operating system, SQL Server, and SQL Server Reporting Services, and possibly new hardware. Then you will migrate your existing VCM, SCM, or ECM installation to this new environment. An upgrade uses an existing Collector installation and upgrades the operating system, SQL Server, and VCM to the versions associated with the VCM 5.4 release.

Supported migration paths include:

- Migrate from a 32-bit or 64-bit environment running VCM, SCM, or ECM to VCM 5.4
- Migrate a split installation to a single-server installation of VCM 5.4

The only supported upgrade path is:

- Upgrade from a 64-bit single-server installation environment running VCM, SCM, or ECM to VCM 5.4

Supported versions for migration include:

- VMware VCM 5.3 or later
- EMC Ionix SCM 5.0 or later
- Configuresoft ECM 4.11.1 or later

Prerequisites

VCM 5.4 now supports 64-bit environments only, which include 64-bit hardware, a 64-bit operating system, and SQL Server 2008 R2. If you migrate from a 32-bit environment to a 64-bit environment, you must prepare your 64-bit environment for a VCM installation. For details about configuring a 64-bit machine as a Collector, see the *VCM Hardware and Software Requirements Guide*.

Before you migrate to VCM 5.4:

- Your version of VCM must be VMware VCM 5.3, EMC Ionix SCM 5.0 or later, or Configuresoft ECM 4.11.1 or later.
- The current VCM installation must be functional.
- Back up your content, including databases, the CMFILES\$ share, any files used to customize the Collector, any reports that are exported to a non-default location, and certificates.
- All running jobs must be complete and jobs must not be scheduled to begin during the migration process. The migration process stops the SQLAgent service, which prevents any new jobs from starting.
- All users must be logged off, and users must not attempt to access VCM for the duration of the migration process.
- To simplify the steps to reconfigure scheduled jobs and product logins, download the VCM SQL Migration Helper Tool from the VMware download site.
- If you upgrade VCM Remote, and want older agents to function properly, you must use the same name for the new Remote virtual directory that was used in your previous installation. If you change the Remote virtual directory name, all corresponding agents must be updated to reflect the new virtual directory.
- Your existing environment must include Microsoft .NET Framework required versions.
- Existing 32-bit environments must include SQL Server 2005 and SP3.
- Existing 64-bit environments must include 64-bit SQL Server 2005 and SP2 **and** 32-bit SQL Server Reporting Services and SSRS SP3. Prior to VCM 5.4, only the 32-bit of SSRS was supported in 64-bit VCM environments.

CAUTION Before you begin the migration, to avoid any potential loss of data you must back up your content, including databases, the CMFILES\$ share, any files used to customize the Collector, any reports that are exported to a non-default location, and certificates.

Back up Your Databases

Back up all of the databases used in your configuration. Depending on which version you migrate, the database names differ slightly.

Before you migrate from a previous version of VCM, back up these databases:

Table 4-1. Before You Migrate, Back Up Your Databases

If you migrate from	Back up these databases
VMware VCM	CSI_Domain, VCM, VCM_Coll, VCM_UNIX, ReportServer, master, and msdb
EMC Ionix SCM	CSI_Domain, SCM, SCM_Coll, SCM_UNIX, ReportServer, master, and msdb
Configuresoft ECM (versions 4.11.1 to 5.0)	CSI_Domain, ECM, ECM_Coll, ECM_UNIX, ReportServer, master, and msdb

Back up Your Files

Back up the entire content of the CMFILES\$ share. The default location is C:\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\ on 64-bit systems, or C:\Program Files\VMware\VCM\WebConsole\L1033\Files\ on 32-bit systems.

If your Collector was originally installed as EMC Ionix SCM or as Configuresoft ECM, this default path will be different.

If you customized the Collector, back up the relevant files.

If you exported reports to a non-default location, back up the relevant files.

Back up Your Certificates

Export and back up your Collector and Enterprise certificates.

Software Supported by the VCM Collector

The migration to VCM 5.4 requires that the VCM Collector be upgraded or migrated to:

- Windows Server 2008 R2
- SQL Server 2008 R2
- SQL Server 2008 R2 Reporting Services

NOTE Because Windows Server 2008 R2 is supported only on 64-bit hardware, if your Collector is currently installed on a 32-bit platform, see the *VCM Hardware and Software Requirements Guide* for information about system specifications.

For a complete list of requirements, see the *VCM Hardware and Software Requirements Guide*.

For questions about any of the migration procedures, contact VMware Customer Support before you begin the migration.

Migration Process

You can migrate these environments to support VCM 5.4:

- ["Migrate a 32-bit environment running VCM 5.3 or earlier to VCM 5.4" on page 50](#)
- ["Migrate a 64-bit environment running VCM 5.3 or earlier to VCM 5.4" on page 51](#)
- ["Migrate a split installation of VCM 5.3 or earlier to a single-server installation" on page 52](#)

To install VCM, you must obtain the installation package from the VMware download site or use the VCM 5.4 CD.

Prerequisites

For a list of prerequisites to install a new Collector, see the *VCM Hardware and Software Requirements Guide*.

Foundation Checker Must Run Successfully

As part of the migration process, Installation Manager runs Foundation Checker when you install VCM 5.4. Foundation Checker must complete successfully to ensure your machine is ready for the VCM 5.4 migration.

To run Foundation Checker as a standalone utility, see the *VCM Hardware and Software Requirements Guide*.

If errors occur when you run Foundation Checker, you must resolve the errors using the Foundation Checker online Help and the *VCM Hardware and Software Requirements Guide*.

Use the SQL Migration Helper Tool

When you migrate from one of the supported scenarios to VCM 5.4, to simplify the steps to recreate scheduled jobs and membership logins, use the SQL Migration Helper Tool, which you download from the VMware Web site.

Migrate Only Your Database

You can migrate the VCM database from version 4.11.1 or later. To migrate the database, you must:

1. Move the database to a prepared machine that has 64-bit SQL Server 2008 R2.
2. Attach the database to SQL Server 2008 R2.
3. Ensure that **sa** or the VCM service account is the owner of the newly attached database.
4. Install VCM 5.4.

Replace your existing 32-Bit Environment with the Supported 64-bit Environment

A 32-bit environment must be functional before you migrate to VCM 5.4. Before you start the migration, you must:

1. Replace the 32-bit architecture with 64-bit hardware.
2. Install Windows Server 2008 R2.

Prepare the Hardware

To prepare your hardware for the migration to VCM 5.4, you must replace your 32-bit Collector machine with a 64-bit machine.

Prepare the Software

To prepare your software for the migration to VCM 5.4:

1. Ensure that the existing installation of VCM is version 4.11.1 or later, and if not, use previous version installation packages and documentation to upgrade the installation to version 4.11.1 or later.
2. Install the supported 64-bit Windows Server 2008 R2 operating system.

Make Sure these Software Components are Installed

Older versions of VMware VCM, EMC Ionix SCM, and Configureoft ECM supported older versions of SQL Server. To migrate a 32-bit environment to VCM 5.4, the 32-bit environment must include these components, which must be installed in this order:

- SQL Server 2005
- 32-bit version of SQL Server Reporting Services
- SQL Server 2005 SP3
- VMware VCM 5.3, EMC Ionix SCM 5.0 or later, or Configuresoft ECM 4.11.1 or later

How to Recover Your Machine if the Migration is not Successful

If the migration is not successful, you must:

- Reinstall the versions of software that were installed on the machine before you started the migration.
- Reconnect the databases from your backed up copies.
- Recopy the files to the CMFILES\$ share.

Before you attempt to migrate to VCM 5.4 again, contact VMware Customer Support to help you identify the causes of an unsuccessful migration. For questions about any of the migration procedures, contact VMware Customer Support.

Migrate a 32-bit environment running VCM 5.3 or earlier to VCM 5.4

Your 32-bit environment must be functional before you migrate to VCM 5.4.

CAUTION Before you begin the migration, to avoid any potential loss of data you must back up your content, including databases, the CMFILES\$ share, any files used to customize the Collector, any reports that are exported to a non-default location, and certificates.

Procedure

1. Install Windows Server 2008 R2 on the machine that is to be the new 64-bit VCM Collector.
2. Install SQL Server 2008 R2.
3. Stop the VCM services, including the VCM Collector and VCM Patch Management services.
4. Use the SQL Migration Helper Tool to script any scheduled jobs on your old Collector so that you can import them into the new Collector.
5. Use the SQL Migration Helper Tool to build a script that contains the existing login and role membership information on the old Collector so that you can import the membership information into the new Collector.
6. Detach the databases.
7. Attach or restore the VCM databases to SQL Server 2008 R2 on the new Collector.
8. Make sure that the owner for the restored or attached databases is **sa** or the VCM service account.
(Optional) Use the built-in **sp_changedbowner** stored procedure to change the ownership of the databases.

9. Start the VCM 5.4 installation and select the **Install** option.

Make sure all of the components are marked for installation. If a component cannot be upgraded, the check box is cleared and a note appears indicating the reason. This situation can occur due to an invalid upgrade or an incomplete copy of the install image.

At the start of the installation, Foundation Checker will gather information about the machine to prepare it for the installation. For the upgrade to proceed, the results must be successful. If the system checks encounter errors, you must resolve the errors before you proceed.

CAUTION When you begin the VCM installation, do not select the **Repair** option unless you are directed by VMware Customer Support. The repair process requires access to your original installation media to check for missing files and settings, and replaces them.

10. During the installation, select the existing databases to migrate them to VCM 5.4, and follow the wizard to complete the upgrade. If you arrive at a step where the installation wizard asks you to create a new database, back out of this wizard and ensure that you have selected your existing database that you attached in the step above.
11. During the installation, do not select SSL unless your machine is already configured for SSL.
12. After the upgrade completes, copy the contents of `WebConsole\L1033\Files` from the previous Collector so that any remote commands, and discovery and imported template files, will be available on the new Collector.
13. On the Collector, run the script you created to import VCM scheduled jobs.
14. On the Collector, run the script you created to import VCM membership logins.
15. Re-import any custom SSRS report RDL files.

For information about the `sp_changedbowner` stored procedure, see SQL Server 2008 R2 Books Online.

Migrate a 64-bit environment running VCM 5.3 or earlier to VCM 5.4

An existing 64-bit Collector can be migrated to VCM 5.4. In the migration, you install a new system, copy over the VCM database and other components, and then install VCM 5.4 pointing to the existing database so that its configuration is preserved and its structure is updated.

Use this option when you want to refresh or replace the VCM hardware as part of the VCM 5.4 installation process, to change editions of the operating system, or if a fresh install of the operating system is preferred over an upgrade.

Your existing 64-bit environment must be functional before you migrate to VCM 5.4.

CAUTION Before you begin the migration, to avoid any potential loss of data you must back up your content, including databases, the CMFILES\$ share, any files used to customize the Collector, any reports that are exported to a non-default location, and certificates.

Procedure

1. Install Windows Server 2008 R2 on the machine that is to be the new 64-bit VCM Collector.
2. Install SQL Server 2008 R2.
3. Stop the VCM services, including the VCM Collector and VCM Patch Management services.
4. Use the SQL Migration Helper Tool to script any scheduled jobs on your old Collector so that you can import them into the new Collector.
5. Use the SQL Migration Helper Tool to build a script that contains the existing login and role membership information on the old Collector so that you can import the membership information into the new Collector.
6. Detach the databases.
7. Attach or restore the VCM databases to SQL Server 2008 R2 on the new Collector.
8. Make sure that the owner for the restored or attached databases is **sa** or the VCM service account.
(Optional) Use the built-in **sp_changedbowner** stored procedure to change the ownership of the databases.
9. Start the VCM 5.4 installation and select the **Install** option.

Make sure all of the components are marked for installation. If a component cannot be upgraded, the check box is cleared and a note appears indicating the reason. This situation can occur due to an invalid upgrade or an incomplete copy of the install image.

At the start of the installation, Foundation Checker will gather information about the machine to prepare it for the installation. For the upgrade to proceed, the results must be successful. If the system checks encounter errors, you must resolve the errors before you proceed.

CAUTION When you begin the VCM installation, do not select the **Repair** option unless you are directed by VMware Customer Support. The repair process requires access to your original installation media to check for missing files and settings, and replaces them.

10. During the installation, select the existing databases to migrate them to VCM 5.4, and follow the wizard to complete the upgrade. If you arrive at a step where the installation wizard asks you to create a new database, back out of this wizard and ensure that you have selected your existing database that you attached in the step above.

11. During the installation, do not select SSL unless your machine is already configured for SSL.
12. After the upgrade completes, copy the contents of `WebConsole\L1033\Files` from the previous Collector so that any remote commands, and discovery and imported template files, will be available on the new Collector.
13. On the Collector, run the script you created to import VCM scheduled jobs.
14. On the Collector, run the script you created to import VCM membership logins.
15. Re-import any custom SSRS report RDL files.

Migrate a split installation of VCM 5.3 or earlier to a single-server installation

A split installation is a previously supported configuration of VCM, where all of the databases except the main Collector database reside on a database server machine that is physically separate from the VCM Collector machine. In a split installation, the databases are located on two machines:

- **Collector machine.** Includes the VCM_Coll database only.
- **Database Server machine.** Includes the VCM, VCM_UNIX, ReportServer, master, and msdb databases.

If your previous environment was a split installation, you must migrate to a single-server installation for VCM 5.4. A single-server installation places all of the databases on the Collector machine.

CAUTION Before you begin the migration, to avoid any potential loss of data you must back up your content, including databases, the CMFILES\$ share, any files used to customize the Collector, any reports that are exported to a non-default location, and certificates.

To migrate a split installation to a single-server installation, during the installation you must select to attach the databases from the Database Server to SQL Server 2008 R2. See ["Migrate a 32-bit environment running VCM 5.3 or earlier to VCM 5.4" on page 50](#) for instructions.

After You Migrate VCM

After you migrate VCM:

- Import custom SRS reports.
- Import dashboard RDLs.
- If you did not use the SQL Migration Helper Tool, recreate your scheduled jobs and VCM user accounts and logins.
- Configure the SQL Server settings, including the VCM database file growth and database recovery settings to fine-tune your VCM database, as described in the chapter on maintaining VCM after installation.

Upgrade Process

You can upgrade your 64-bit environment that is running VCM 5.3 or earlier to VCM 5.4. Before starting an upgrade, you should perform the backup tasks mentioned in the prerequisites of this section, and you must verify that your existing Collector system meets the hardware requirements from the *VCM Hardware and Software Requirements Guide*.

To upgrade VCM, you must obtain the installation package from the VMware download site or use the VCM 5.4 CD.

To upgrade to VCM 5.4:

1. Upgrade the operating system to Windows Server 2008 R2.
2. Uninstall the 32-bit version of SQL Server Reporting Services (SSRS) 2005.
3. Upgrade SQL Server 2005 to SQL Server 2008 R2.
4. Run the SQL Server 2008 R2 installation again to add SQL Server Reporting Services 2008.
5. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > Reporting Services Configuration Manager** and configure SSRS 2008 to use the existing ReportServer database.
 - a. Select to use the existing ReportServer database.
 - b. Configure the Web Service and Report Manager URLs.
 - c. Use the Encryption Keys option to delete encrypted content so that the new installation of SSRS can use the existing SSRS database.
6. Run the VCM Installation Manager to upgrade the existing VCM installation to version 5.4.

After the installation completes, log in and begin using VCM.

After You Upgrade VCM

After you upgrade VCM, configure the SQL Server settings, including the VCM database file growth and database recovery settings to fine-tune your VCM database, as described in the chapter on maintaining VCM after installation.

Upgrading Existing Windows Agents

Use the Upgrade Agent wizard to upgrade the Agent files on one or more machines.

To upgrade an Agent:

1. Click **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines**.
2. Select the machine or machines you are upgrading, and then click the **Upgrade Agent** icon on the Licensed Windows Machines toolbar. The Machines page appears.
3. Select a machines option.

Option	Definition
All machines	Upgrade the Agent on all machines that appear in the list of licensed machines.
Filtered machines only	This option is available only if the Licensed Machines list is being filtered. Upgrade the Agent on all machines that appear in the filtered list of machines.
Selected machine(s) only	Upgrade the Agent only on select individual machines. Use the standard selection method to select individual machines.

4. Click **Next**. The **Install Options** page appears.
5. In the **Install From** field, select or verify the necessary information. Note that vCenter inspections will not work until you deploy the VCM 5.4 agent on the vCenter server system(s).

The default source of the Agent files is the Collector machine. If you have created an Alternate Source, you can select it from the drop-down list.

The Upgrade process:

- Will fail for any machine on which an Agent does not already exist.
 - Will use an Agent's current settings. For example, if the Agent uses DCOM, the Upgrade will maintain that setting, or if the Agent uses HTTP on Port 26542 the Upgrade will maintain that setting.
 - Will not upgrade components that do not require upgrading.
6. Click **Next**. The **Schedule** page appears.
 7. Schedule the operation. You can enter the Date in the specified format or click the Calendar icon.
 8. Click **Next**. The **Important** page appears.
 9. Verify the actions that will be performed and then click **Finish**.

Upgrading Existing Remote Clients

VMware recommends that you upgrade your Remote client versions. When the automatic upgrade setting (**Will Remote automatically upgrade old Remote clients**) is set to **Yes**, the next client-server contact automatically downloads and installs the upgrade files.

If the Remote client does not have a certificate, the upgrade process will automatically extract the certificate and send it to the client, along with the new Agent.

To automatically upgrade your remote clients:

1. Click **Administration > Settings > General Settings > VCM Remote**.
2. Select **Will Remote automatically upgrade old Remote clients**.
3. Click **Edit Setting**. The **Edit Setting** wizard appears.
4. Change the setting to **Yes**.
5. Click **Next**. The confirmation page appears.
6. Click **Finish**. The setting change is saved.

Upgrading Existing UNIX Agents

Upgrade packages are available to update the UNIX Agents on various platforms. To upgrade the UNIX Agents to the latest software release, use one of these methods:

- Upgrade the UNIX Agent(s) with the Local Package
- Upgrade the UNIX Agent(s) with a Remote Package

VCM supports TLS for UNIX/Linux. For more information, see the VCM TLS Implementation white paper, posted on the Download VMware vCenter Configuration Manager.

If you install the Agent on HP-UX 11.11, you must also install Patch PHSS_30966, which is required. If you need assistance, contact VMware Customer Support.

Upgrading Red Hat Workstations

In previous versions of VCM, either Red Hat workstations or servers were licensed as Red Hat servers. Beginning with VCM version 5.2.0, Red Hat machines were licensed as either workstations or servers. When you upgrade to 5.2.0 or later, the workstations previously managed with server licenses will be unmanaged in VCM. The unmanaged Red Hat workstations should be listed in the Available UNIX Machines list. To manage the machines in VCM, select **Administration > Machines Manager > Available Machines > Available UNIX Machines** and re-license the machines using Linux/Mac Workstation licenses.

If you are not able to identify your unmanaged Red Hat machines, contact VMware Customer Support.

Platforms Not Supported for Upgrade to 5.4 Agent

Installing or upgrading on the following platforms is supported only to the 5.1.3 UNIX Agent. You can install the 5.4 Agent. However, these platforms are not tested with any additional 5.4 functionality.

Platform	Supported Agent Version	Agent File Name
AIX 4.3.3	5.1.3	CMAgent.5.1.0.AIX.4
Red Hat 2.1	5.1.3	CMAgent.5.1.0.Linux.2.1
Solaris 2.5	5.1.3	Contact VMware Customer Support if you are installing or upgrading the Agent on this platform.
Solaris 2.6	5.2.1	Contact VMware Customer Support if you are installing or upgrading the Agent on this platform.

To Upgrade the UNIX Agent(s) with a Local Package

To upgrade the UNIX Agent(s) using the local upgrade package, follow these steps:

1. Locate the AgentUpgradeLocal.sh file in \Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\UNIX_Remote_Command_Files.
2. Open the AgentUpgradeLocal.sh file with a text editor like Wordpad.
3. In the AgentUpgradeLocal.sh file, locate the following entry:
CSI_INSTALL_PACKAGE_LOCATION = CHANGE_THIS_TO_A_LOCAL_OR_NFS_DIRECTORY
4. Change this entry to point to either a local directory or an NFS directory where the VCM Agent Install Packages are located (for example, /tmp/VCMu_Agent).

Agent install packages are installed on the Collector machine at \Program Files (x86)\VMware\VCM\Installer\Packages.
5. Save and close the AgentUpgradeLocal.sh file.
6. Log into VCM and open the Console slider. Navigate to **Console > UNIX Remote Commands > UNIX Agent Upgrade**. The UNIX Agent Upgrade data grid appears.
7. Select **Agent Upgrade - Local Package**.
8. Click **Run**. The Remote Commands wizard appears.
9. Select the machine(s) on which you want to upgrade the agent.

To determine which Agent is currently on a UNIX machine, navigate to **Administration > Machines Manager > Licensed Machines > Licensed UNIX Machines**. To determine the latest version number for the Agent, select **About > Versions**.
10. Click the arrow button to move the machines from the **Available list** to the **Selected list**. Click **Next**.
11. Select whether you want to upgrade the Agent now or later. To change the date, click the **Calendar** icon. When you schedule the action, it is placed in the **Administration > Job Manager > Scheduled** list.

The Time of Day settings you choose are based on your User time zone. All VCM jobs run based on the VCM Database time zone. You must account for the time and date differences between your VCM User time and your VCM Database time. For example, if your VCM Database server is in the Eastern time zone, and your VCM User is in the Pacific time zone, to run your job at midnight, you would enter 9 PM.
12. Click **Next**, and then click **Finish**.

To Upgrade the UNIX Agent(s) with a Remote Package

This method sends the upgrade package with the remote command to execute on the UNIX machine. The following remote upgrade packages are designed specifically for the various operating systems where the Agent(s) can be upgraded:

- AIX 4.3.3 Agent Upgrade (use only CMAgent.5.1.0.AIX.4)
- AIX 5 Agent Upgrade
- HP-UX (Itanium) Agent Upgrade
- HP-UX (PA-RISC) Agent Upgrade
- Red Hat Enterprise 2.1 Agent Upgrade (use only CMAgent.5.1.0.Linux.2.1)
- Red Hat Enterprise 3.0, 4.0, 5.0, 5.1, 5.2, SUSE Enterprise 9 and above Agent Upgrade
- Solaris (SPARC) Agent Upgrade
- Solaris (x86) Agent Upgrade

To upgrade the UNIX Agent(s) using one of the remote upgrade packages, follow these steps:

1. Select **Console > UNIX Remote Commands > UNIX Agent Upgrade**. The UNIX Agent Upgrade data grid appears.
2. Click to highlight the remote upgrade package that is appropriate for the operating system and version of the machine(s) that you want to upgrade.
3. Click Run and follow the wizard instructions to send the remote command and the upgrade package to the Agent(s) on the selected machine(s). The Agent will then execute the upgrade package.

Because the UNIX Agents are using TLS, the Enterprise Certificate is embedded in the Agent package. If multiple Collectors need to talk to a single Agent, all of the Collectors should share an Enterprise Certificate. If the Collectors have different Enterprise Certificates, the Enterprise Certificate from each Collector must be uploaded to the Agent. For more information, see the VCM TLS Implementation white paper, located on the Download VMware vCenter Configuration Manager.

Upgrading VCM for Virtualization

When upgrading vCenter collections, you must install the VCM 5.4 Agent or later on the Windows machines running vCenter. For more information, see ["Configuring vCenter Server Data Collections" on page 135](#).

When upgrading a Collector to VCM 5.4, the Agent Proxy on the Collector is automatically upgraded, and the Agent Proxy protected storage and user account configuration settings are preserved. However, for existing non-Collector Agent Proxy machines, you must upgrade VCM for Virtualization and select to retain the Secure Communication settings.

To upgrade the VCM for Virtualization Agent Proxy on non-Collector machines, you must use one of these methods, depending on your configuration:

- Manually Upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine
- Use VCM to Upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine

CAUTION When upgrading VCM for Virtualization, take the following precautions:

Do not change the password for the CSI Communication Proxy service. Doing so may require the Agent Proxy to be reinstalled and reconfigured.

Avoid installing the Agent Proxy and the Active Directory product on the same machine. The operations involved to install, uninstall, upgrade, and reinstall these products may result in the Agent Proxy needing to be reinstalled and reconfigured.

If you plan to uninstall VCM for Virtualization manually, make sure that you execute `RetainSecureCommSettings.exe` before uninstalling it. Otherwise, the Agent Proxy configuration settings will be removed, and the Agent Proxy will need to be reconfigured. The `RetainSecureCommSettings.exe` is located at: `C:\Program Files (x86)\VMware\VCM\Installer\Packages`, or in the path relative to where you installed the software.

Platform Not Supported for Upgrade to 5.4 Agent Proxy

You can install or upgrade an Agent Proxy machine only to the 5.1.3 Agent if it is collecting from this platform. This platform is not tested with the 5.4 functionality.

Platform	Supported Agent Version	Agent File Name
ESX 2.5	5.1.3	

Upgrading an Agent Proxy Machine

If a new version of the Agent Proxy becomes available, the upgrade process installs the newer version on your agent proxy machine.

1. Click **Administration > Machines Manager > Additional Components > VCM for Virtualization > Agent Proxies**. The **Agent Proxies** data grid appears.
2. Select the machine or machines on which you are upgrading the Agent Proxy.
3. Click **Upgrade**. The **Machines** page of the **Upgrade Agent Proxies** wizard appears.
4. The available machines are displayed in the upper list. The selected machines are displayed in the lower list. You can perform these actions:
 - **All Machines:** Selects the option to run the process on all eligible machines.
 - **Selected Machines Only:** (Default option) Selects the option to run the process on all machines listed in the lower pane.
 - **Filtered Machines:** Click **Define** to create a filter based on Machine Name or Domain Name, and then select the Filtered Machines option.
 - **Arrow buttons:** Selects a machine name in one of the panes and use the arrow buttons to move it from one pane to the other. Additionally, you may double-click a machine name to move it between panes.
5. Click **Next**. The **Option** page appears.
6. Configure the following options:
 - **Install From:** In the drop-down list, select the name of the Collector used to manage virtual machines.
 - **Schedule:** Select **Run Action now** to install immediately, or select **Schedule the Action to run later** and configure the settings to run at a designated time.

7. Click **Next**. The **Important** page appears. Review the contents, click **Back** to make any necessary alterations.
8. Click **Finish**. The Agent Proxy is upgraded at the time specified.
9. To verify the completion of the upgrade process, click **Jobs** on the Portal toolbar to access the Jobs Summary. You can also verify jobs for the past 24 hours if you think that you may have missed it. Go to **Administration > Job Manager > History > Other Jobs > Past 24 Hours**.

Manually Upgrading an Agent Proxy Machine

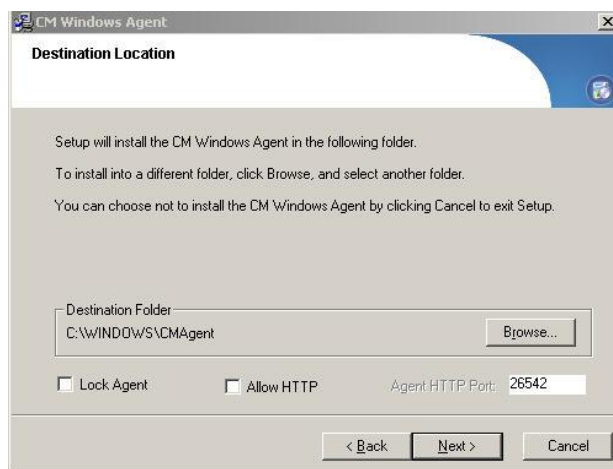
The steps in this section provide an optional upgrade method if you choose not to use the Upgrade option in VCM. To manually upgrade an Agent Proxy machine, you must have already upgraded your Collector machine to VCM 5.4. Then you will uninstall the VCM Agent, select to retain the Secure Communication settings, install the VCM Agent (version 5.4), and then install VCM for Virtualization, as described in these steps.

1. The following executable must be accessible from your non-Collector Agent Proxy Machine. The path to this file on the Collector machine is as follows, or is in the path relative to where you installed the software.

```
C:\Program Files (x86)\VMware\VCM\AgentFiles\CMAgentInstall.exe
```

Execute `CMAgentInstall.exe` on your Agent Proxy machine.

2. The installer detects the previous version of VCM, and then requests permission to uninstall it. Select **Yes**.
3. The installer detects that Secure Communication is installed, and requests whether you want to retain your settings. Select **Yes**. The installer proceeds to remove the VCM Virtualization product and VCM Agent from your Agent Proxy machine. During this process, your Secure Communication settings are retained.
4. When the installer displays the license agreement, read and accept the conditions.
5. The installer prompts whether to perform the installation of the VCM Windows Agent in HTTP mode. Allowing HTTP communication will allow the Agent to communicate through the HTTP port specified if DCOM is not available. Locking an Agent will prevent the Agent from being removed or upgraded. To use this mode, select **Allow HTTP** and click **Next**.



6. The installer proceeds with the installation. When the VCM Windows Agent has been successfully installed, click **Finish**.
7. Copy the following executable from your upgraded Collector machine to any location on your non-Collector Agent Proxy machine. The path to this file on the Collector machine is as follows, or is in the path relative to where you installed the software.

```
C:\Program Files
(x86)\VMware\VCM\AgentFiles\Products\VirtualizationProductInstall.exe
```

Run `VirtualizationProductInstall.exe` on your non-Collector Agent Proxy machine. This step begins the installation of VCM for Virtualization.

8. Proceed through the installation screens to install VCM for Virtualization.
9. The installer proceeds to install VCM for Virtualization. When VCM for Virtualization has installed successfully, click **Finish**. You can now begin collecting using your upgraded Agent Proxy.

NOTE If you have previously used this Agent Proxy to perform a collection from your upgraded Collector, the first collection may fail due to a password encryption issue. If so, try resetting the VM Host password at **Administration > Machines Manager > Additional Components > VCM for Virtualization > Licensed VM Hosts**. You may set the password for multiple hosts at the same time if desired.

All VCM-managed Windows machines will include the VCM Agent extension for VCM Provisioning, which is a separate installation.

For Agent Proxy machines, if the Virtualization proxy and VCM Agent extensions for Provisioning are installed, you must run `ProvisioningProductInstall.exe` from the Collector.

Upgrade the vSphere Client VCM Plug-In

Upgrading the plug-in is necessary only if you have a vSphere Client VCM Plug-In version 5.3 or earlier, or if the URL to the VCM instance has changed.

Prerequisites

Unregister the previous version of the vSphere Client VCM Plug-In. See ["Unregister the Previous Version of the vSphere Client VCM Plug-In" on page 146](#).

Procedure

1. Upgrade VCM.

What to do next

Register the new vSphere Client VCM Plug-In by following the instructions in ["Register the vSphere Client VCM Plug-In" on page 143](#).

Unregister the Previous Version of the vSphere Client VCM Plug-In

You must unregister a previous version of the vSphere Client VCM Plug-In before you can upgrade to the new version provided when you upgraded VCM. The upgrade to VCM removes files for the previous plug-in and installs the new plug-in files in new locations and with new names, but it does not register the new plug-in with the vSphere Client.

Procedure

1. Go to `https://vCenter machine name/mob/?moid=ExtensionManager`.
vCenter machine name represents the name of your vCenter Server 4.0 instance.
2. In the **Methods** area, click the **UnregisterExtension** link.
3. Type the string value for **extensionKey**:
`com.CM.VirtualCenterCompliancePlugIn`
4. Click **Invoke Method**.
The plug-in is unregistered.

Getting Started with VCM Components and Tools

5

This chapter covers global getting started procedures for VCM and all of its components and tools. After completing this chapter, proceed to the specific getting started chapters that apply to the components you have licensed and the VCM tools you plan to use. The remaining getting started chapters build on this one. Therefore, you should have a solid understanding of the content in this chapter before you proceed to the remaining chapters.

This chapter describes:

- [Understanding User Access](#)
- [Launching and Logging onto VCM](#)
- [Getting Familiar with the Portal](#)
- [Where to Go Next](#)

Understanding User Access

After your installation is complete, the user who performed the installation is explicitly granted access and is placed in the roles of ADMIN and USER. This user is also placed into the Admin role. Hence, this user can immediately log in using the Admin role. The role of AD_Admin allows full administration access to AD objects only.

Other user accounts can then be added after the Admin user logs in by going to **Administration > User Manager > VCM Logins**. For instructions on how to add user accounts, see the online Help.

Whenever a user is either added to the Admin role in VCM, or granted access to the **Administration > User Manager** node, the user is placed in the fixed machine roles Security Administrators and Bulk Insert Administrators Groups. They are also added to the database roles public, ADMIN, and User on 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 any particular user, more or fewer privileges may be needed in order for their role to function properly.

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$\Exported_Reports` folder for exporting reports.
- If default permissions have been changed, read access to the `C:\Program Files (x86)\VMware\VCM\WebConsole` directory, along with all subdirectories and files. In addition, any users who will be adding machines to VCM from a file or through the Add Machines action on Available Machines will need write access to `CMFiles$\Discovery_Files`.

Do Not Use the Collector as a Web Console

By default for localhost, Internet Explorer on Windows Server 2008 R2 runs with Protected Mode enabled. If you are logged in as an Administrator, because Protected Mode is enabled, problems can occur with the SQL Server Reporting Service (SSRS) Web service interface components such as dashboards and node summaries, or when using the License Manager Click Once application.

When you update a VCM license using the License Manager application from the Collector's Web console, you must run Internet Explorer as administrator.

CAUTION Although you should not use the Collector as a Web console, to restore the SSRS and License Manager functionality you can run Internet Explorer as administrator or disable Protected Mode for the zone of the Collector (localhost). If you perform either of these actions, 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.

Starting and Logging Onto VCM

If you have not already started VCM after closing Installation Manager, follow the procedure detailed below to start and log onto VCM.

IMPORTANT Before you start VCM, you must either configure 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 > Tools > Popup Blocker Settings** and then add the path for your Collector in the allowable address field.

How to Start VCM and Log On

1. If you are starting VCM on the Collector Machine, go to **Start > All Programs > VMware vCenter Configuration Manager > Web Console**. If you prefer to connect to VCM from another machine on your network, you may do so by pointing your browser to `http://<name_of_Collector_machine>/VCM`. For the specific browsers that are supported, see the *VCM Hardware and Software Requirements Guide*. The Logon screen appears.



2. Depending on your browser security settings, you may have to supply your user network credentials.
3. (Optional) Select **Automatically log on using this role** to have VCM automatically log you on without prompting you for a role in future logons.
4. Click **Log On**. The Portal appears.

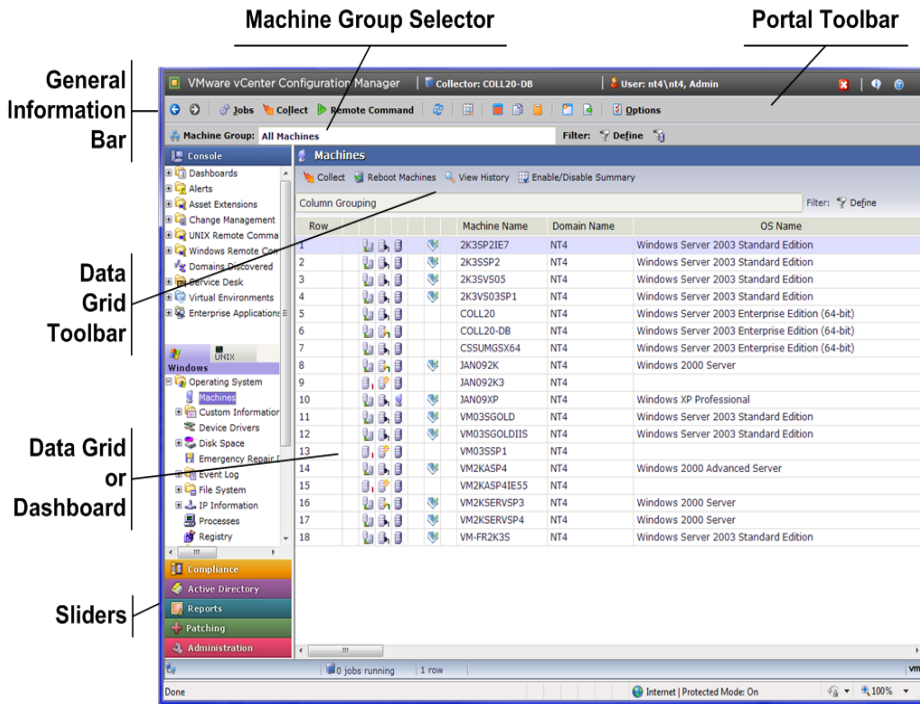
In the future, your VCM user account may have multiple roles. At that time, if you have the Automatically log on using this role option checked, VCM will automatically log you on as the User Role displayed on the Logon screen. To change roles, you must use the Logoff button in the top right corner of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

Getting Familiar with the Portal

The VCM portal provides access to all VCM features to manage your enterprise.

The portal uses a browser-based interface to run from any Windows machine that is running Internet Explorer, or Mozilla Firefox with the Internet Explorer tab plug in, that has access to the machine where VCM is installed.

Several major areas and controls exist in the Portal.



General Information Bar






The general information bar displays the VCM Collector’s (active SQL Server) name, your VCM user name and active Role, and these buttons:

- **Log Out.** Exits the Portal. The Portal closes, and the VCM Logon screen appears again.
- **About.** Displays information about how to contact VMware Customer Support. It also displays version information for VCM and all of its components. This information may be important when contacting VMware Customer Support.
- **Help.** Launches the online Help for the currently-active display.

Portal Toolbar

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

	The left and right arrow buttons navigate to the previous or next page in the data area.
	The Jobs button launches the Jobs Running status window. This button also provides access to the Collector status and allows you to stop/restart the Collector service.
	The Collect button launches a wizard allowing you to define and initiate data collections.
	The Remote Commands button allows you to invoke the Remote Commands wizard from the toolbar without having to access the node.
	The Refresh data grid view button refreshes the data grid view. Pressing F5 on the keyboard accomplishes this as well.
	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.
	The Select all displayed data rows button selects all the rows in the data grid.

	The Copy button is used to copy information from the selected rows in the data grid to the clipboard.
	The Copy link to clipboard button is used to copy the link of the content on-screen to the clipboard.
	Click the View data grid in separate window button to display the data grid in a separate window.
	The Export displayed data button exports data to a CSV formatted file. This file is exported to \\<name_of_collector_machine>\CMfiles\$\Exported Reports.
 Options	The Options button opens the User Options window. These settings pertain to the User who is logged on to VCM. All VCM Users will want to configure these to their individual preferences.

Sliders

The sliders on the left side of the Portal 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.

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

Select:	If you want to:
Console	<ul style="list-style-type: none"> ■ View, export, or print enterprise-wide, summary information. ■ Review or acknowledge current alert notifications. ■ Manage both VCM discovered and non-VCM discovered hardware and software assets. ■ Review changes that occurred from one collection to the next. ■ Create, edit, or run remote commands on a VCM managed Windows or UNIX machine. ■ View information about VCM discovered domains. ■ Navigate and manage VCM-integrated service desk events. ■ Manage VCM-managed virtual machines. ■ View your Windows NT Domain and Active Directory related data. ■ View information for enterprise-level applications. ■ Review non-security related UNIX machine-specific information. ■ Review UNIX security data to ensure consistent security configurations across your enterprise.
Compliance	<ul style="list-style-type: none"> ■ Create and manage Compliance rule groups and templates based on either AD objects* or machine group data.
Active Directory*	<ul style="list-style-type: none"> ■ View, export, or print enterprise-wide, summary information for Active Directory objects. ■ Review alert notifications for the selected AD location. ■ Review Active Directory-related changes that occurred from one collection to the next. ■ View collected information about Active Directory objects such as Users, Groups, Contacts, Computers, Printers, Shares, and Organizational Units. ■ Review Active Directory site lists, including Site Links, Site Link Bridges, Subnets, Intersite Transports, Servers, Connections and Licensing.

Select:	If you want to:
	<ul style="list-style-type: none"> ■ View Active Directory Group Policy Container Settings. ■ View information about Active Directory Domains, DCs, and Trusts. ■ Track and display access control entries and security descriptor data on all collected objects. ■ View Active Directory Schema information.
Reports	<ul style="list-style-type: none"> ■ Run "out-of-the-box" reports against your collected data. ■ Write your own SQL and SSRS reports using VCM's report wizard.
Patching(**)	<ul style="list-style-type: none"> ■ Review a list of Microsoft bulletins available to VCM. ■ Create, run, or import VCM Patching templates to show which machines require the patches described in each bulletin. ■ Select machines to license, set options for assessment and deployment, or monitor VCM Patching jobs. ■ Deploy patches.
Administration***	<ul style="list-style-type: none"> ■ Manage basic configuration options for VCM. ■ Establish filters to limit the data you collect from machines in your enterprise. ■ Manage your VCM licenses. ■ Organize and manage your enterprise using VCM. ■ Manage VCM Logins and Roles. ■ View the status of jobs that are currently running, scheduled to run, or completed. ■ Configure VCM to notify you of certain conditions in your enterprise.

* Available only when VCM for Active Directory (AD) is licensed. This slider is viewable based on your role.

** Available only when VCM Patching is licensed. This slider is viewable based on your role.

*** Visible only to users with Administrative rights to VCM as part of their VCM role.

Where to Go Next

You are now ready to proceed to [Getting Started with VCM](#) to start using VCM and all of its components and tools.

After you have completed the steps in [Getting Started with VCM](#), you must proceed to the next applicable chapter that is relevant to the components you have licensed in your installation. VMware has intentionally ordered the instructions in the remainder of this guide such that they build upon one another as you proceed through this guide; therefore, it is imperative that you proceed in order.

You can skip any chapters that do not pertain to your installation as you proceed through this guide in order.

NOTE If you choose to license another VCM component at a later date, you will be able to go back and configure it at that time.

Getting Started with VCM

Before you can begin using VCM to manage the machines in your enterprise, you must complete the following steps:

1. [Discover, License, and Install Windows Machines.](#)
2. [Discover, License, and Install UNIX/Linux Machines.](#)
3. [Discover, License, and Install Mac OS X Machines.](#)
4. [Discover, License, and Collect Oracle Data from UNIX Machines.](#)
5. [Customize VCM for your Environment.](#)
6. [Set up and use VCM auditing.](#)

Discover, License, and Install Windows Machines

The following steps must be performed before collecting data from Windows machines:

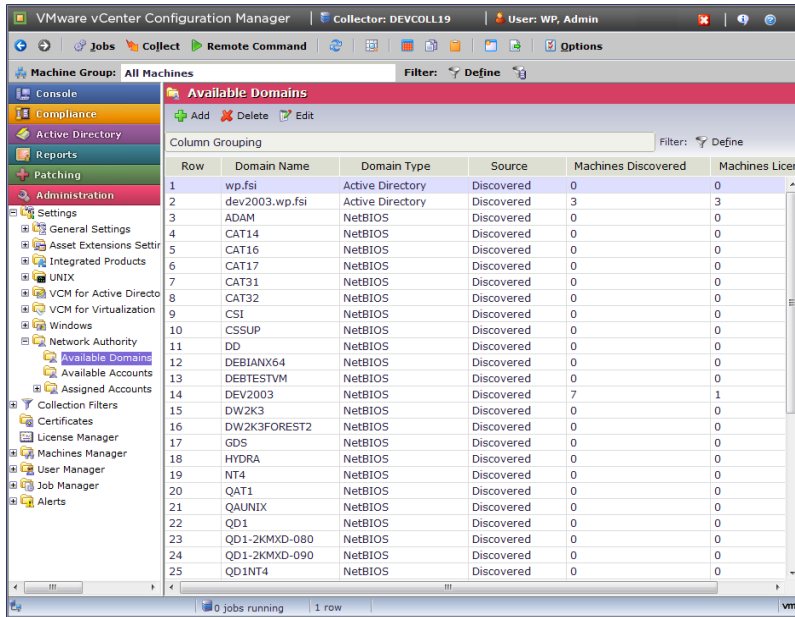
1. Verifying Available Domains
2. Checking the Network Authority
3. Assigning Network Authority Accounts
4. Discovering Windows machines.
5. Licensing Windows machines.
6. Installing the VCM Agent on your Windows machines.
7. Performing an initial Windows collection.
8. Exploring the Windows collection results.

These steps are explained in the following subsections.

Verifying Available Domains

The VCM Collector must gain access to each domain in order to interact with all enterprise Windows machines. During installation, VCM discovered all of the domains that the Network Authority Account you provided had access to.

To view a list of these discovered domains in VCM, navigate to **Administration > Settings > Network Authority > Available Domains**. VCM displays the available domains in the data grid.



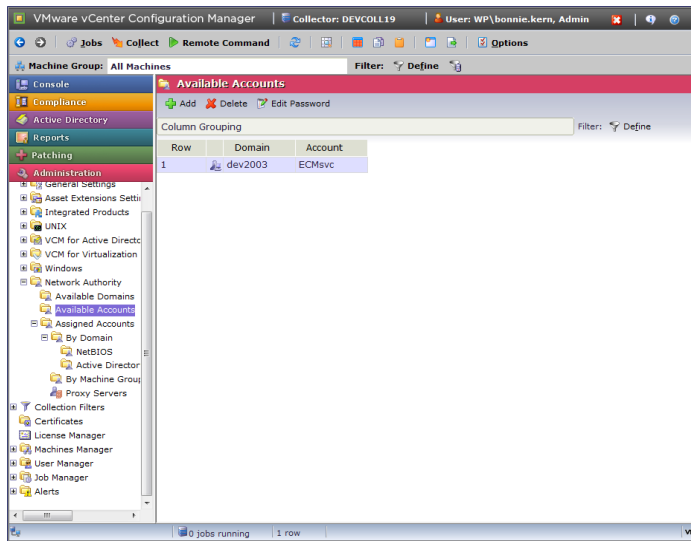
If the Windows machines that you want to manage belongs to a domain that is not shown in this list, then you must add that domain manually. Click **Add**, then follow the steps in the Add Domain wizard to manually add that domain. Once the domain is shown in the Available Domains list, you will be able to manage Windows machines in that domain.

Checking the Network Authority

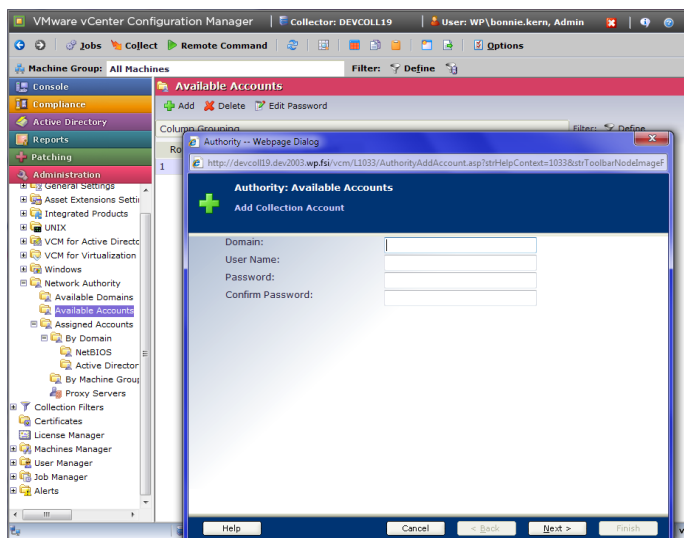
Your VCM Collector has to gain access to each domain to interact with the Windows machines in your enterprise. An account having Domain Administrator rights must be created for each domain that has Windows machines you want to manage. An initial account (your default Network Authority Account) was specified through VCM Installation Manager during installation; you may need to create others. Once an account has been created, it must be assigned to domains or machine groups (see [Assign Network Authority Accounts](#)).

The following procedure enables you to check for available accounts and add new ones if necessary.

1. Click **Administration > Settings > Network Authority > Available Accounts**.



2. If you need to add a new account, click **Add** and follow the prompts.



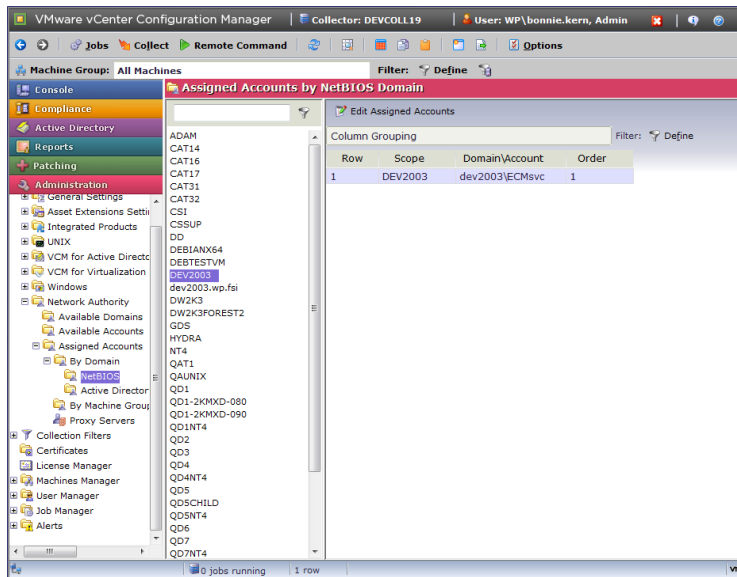
NOTE Repeat the Network Authority Available Accounts wizard, creating a specific account for each domain that has machines that you intend to manage through VCM.

Assigning Network Authority Accounts

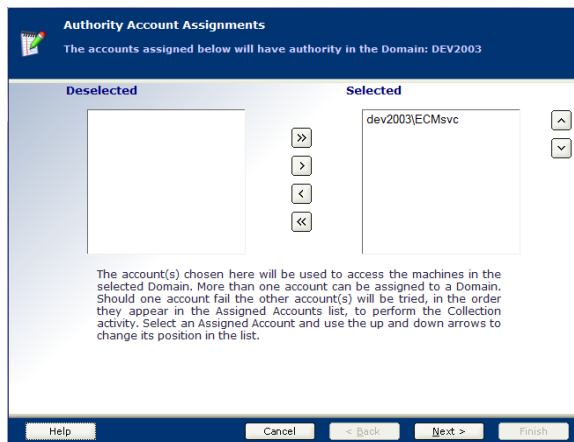
VCM offers considerable flexibility in assigning Network Authority Accounts to domains and machine groups. You can assign one account to all domains and machine groups, or assign a different account to each. You can even assign multiple accounts to each domain and machine group.

The following procedure illustrates how to assign Network Authority to accounts by NetBIOS domain. However, you can also assign Network Authority by Active Directory Domain, or even by Machine Group (**Administration > Settings > Network Authority > Assigned Accounts > By Machine Group**). For more information on these options, see the online Help.

1. Click **Administration > Settings > Network Authority > Assigned Accounts > By Domain** and then select **NetBIOS**.
2. Select a listed domain.



3. Click **Edit Assigned Accounts** and follow the prompts.



Discovering Windows Machines

The discovery process identifies which machines can be accessed on your network. VCM uses one or more Discovery Rules to discover the machines that are present on your network and available to VCM. The Discovery Rules can be very general to discover many machines, or very precise to discover a particular subset of your machines.

Your initial discovery can take anywhere from one afternoon to a couple of days, depending on the size of your network. You may not have a 100% success rate with the first discovery process you run because some machines may not be available during that time (for example, laptops that are not currently on the network). It may, therefore, take a few days to coordinate and resolve scenarios in order for you to discover the machines in your enterprise.

NOTE It is not necessary to complete the discovery of every machine in your enterprise before you proceed with licensing machines. If you choose to move forward and license a subset of your machines, be sure to review these chapters when you discover additional machines at a later time.

All discovered Windows machines will be placed in the **Administration > Machines Manager > Available Windows Machines** list, and all discovered UNIX/Linux machines will be placed in the **Administration > Machines Manager > Available UNIX Machines** list.

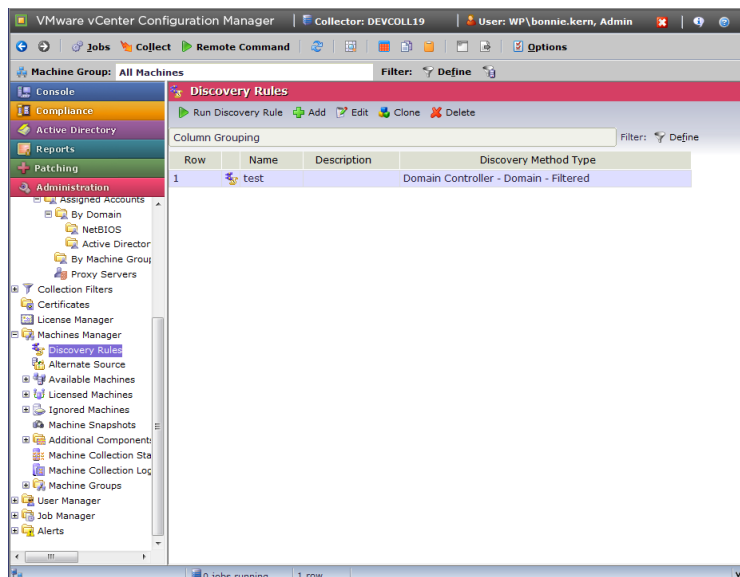
NOTE A Discovered Machines Import Tool (DMIT) is available from VMware Customer Support to assist you with the following process. This tool imports machines discovered by the Network Mapper (Nmap) into the configuration database. To use the tool, contact VMware Customer Support; otherwise, use the following process.

After the initial discovery, VMware recommends that you generally perform a discovery about once each week to keep the list of available machines current. You can schedule these future discoveries during your organization's off-hours, if you prefer.

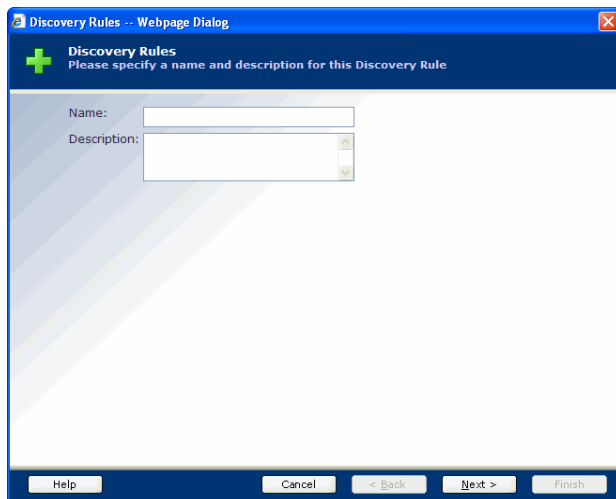
NOTE To schedule a VCM job for discovery, go to **Administration > Job Manager > Scheduled** and follow the Wizard. Refer to the online Help for more information.

Use the following procedure to discover machines.

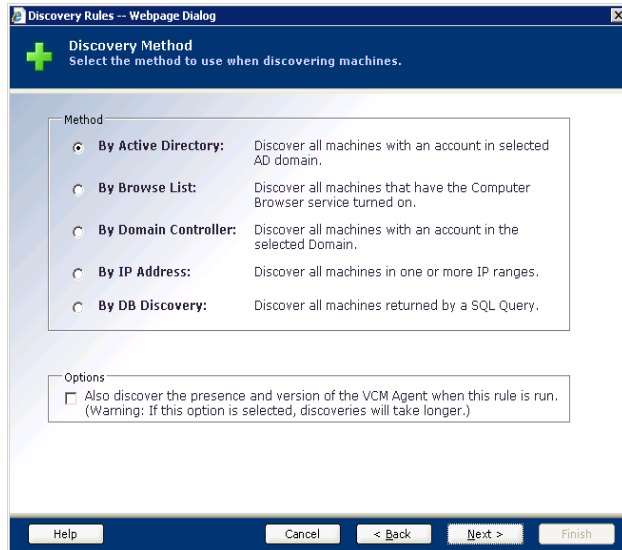
1. Click **Administration > Machines Manager > Discovery Rules**.



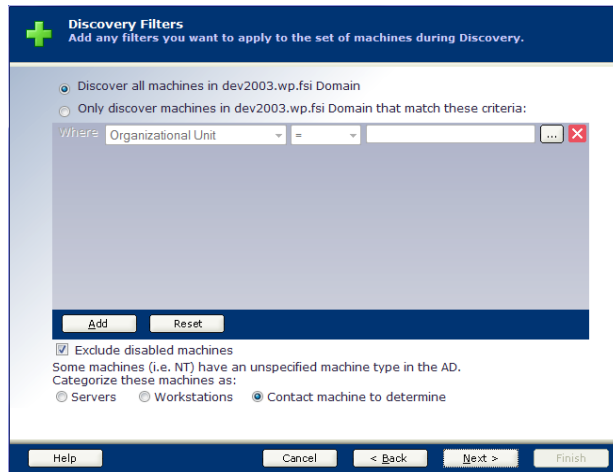
2. Click **Add** to create a Discovery Rule. The Discovery Rules wizard appears.



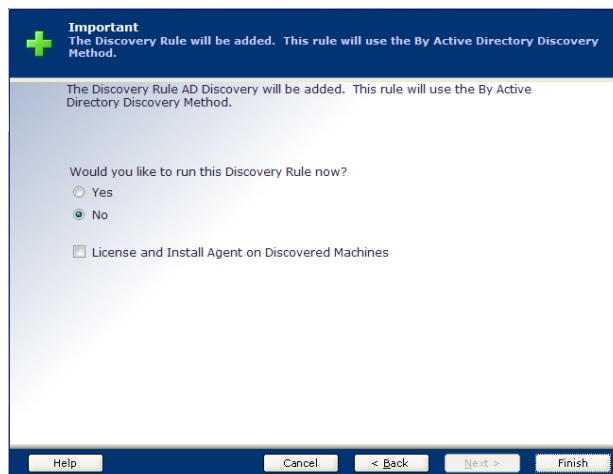
3. Type a **Name** and **Description** for this new Discovery Rule, then click **Next**. The **Discovery Method** page appears.



4. If you have Active Directory in your environment, VMware recommends a discovery that is targeted for Active Directory. Select **By Active Directory**.
5. For an initial discovery, do not select **Also discover the presence and version of the VCM Agent when this rule is run**. Because the VCM Agent is not present on the machines yet, you cannot discover the Agent version.
6. Click **Next**. If you used By Active Directory, the **AD Domain** page appears.
7. Specify the **AD Domain**, accept the defaults, and then click **Next**. The **Discovery Filters** page appears.



8. Create the filter. For more specific filtering of machines for discovery and other advanced features, refer to the online Help. Click Next. The **Important** page appears.



9. Select **Yes** so that you can run the Discovery Rule immediately. Because you are discovering machines for the first time, you want to run the discovery now. Leave **License and Install Agent on Discovered Machines** unselected. If the box is checked, VCM will proceed with licensing and installing the Agent on each machine discovered, potentially exceeding your license count. For future scheduled discoveries, VMware suggests checking the box, but not for your initial discovery.
10. Click the **Jobs** button at the top of the Portal to verify that your discovery job has completed before proceeding to the next step. The Jobs Running window appears, listing your job name and summary information. If the job has completed, it will not appear here.

NOTE You can also verify jobs for the past 24 hours if you think that you may have missed your running discovery job by going to **Administration > Job Manager > History > Other Jobs > Past 24 Hours**. Refer to the online Help for additional information regarding VCM Jobs.

Licensing Windows Machines

You are now ready to license the Windows machines you have discovered. In the following sections, you will license, install VCM Agents on, and collect data from your Windows machines. Later, we will guide you through these actions on your UNIX/Linux machines.

VCM requires that you specify the machines you want to manage. Remember, the number of licenses you have purchased may not match the number of machines that have been discovered and are visible in **Administration > Machines Manager > Available Machines > Available Windows Machines** or **Administration > Machines Manager > Available UNIX Machines**.

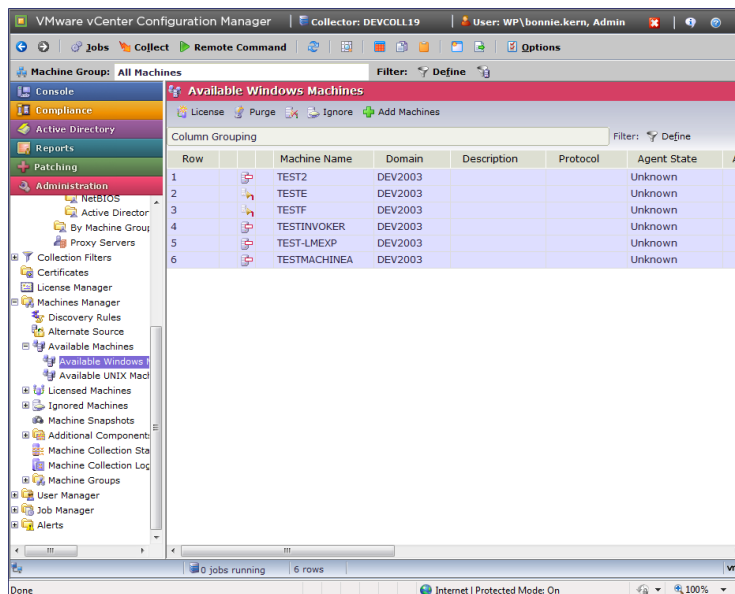
IMPORTANT If the machine type (that is, workstation or server) of a discovered Windows machine is indeterminate, then the machine cannot be licensed. The machine type is visible in the second column of the Available Machines Data Grid found at **Administration > Machines Manager > Available Machines > Available Windows Machines**. If you need assistance resolving the machine type for machines you plan to license, contact VMware Customer Support for guidance.

Use the following procedure to license your Windows machines.

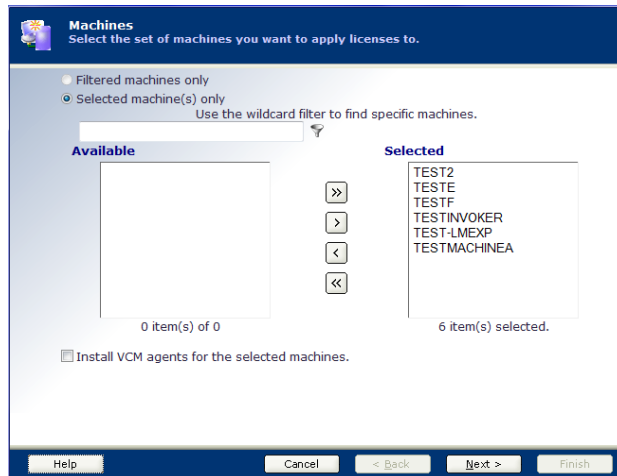
1. Select **Administration > Machines Manager > Available Machines > Available Windows Machines**.

NOTE Remember, discovered machines with an indeterminate **Machine Type** will not be licensed if they are included in your selection.

2. Select the machine(s) you want to license. To select multiple machines, use **Shift-click** or **Ctrl-click**.



3. Click **License**. The Available Machines License dialog box appears.



4. Leave the **Install VCM Agents for the selected machines** box unchecked during your first pass at licensing machines. Once you have more experience licensing machines and deploying the VCM Windows Agent, you may choose to check this box when licensing. The machines that you selected appear in the Selected area. Click **Next** to view your Product License Details. The licensed machine count has increased by the number of machines that you have selected to license.
5. Click **Next**. VCM confirms that the licenses you requested will be applied to the selected machine(s).
6. Click **Finish**.

Installing the VCM Windows Agent on your Windows Machines

Before you can collect data from a machine, the VCM Windows Agent must be installed on your licensed Windows machine. You can install the VCM Windows Agent through VCM or manually. Both methods are described here.

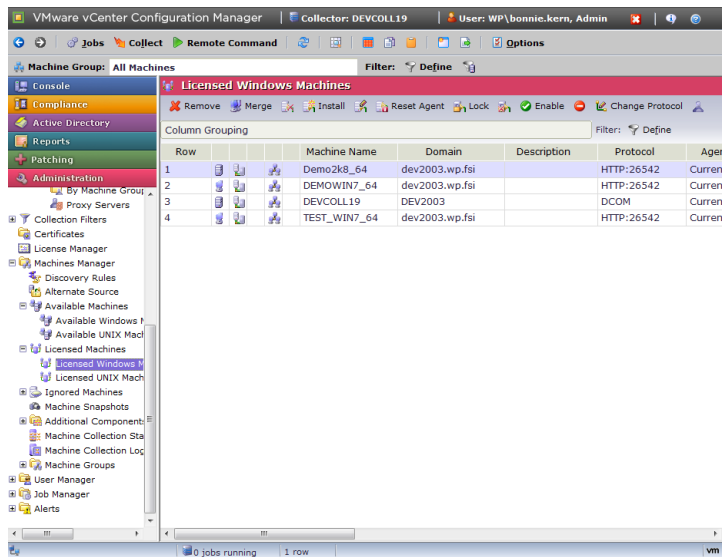
Machines that will be affected are those that are listed in the **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines** view.

The following procedure describes how to install the VCM Windows Agent on your licensed Windows machines.

NOTE If you are installing the Agent on Windows 7, 2008, 2008 R2, or Vista, you may need to disable the UAC during installation. See "[Disabling UAC for Agent Installation](#)" on page 81 for information.

Use the following steps to install the VCM Windows Agent on your licensed Windows machines.

1. Navigate to **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines**.
2. Select the Windows machine(s) on which you want to install the VCM Windows Agent. To select multiple machines, use **Shift-click** or **Ctrl-click**.



3. Click **Install** and follow the prompts.

NOTE To use advanced options such as HTTP communication for your agent, or to deploy the agent from an alternate source, refer to the online Help. To access the online Help at any time during the wizard, click the **Help** button in the lower left corner of the dialog box.

4. Verify that your agent installation job has completed. To check the status of an active job, click the **Jobs** button at the top of the Portal window to access the Jobs Summary.

NOTE You can also verify jobs for the past 24 hours if you think that you may have missed your running discovery job by going to **Administration > Job Manager > History > Other Jobs > Past 24 Hours**. Refer to the online Help for details regarding VCM Jobs.

Manually Installing the VCM Windows Agent

You can manually install the VCM Windows Agent using either the EXE (.exe, executable) file or the MSI (.msi, Microsoft Installer) file that is supplied with VCM. Choose your install method based on the following:

- EXE files detect an existing software version and provide the option to uninstall the existing version. EXE files can also be used for unattended silent installations.
- MSI files are database files executed by the Windows MSIEXEC.EXE executable, which reads data in the MSI file and executes the installation. MSI files can be used for unattended, silent installations. The MSI installer will also uninstall an existing agent (non-msi), but it does not ask. If you run it again, you have the option of removal only. If you upgrade an MSI-installed agent with the new MSI, the old agent is uninstalled.

The VCM Enterprise Certificate, which is selected during the initial installation of VCM, is installed in the certificate store on the Agent machine during the Agent installation process if HTTP is selected. The Collector root certificate (Enterprise Certificate) is used to authenticate requests from a collector (using the Collector Certificate and its established trust to the Enterprise Certificate) on the Agent machine before a collection/change request is processed.

Using the .exe

To manually install the VCM Windows base Agent (CMAgentInstall.exe) on a target machine using the .exe file, follow these steps.

1. On your Collector, navigate to the Agent files directory at:
C:\Program Files (x86)\VMware\VCM\AgentFiles
2. Locate the `CMAgentInstall.exe` file, and then install it from a network share or copy it to the target machine.
3. Navigate to the Collector data directory at `c:\Program Files (x86)\VMware\VCM\CollectorData`. Locate the Enterprise Certificate `.pem` file. This file must be accessible during the agent installation. The path used here is the default location. If your files are not in the default location, click **Administration > Settings > General Settings > Collector**. In the data grid, go to the **Root directory for all collector** files. The current path is displayed in the **Value** column.

NOTE If the Enterprise Certificate has been distributed by a mechanism outside of the scope of VCM, such as a corporate Public Key Infrastructure (PKI), you may not need to include the Enterprise Certificate file.

4. In Windows Explorer, double-click the `CMAgentInstall.exe`. You will be asked for the certificate path and port.

If you are performing a silent install, on the target machine run the `CMAgentInstall.exe` using the following parameters:

```
CMAgentInstall.exe /s INSTALLPATH=%Systemroot%\CMAgent PORTNUMBER=26542
CERTIFICATEFILE=<filename>
```

NOTE The `%Systemroot%` environment variable specifies the directory where Windows is installed (typically `\WINNT` or `\WINDOWS`).

Where:

- **CMAgentInstall.exe** is the executable used to install the Agent.
- **/s** indicates a silent install, which means that popups and menus do not appear. When running this command from the command line, VMware recommends using the `/s` option. When performing a silent install, if the VCM Windows Agent is found locked, the installation will fail. To unlock the Agent so that the installation will proceed, use the `-UNLOCK` option. When used, the Agent will remain unlocked when the installation completes. The syntax is:

```
CMAgentInstall.exe /s -UNLOCK INSTALLPATH=%Systemroot%\CMAgent
PORTNUMBER=26542 CERTIFICATEFILE=<filename>
```

NOTE To re-lock your machine, submit a lock request from the VCM Collector.

- **INSTALLPATH** is the location where the Agent will be installed.
- **PORTNUMBER** is specified for HTTP Agents. If the `PORT` parameter is not present, the protocol will be `DCOM`. In this case, the communication socket listener service will not be installed and the certificate is not required.
- **CERTIFICATEFILE** is the certificate that was generated or specified on the Collector during the Collector installation. The location of the certificate file will be in the path relative to where you installed the software on the Collector, and by default is `C:\Program Files (x86)\VMware\VCM\CollectorData\[certificate name].pem`. If you specify a `PORTNUMBER`, but do not want to use a certificate, you must use the parameter `CERTIFICATEFILE=SKIP` to allow an HTTP Agent without a valid `CERTIFICATEFILE` path.

NOTE For Vista, Windows7, and Windows 2008 only: If you set compatibility mode on any Agent executables to a prior version of Windows, the operating system may be reported incorrectly in VCM.

To Manually Uninstall the VCM Windows Agent

The VCM Windows Agent uninstall executable will be present only if the Agent was installed manually using CMAgentInstall.exe or CMAgentInstall.msi. To uninstall the VCM Windows Agent manually, execute the following command (this command assumes the default installation directory was selected):

```
%SystemRoot%\CMAgent\Uninstall\Packages\CMAgentInstall\UnCMAgentInstall.exe
```

Using the .msi

To manually install the VCM Windows base Agent (CMAgent[Version].msi) on a target machine using the .msi file, follow these steps:

1. On your Collector, navigate to the agent files directory. The location of the .msi will be in the path relative to where you installed the software on the Collector, and by default is
c:\Program Files (x86)\VMware\VCM\AgentFiles.
2. Locate the CMAgent[Version].msi file. This file must be accessible by the target machine.
3. Navigate to the Collector data directory at c:\Program Files (x86)\VMware\VCM\CollectorData. Locate the VCM Enterprise Certificate .pem file, and then copy this file to the target machine in a secure manner.

NOTE If your Collector is operating in a full Public Key Infrastructure (PKI), and the client can validate the Collector root certificate (Enterprise Certificate), the .pem file is not necessary.

4. On the target machine, double-click the .msi or run the .msi file using the command line syntax. Command line options and parameters are described below.

```
msiexec /Option <Required Parameter> [Optional Parameter]
```

For example:

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

When executing the Windows installer file with default options, any existing Window Agent is removed. The new VCM Windows Agent is then installed in the %SystemRoot%\CMAgent directory, and will use DCOM to communicate. The %SystemRoot% variable defaults to C:\WinNT or C:\Windows.

For HTTP installs, where PORTNUMBER is set, you must also specify an Enterprise Certificate. To do so, use this syntax: CERTIFICATEFILE="x:\[mypath]\[mycert].pem". If you specify PORTNUMBER, you must also provide CERTIFICATEFILE with either SKIP or the path to a certificate file.

Command line options, showing required and optional parameters, include the following. These options are all parameters to msiexec.

- **/qb** - Runs the command in a basic user interface, displaying the progress and error messages.
- **/qn** - Runs the command in quiet mode; no user interaction is required.
- **/i** - Specifies the command as an installation.
- **/x** - Specifies the command as an uninstall process.

- **PORTNUMBER:** Installs the Windows Agent on the port number specified, using HTTP instead of DCOM. For HTTP installs, where PORTNUMBER is set, you must also specify a certificate file using the syntax: CERTIFICATEFILE="x:\[mypath]\[mycert].pem". For example:
`msiexec.exe /qn /i "C:\temp\CMAgent[VersionNumber].msi" PORTNUMBER=2666
CERTIFICATEFILE="x:\mypath\mycert.pem"`
- **INSTALLDIR:** Changes the default root directory specification (%SystemRoot%\CMAgent). For example:
`msiexec.exe /qn /i "C:\temp\CMAgent[VersionNumber].msi" INSTALLDIR="C:\VCM"`
- **CERTIFICATEFILE:** Specifies the Enterprise Certificate. For example:
`CERTIFICATEFILE="x:\[mypath]\[mycert].pem" or CERTIFICATEFILE="SKIP"`

For more information about the command line options and descriptions, click **Start > Run > msiexec** or visit <http://www.microsoft.com>.

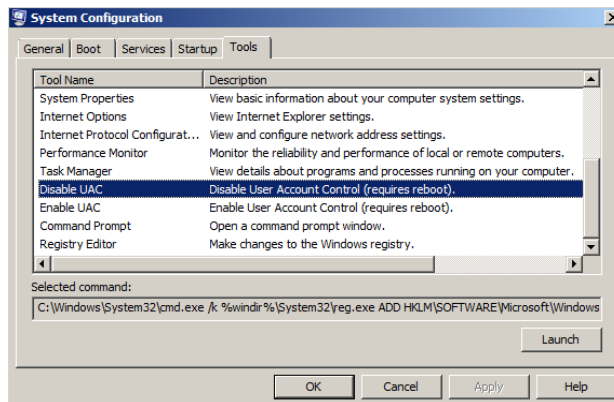
You must specify optional parameters using UPPERCASE letters, following the required "/i" parameter. Quotation marks are necessary only when a path includes spaces. For example, when one or more spaces exist in the source file location and the INSTALLDIR parameter. The optional parameters can be specified in any combination and order.

Disabling UAC for Agent Installation

The following steps are required only if you are installing the Agent on a Windows 2008 or Vista machine. When installing the Agent on Windows 2008 or Vista, you must disable the User Account Control (UAC), install the Agent, and then re-enable the UAC.

Disabling UAC on One Machine

1. On the target Windows 2008 machine, click **Start > Run**. The **Run** dialog box appears.
2. Type **msconfig** in the **Open** text box.
3. Click **OK**. The **System Configuration** dialog box appears. (This dialog box differs for Windows 2008 R2 machines.)



4. Click the **Tools** tab.
5. In the **Tool Name** list, select **Disable UAC**.
6. Click **Launch**. A **Command** window displays the running action. When the command is completed, close the window.
7. Close the **System Configuration** dialog box.

8. Restart the machine to apply the changes.
9. Install the Agent as specified in Licensing and Deploying the VCM Agent.
10. After installing the Agent on the target machine, re-enable UAC. To enable, perform the steps specified above. In Step 5, select **Enable UAC** in the **Tool Name** list.
11. Restart the machine to apply the changes.

Disabling UAC using Group Policy

Use the following procedure to disable the UAC on multiple machines. The instructions assume you have configured the Windows 2008 and Vista machines targeted for Agent install in a common Active Directory domain/OU.

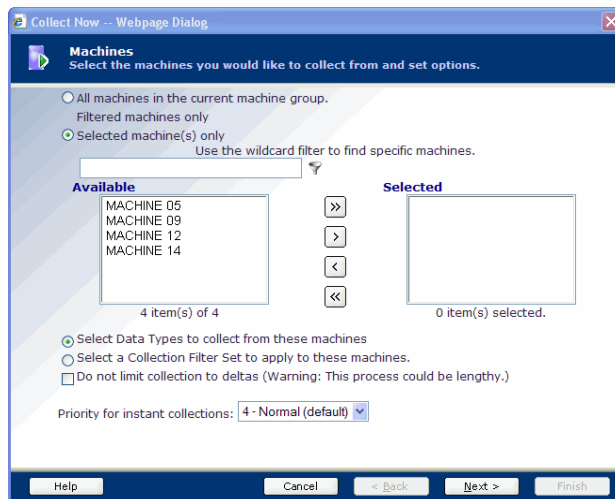
1. On a Domain Controller, click **Start > Run**. The **Run** dialog box appears.
2. Type **mmc** in the **Open** text box.
3. Click **OK**. The **Console** window appears.
4. Select **Console Root**, and then click **File > Add/Remove Snap-in**. The **Add or Remove Snap-ins** dialog box appears.
5. In the **Available snap-ins** list, double-click **Group Policy Management Editor**. The **Select Group Policy Object** dialog box appears.
6. Click **Browse**. The **Browse for a Group Policy Object** dialog box appears.
7. On the **Domains/OUs** tab, select the domain/OU to which the target machines belong, and then click **OK**.
8. On the **Select Group Policy Object** dialog box, click **Finish**.
9. On the **Add or Remove Snap-Ins** dialog box, click **OK**.
10. The domain/OU policy is added to the Console Root in the left pane.
11. Expand the added domain/OU and browse to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**.
12. In the right pane, locate the **User Access Control** policies. On each of the policies specified below, right-click and select **Properties**. Configure as follows:
 - **User Account Control: Behavior of the elevation prompt for administration in Admin Approval Mode:** Elevate without prompting.
 - **User Account Control: Detect application installations and prompt for elevation:** Disabled
 - **User Account Control: Run all administrators in Admin Approval Mode:** Disabled
13. Restart the machine to apply the changes.
14. Install the Agent as specified in the previous section, "Licensing and Deploying the VCM Agent".
15. After installing the Agent on the target machines, re-enable UAC. To enable, perform the steps specified above. In Step 5, change the policies to Enabled.
16. Restart the machine to apply the changes.

Performing an Initial Collection

You are now ready to collect data. VMware recommends using the default filter set, which collects a general view of the licensed Windows machines in your enterprise configuration, until you are ready to build specific filters and target your collections. The first time you use the default filter set for a collection, the VCM Agent will return all of the data (as specified by the filters in the default filter set) to be stored in the VCM database. Subsequent collections using the default filter set will return only a delta collection (meaning the differences between the data found on the target machine and what is already stored in the VCM database), unless you specify within the Collect Wizard to return the full collection. The delta collection feature makes subsequent collections run faster and more efficiently than the initial collection with that particular filter set.

IMPORTANT You can run Compliance Templates and perform reporting on data that has been collected and stored in VCM. Therefore, it is necessary to perform collections on a regular basis. This ensures that the data you are reporting on is current. When performing a full collection on your entire enterprise, you may want to run VCM overnight because the collection could potentially affect the performance of your machines. Once the initial collection completes, any future delta collections should be unnoticed by users. Be sure to perform collections on a routine basis to ensure accurate reporting.

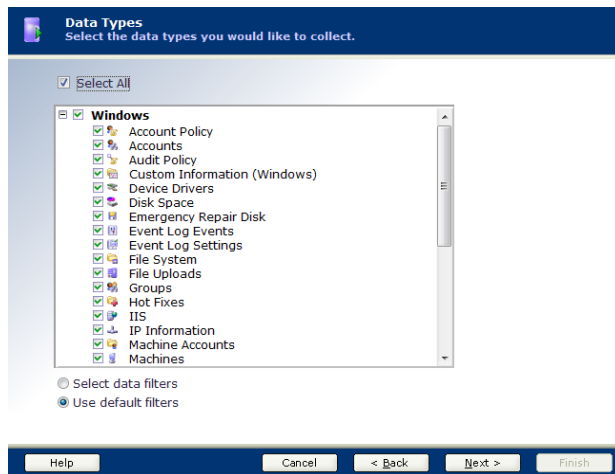
1. Click **Collect**, located on the main Portal toolbar. The **Collection Type** page of the wizard appears.
2. Select **Machine Data**, and then click **OK**. The **Machines** page appears.



3. Select the machine(s) from which you want to collect data. To select multiple machines, use Shift-click or Ctrl-click. Use the double arrow to move all visible machines to the selection window, 500 at a time. Leave the default options selected, then click **Next**.

IMPORTANT To collect from machines running Windows XP SP2 or Vista using DCOM, you must either enable ICMP pings in the firewall settings, or disable ICMP pings in the Portal. Refer to the online Help for more information.

4. The Data Types dialog box appears. Check the **Select All** checkbox, then confirm that the **Use default filters** option button is also selected. Click **Next**.



5. For initial collections, there should be no conflicts with previously scheduled or running jobs containing the same data types. Click **Finish**.
6. Verify that your collection job has completed before proceeding to the next step. To do so, click the **Jobs** button at the top of the Portal window to access the **Jobs Summary**.

NOTE You can also verify jobs for the past 24 hours if you think that you may have missed your collection job by going to **Administration > Job Manager > History > Instant Collections > Past 24 Hours**. Refer to the online Help for additional detail regarding Jobs.

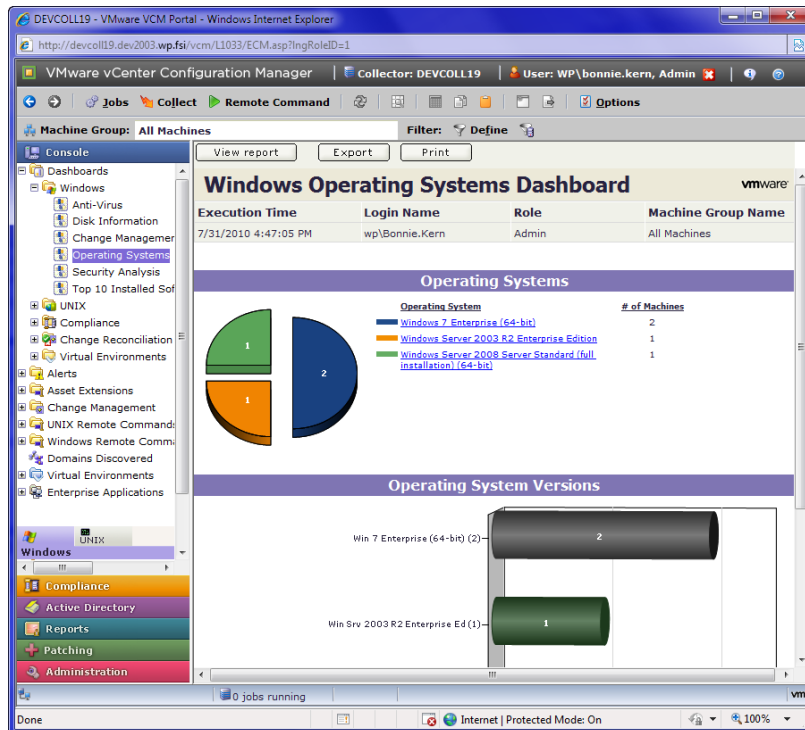
TIP Collecting certain Windows data types the first time results in a secondary SID lookup (looks up user accounts associated with a user ID) query back to the machine from which the data type was collected. To speed up initial collections that require a SID lookup, first collect the Accounts and the Groups data types from the Primary Domain Controller (PDC) of each domain. The PDCs have the necessary account information, and doing so automatically resolves the SIDs. The data types that cause the automatic additional query are:

- User Rights
 - Registry Key Permissions
 - Directory Permissions
 - Share Permissions
 - Disk Quota
 - Event Log
 - Services
 - Processes
-

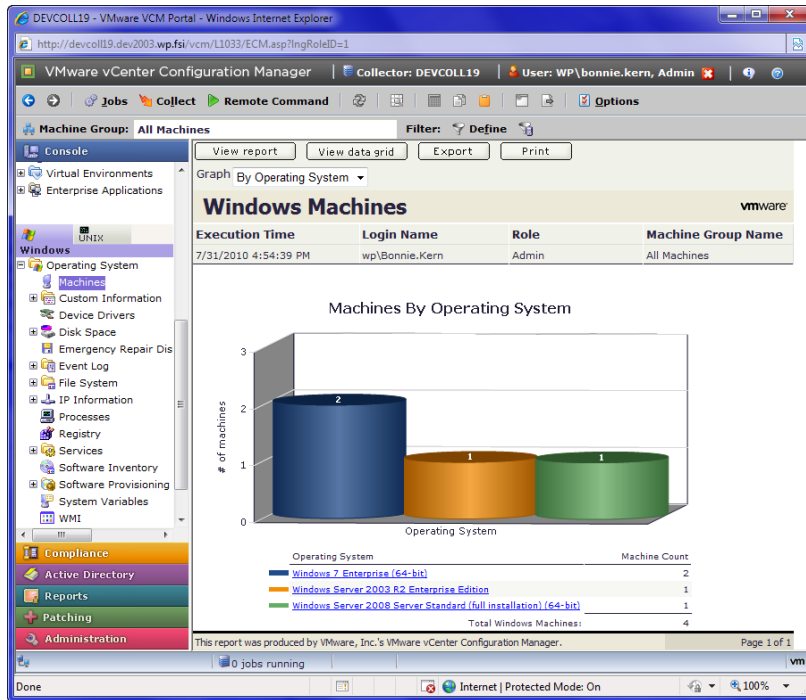
Exploring Windows Collection Results

Now that you have performed an initial Windows collection, you can explore that data in the VCM Portal. VCM presents summary information in graphical SSRS charts, for machines in the active machine group, which you can view, export, or print. The individual VCM Dashboards visible in the VCM Portal will vary, based upon which VCM components you have licensed. Each VCM Dashboard is run only when the node is selected against the current data available in the CMDB for machines in the active machine group. Therefore, Dashboard data is only current as of the time when it was collected. In addition, it may take time for the data to display based upon the volume or complexity of the data requested.

1. Begin by looking at the Windows Operating Systems Dashboard under **Console > Dashboards > Windows > Operating Systems**.



2. Note that several other Windows Dashboards are also available. Take time to familiarize yourself with the remainder of the Windows Dashboards. Windows Collection Results are also available to you in a more "raw" format by data class. This level of "reporting" is more relevant for day-to-day operations, troubleshooting, and analysis, and can be viewed in a Summary report or data grid format.
3. Now take a look at your Windows Operating System Information by clicking the **Windows** tab in the Console. Then, click **Operating System > Machines**.



4. When you select the node, you will see a Summary Report as displayed above of the data class that you selected. Click **View Data Grid** to go directly to the data grid, or click an area of the Summary Report to filter the data before the data grid is displayed.

The screenshot displays the VMware vCenter Configuration Manager interface with the 'Machines' data grid selected. The grid has the following data:

Row	Machine Name	Domain Name
1	Demo2k8_64	dev2003.wp.fsi
2	DEMOWIN7_64	dev2003.wp.fsi
3	DEVCOLL19	DEV2003
4	TEST_WIN7_64	dev2003.wp.fsi

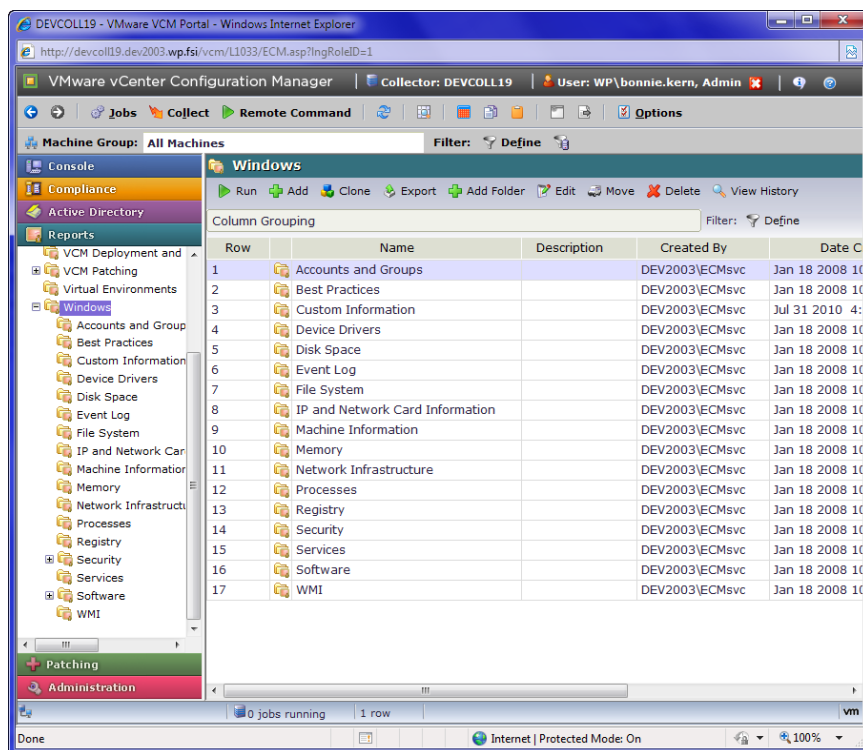
The interface also shows a 'Filter: Define' button and a 'Column Grouping' section. The status bar at the bottom indicates '1 row' and '0 jobs running'.

TIP The default view is the Summary Report; however, at any time you may switch the default view to go directly to the data grid by using the 'Enable/Disable Summary' feature on the data grid view. See About Data Grids in the online Help for more information on how to filter and sort your data and get full use of the data grid.

Several other categories (called "data classes") of information regarding your Windows Collection are available under the Windows tab, which is located in the Console. This is where the remainder of your collected Windows data is visible through the Portal.

An alternative way to view your collected Windows data is by running Reports or creating your own custom reports using the reporting wizard. To begin exploring VCM's Reporting functionality, go to the **Reports** slider, then click **Machine Group Reports > Windows**.

Like Dashboards, Reports are run against the current data available in the CMDB for machines in the active machine group, and therefore are only as current as the last collection. In addition, the report may require significant time to generate based upon the volume or complexity of the data requested. Refer to the online Help for more information on how to schedule and disseminate reports.



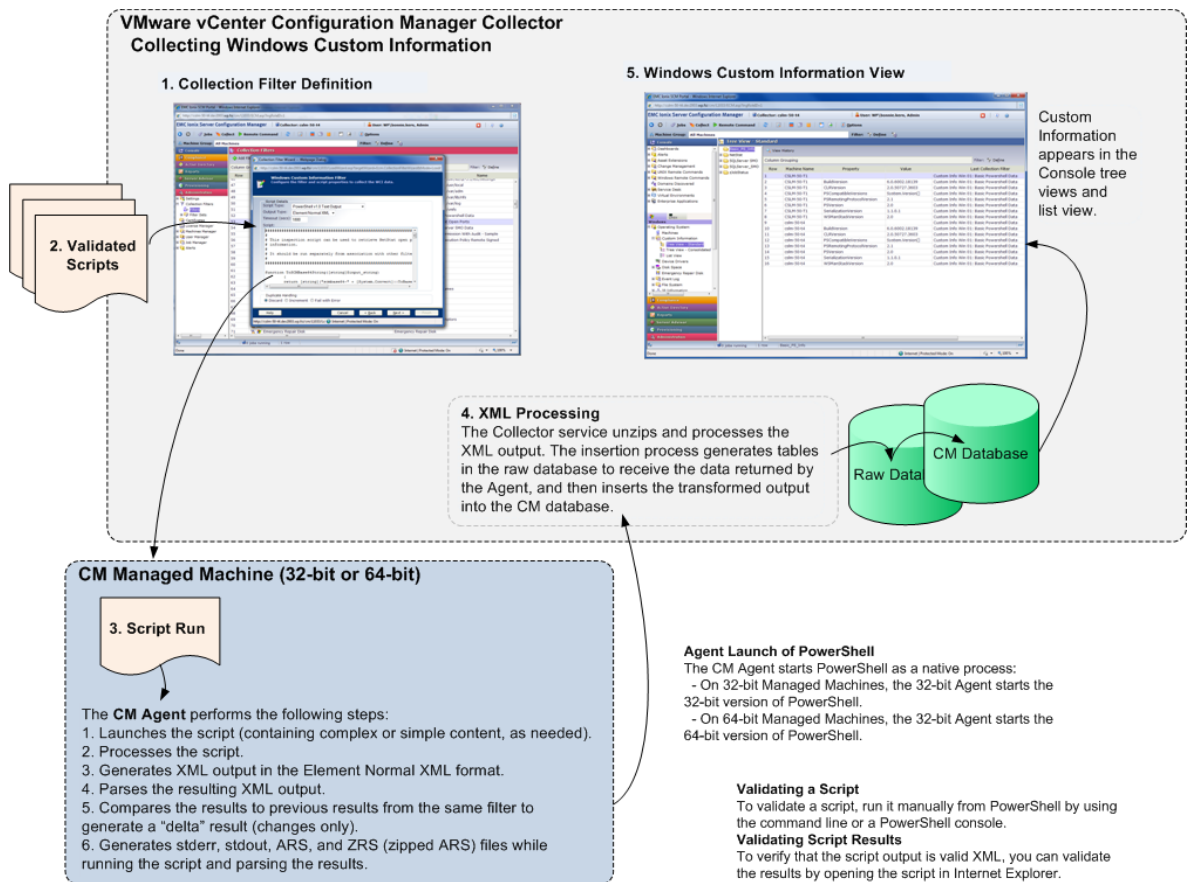
5. You may now begin to check Compliance for your collected data. To run a Compliance check, click the **Compliance** slider, then follow the steps as described in the online Help to create rule groups, rules, filters, and templates.

Getting Started Collecting Windows Custom Information

As a System Administrator, you can extend the data that VCM can collect by using a script, which will allow you to view, report on, alert on, detect change on, and run compliance against data not currently exposed by VCM. This extension allows you to view, report on, alert on, detect change on, and run compliance against custom data not currently exposed by VCM.

You can use the Windows Custom Information data type to perform user-defined, script-based collections from VCM-managed machines. To collect the custom data, you build a collection filter, which includes a script and other parameters relating to the execution of the script and the handling of its results. When this filter is used in a collection, the VCM agent will call a script engine to run the script, and will then parse the results so they can be returned to the VCM database and displayed in the VCM console. As of this release, VCM supports PowerShell scripting and XML output.

During the collection process, the VCM Agent launches PowerShell to execute the script, which in turn generates an XML result file. The Agent then parses the XML result into a format that can be checked for changes (deltas), and then those changes are returned to the Collector.



Prerequisites

Before collecting Windows Custom Information (WCI), you must ensure the following prerequisites are met.

- You must obtain or write a PowerShell script that will return data in a VCM-compatible element-normal XML format.
- The VCM agent (for VCM 5.3 or later) must be installed on each VCM-managed machine used to collect the Windows custom information. Older agents must first be upgraded.
- PowerShell must be installed on each VCM-managed machine. PowerShell is installed by default on Windows 2008 R2 and Windows 7 machines. For Windows XP, 2003, 2003 R2, 2008, and Vista machines, PowerShell must be installed separately. You cannot install PowerShell on Windows 2000 or NT4 machines. In cases where PowerShell is not installed on the target VCM-managed machine, the WCI collection will return a "Not Executed" success status. See [Job Status Reporting for WCI](#).
- Windows Custom Information supports PowerShell version 2.0, and should work with later versions of PowerShell as well.
- After installing PowerShell on a VCM-managed machine, you must reboot the machine to ensure that collections will work properly.
- If the VCM Collector will be used as a client for WCI collections, ensure that PowerShell is installed on the Collector machine.
- VCM ships with default Administration settings for Agent Thread (default is set to below normal thread priority) and Agent Data Retention (default is 15-day change log). However, you can change these settings if you desire.
- Before file-based PowerShell scripts can be executed by the WCI collection filter on the VCM Collector and/or the VCM-managed machine, you change the execution policy on the VCM-managed machines. The PowerShell execution policy on the VCM machine must be set to **Remote Signed**, **All Signed**, or **Unrestricted**. If the policy is set to **All Signed**, the scripts must be signed, and the appropriate certificates distributed before collections can be run.

Procedure

To collect and view Windows Custom Information from VCM-managed machines, follow these steps.

1. Obtain PowerShell script(s) from VMware Professional Services or another source (or you can write your own). For more information about scripts, see [Getting Started with PowerShell Scripts](#).
2. Select **Administration > Collection Filters > Filters**.
3. Click **Add Filter** to add a collection filter. The **Collection Filter Wizard** appears.
4. Enter a name for the filter, and then click **Next**. The Data Type page appears.
5. Select **Windows**, and then the **Custom Information (Win)** data type. Click **Next**. The **Windows Custom Information Filter** page appears.
6. Select your **Script Type**, which defaults to **PowerShell v1.0 Text Output**.
7. Select the **Output Type** of **Element Normal XML**.
8. Specify the **Timeout** in seconds. This setting specifies how long the Agent will allow a PowerShell script to run before attempting to end the process. The purpose of this setting is to prevent blocked or excessively long-running scripts from blocking other Agent requests.
9. In the **Script** area, paste the content of your user-defined PowerShell script, which contains statements specific to the data type you will be collecting. Depending on your script, parameters to be configured may exist near the top of the script.
10. VCM handles violations of any duplicate path attributes in the PowerShell scripts through the Duplicate Handling settings. In the **Duplicate Handling** area, select one of the following: **Discard**, **Increment**, or **Fail with Error**.

11. Click **Next** and then **Finish**.
12. Run a collection using your new collection filter.
13. Ensure the job completes.
14. View data in the Custom Information nodes (**Console > Windows > Operating System > Custom Information**).

When the Windows Custom Information data is available in the VCM database, you can generate reports and enforce compliance.

Change Detection in Windows Custom Information Data

Deltas in WCI are maintained on a per-filter basis at the client side, which means that if multiple filters return data under the same top-level element name (such as NetStat), each filter will have its own change detection.

In the following example, using multiple filters that collect the same open ports data and return it under the NetStat top-level element name, if a client machine has just started listening on port 80, each filter will report this new data as a newly created value the first time the filter “sees” this data. The best practice is to avoid this type of overlap of filters.

For example, two copies of the **File Permission With Audit** filter could be created in order to collect file permissions data from different parts of the file system, but they should not overlap. Having one filter get data from C:\ and another filter get data from C:\Windows would be a good practice. However, having one filter get data from C:\Windows with audit information and another filter get data from C:\Windows without audit information would not be a good practice because both filters would generate “new file” and “deleted file” events each time a new file was added or removed.

- For an element such as NetStat, only one filter should be used.
- For an element such as NTFS file system (`NTFSDirectory`), multiple filters would likely be used. For example, one filter would be used to obtain the details under C:\, and another filter would be used for C:\Windows\System. Both would merge under the `NTFSDirectory` top-level element, but there should be no overlap; instead they would each collect separate parts of the file structure to avoid “extra” change reporting.

Purge for Windows Custom Information

As with other data types, purge for WCI will purge all data for a machine. This means that if a single WCI filter is collected with the “Do not limit to delta” option selected, all WCI data for that machine will be purged from the client’s master file and from the VCM database, and it will be replaced with the resulting data from the single filter.

Job Status Reporting for WCI

Job status reporting for WCI is provided on a per script/filter level, and includes detailed reporting about exit codes and process standard error output. As each script/filter is executed, VCM captures detailed results information during the execution of the WCI collection filter scripts.

You can view the detailed information in the VCM user interface in the **Administration > Job Manager > History** node by selecting the executed job and then selecting **View Details** in the Job History Machine Detail pane of a collection job that includes WCI data.

The Job History Machine Detail view displays a single row for each WCI filter included in the collection job. These rows provide information about the execution of the WCI scripts and the parsing of the script results. In cases where the script cannot be executed because prerequisite components are not installed or available (such as PowerShell is not installed), the status for a row will be “Not Executed.” This status does not result in a failure for the inspection because PowerShell (or other script engines) are optional components and may not even be installable on all VCM-supported OS versions.

If a WCI collection job encounters errors on a machine, detailed information about the failure will be reported. The failure could occur during the launch of PowerShell, during script execution, or during the interpretation of the script results. For example, an error could occur in the PowerShell launch process if PowerShell is not installed on the VCM-managed machine. However, since PowerShell is an optional component, such a failure does not roll up as an error to the job level, although the job details will show Not Executed to show such skipped steps. On the other hand, if a PowerShell script generates errors due to syntactical or typographical defects in the script itself, these errors will roll up to a “completed with errors...” status at the collection job level.

Running Reports

Several reports are included for reporting on Windows Custom Information, including:

- **Netstat Open Ports:** Reports port and protocol information from the `netstat -A` command.
- **SQL SMO Database:** Reports database details collected.
- **SQL SMO Instance:** Reports basic information about SQL Server instances collected.

These reports are in **Reports > Machine Group Reports > Windows > Custom Information**.

Getting Started with PowerShell Scripts

The Windows Custom Information data type (WCI) uses extensions to the VCM Windows agent to allow the agent to invoke scripts that are passed down as part of a collection filter’s parameters, and then parse the results. As a result, these extensions are very flexible in that they use filter parameters to detail the command line to invoke the scripting engine, and a COM class name to specify the parser the Agent will need in order to parse the script output. This allows the eventual extension of the system to support multiple different scripting engines/languages and multiple options for output format.

For this version of WCI, the base requirement supports PowerShell for the scripting engine and a specific XML format, named Element Normal XML, as the output.

This topic describes:

- [Executing PowerShell Scripts](#)
- [Developing Custom Collection Scripts](#)
- [Example of Developing a Custom PowerShell Script for Use with the WCI Data Type](#)
- [Troubleshooting Custom PowerShell Filter Scripts](#)

Executing PowerShell Scripts

PowerShell contains built-in policies, which limit its use as an attack vector. The primary policy is for script execution. By default the script execution policy is set to Restricted, which means that PowerShell can only be used interactively or for executing commands directly from the command line. The additional policy settings are as follows:

- **AllSigned:** Any PowerShell script (.ps1 is the typical extension) must be signed by a verifiable certificate (from the SPC certificate store)
- **RemoteSigned:** Any PowerShell script that is downloaded from the Internet (by a supporting browser such as Internet Explorer) must be signed. Script files that are created locally, or scripts that are downloaded by a means that does not support flagging of the file source, do not need to be signed.
- **Unrestricted:** All PowerShell script files will be executed regardless of whether they are signed.

In addition, PowerShell 2.0 adds the capability to set different script signing policies at the machine, user, and process (single execution of powershell.exe) scopes.

WCI uses Script Type information in the collection filter definition to indicate how PowerShell should be executed and how the script should be passed to it. The primary ways a WCI script may be passed to PowerShell is either in-line or through a script file

- **In-line:** Requires a collection script that can be represented as a single line of PowerShell code. In-line scripts can be run regardless of the execution policy; because an in-line script is run on the PowerShell command line rather than from a file, the execution policy does not apply. The default WCI filter uses an in-line script to collect basic information about the PowerShell version, .NET version, and execution policy settings of a system.
- **Script file:** Requires that the execution policy be set to Remote Signed at the most restrictive, since the script is being run from a file locally on the client system. Because of its additional ability to have execution policy set at the process level, PowerShell 2.0 is the base requirement for WCI in VCM. The default script type command line used for script based filters in WCI includes options to set the process-level execution policy to Remote Signed. This allows WCI to execute collection scripts against systems whose machine and user level signing policies may be anything, without having to change the setting. Out-of-the-box VCM WCI non-in-line collection filters will fail if executed against PowerShell 1.0 client systems.

VMware recommends that you upgrade from PowerShell 1.0 to PowerShell 2.0, which introduced a number of useful functions. PowerShell 2.0 is also supported on all platforms that support PowerShell 1.0.

It is possible to execute WCI PowerShell collection scripts against PowerShell 1.0 systems as well, although it has not been tested, and is not officially supported. In-line WCI filters that do not employ PowerShell 2.0 commands should work directly. For script file based filters to work, you must create them with the PowerShell v1.0 Text Output script type, and the system must already have its execution policy set to Remote Signed, at the most restrictive, with un-signed scripts, or to All Signed with signed scripts (see below). This setting can be accomplished by the Group Policy Object (GPO), through the use of a VCM Remote Command, or by using a registry change action or enforceable compliance to set the policy directly. For example:

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

For additional information about Windows PowerShell and signing scripts, see:

- **Scripting with Windows PowerShell:** <http://technet.microsoft.com/en-us/scriptcenter/dd742419.aspx>
- **Windows PowerShell Owner's Manual:** <http://technet.microsoft.com/en-us/library/ee176949.aspx>
- **Signing Windows PowerShell Scripts:** <http://technet.microsoft.com/en-us/magazine/2008.04.powershell.aspx>
- **Execution Policies:** <http://technet.microsoft.com/en-us/library/dd347641.aspx>
- **Registry value that controls execution policy:** [http://msdn.microsoft.com/en-us/library/bb648598\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb648598(VS.85).aspx)

Developing Custom Collection Scripts

Development of custom collection scripts requires planning the data structure. WCI internally stores data hierarchically, as displayed in the Tree View - Standard node. The collection script is required to provide all of the structure that can be seen in any branch under this node.

The root element in the XML result data set will become a top level (root) element in the WCI data type node. Child elements will appear in the same locations in the VCM user interface as the locations they populate in the XML document that is returned by the script.

When developing custom collection scripts, follow these guidelines:

- XML element names must be unique at their level (for example, two "Child1" nodes can exist, as long as they are not siblings).
- Attributes must be unique at their level.
- Element and attribute names used must be valid XML when returned by the script. If data is to be returned as an element or an attribute name that is not valid for XML, the name can be encoded using the [ToCMBase64String] function. The inserter will recognize names encoded with this function and will decode them during the raw insert process. The inserter is a Collector job that is executed during each collection. It is responsible for parsing the Agent results files and putting the data into a new raw database table. The raw data is then transformed into the data that appears in the nodes in the user interface.

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

- If a script has configurable parameters, they should be described in a comment block near the top of the script, along with configurable entries of the parameters near the top of the script, so that a user who is cloning a WCI collection filter can easily see and set the parameters in the **Edit Filter** wizard (in **Administration > Collection Filters > Filters**).
- Declaration of variables, and any other tasks in a script that produce output that is not part of the XML result set, should be redirected to out-null, such as:

```
[reflection.assembly]::LoadWithPartialName("Microsoft.SqlServer.Smo") > out-null
```

- The default WCI filter returns PowerShell version information from VCM-managed machines.
- Do not include any formatting white space. For example, do not use CR LF at the end of elements, nodes, or attributes.

See also the example below of developing a custom PowerShell script for use with the WCI data type.

Example of Developing a Custom PowerShell Script for Use with the WCI Data Type

In this example, the objective is to collect scheduled tasks information from Windows clients. On newer systems, Windows conveniently provides the `schtasks.exe` utility to report on scheduled tasks created either through the Task Scheduler user interface or through use of the `AT` command.

- Running `schtasks` by itself returns only basic data about tasks.
- Adding the `/query /v` switches provides additional information, but the formatting is difficult for automated processing.
- The `schtasks /query /?` command provides additional possibilities.
- The option set of `schtasks /query /v /fo:csv` is selected as the source for the data for the collection script. These options give full details for all tasks in a comma-separated value result set.

PowerShell makes working with tabular result sets from commands easy. A first step for this script is to run a command similar to:

```
$schtasks = schtasks /query /v /fo:csv
```

Since the data returned from `schtasks` includes multiple rows, PowerShell makes the `$schtasks` variable into an array. As such, `$schtasks[0]` represents the first row returned from the command. Viewing the result set by looking at `$schtasks[n]` shows that that the first line, `$schtasks[0]`, is blank; `$schtasks[1]` contains column names, and `$schtasks[2]` is the first row of task data. The goal, then, is to parse this data into a structure compatible with VCM's XML format for return to the Collector.

The Scheduled Tasks script uses the `split` method of PowerShell strings to separate the columns of the `$schtasks` rows into separate values in arrays. The column names row provides the names to use for attributes, and the corresponding data from the scheduled task rows provide the values to use for these attributes.

Once parsed, the XML returned by the script should look something like:

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

The <schtasks> top-level name is an arbitrary name picked to distinguish the results of this script from others. A couple of additional challenges must also be overcome with this data, related to column names returned by the `schtasks` command, and the fact that the `schtasks` command does not include any unique and repeatable identifier for specific task entries. Details about these challenges are described next.

The first challenge can be seen by looking at the column names returned by the `schtasks` command. Even the basic `schtasks` command (no options) has a column name of Next Run Time. Since this column name includes spaces, it cannot be used as-is as an attribute name in an XML document. Other column names returned by the more verbose execution of `schtasks` have similar problems. To preserve these column names in the form that they are returned from the `schtasks` command, but still allow for XML handling, the names are encoded with the `ToCMBase64String` function:

```
function ToCMBase64String([string]$input_string)
{
    return [string]("cibase64-" +
[System-
tem.Co-
nvert]::ToBase64String([System.Text.Encoding]::UNICODE.GetBytes($input_
string))).replace("=","-")
}
```

This function uses Unicode base64 encoding, along with some character substitution (a dash instead of an equal sign) to create an XML-legal form of any element or attribute name. The string is prefixed with `cibase64-` to indicate to the VCM inserter that the data will need to be decoded prior to loading it into the VCM database. The end result is that rather than containing invalid data like this:

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

The XML will contain this:

```
<cibase64-TgBlAHgAdAAgAFIAdQBucAAVABpAG0AZQA->
    12:32:00, 5/26/2010
</cibase64-TgBlAHgAdAAgAFIAdQBucAAVABpAG0AZQA->
```

The second problem is that the <schtasks> command does not include any unique and repeatable identifier for specific task entries. For example, many test systems observed had more than one task with the name: `GoogleUpdateTaskMachineCore`. Unique element names are a requirement for valid VCM XML, and repeatable identifiers are desirable to prevent false indications of changes at the VCM Collector. For example, if the script was to arbitrarily label rows as `Task1`, `Task2`, ..., and `Task1` was deleted, `Task2` would then become `Task1`, and VCM would show a lot of changed details for `Task1` (command line changed, next run time changed, etc), when in fact, that task had not changed at all – it had only changed places in the sequence.

One way to handle creation of unique and repeatable names for elements is to create a name based on a hash of the data contained in the row. That is useful for data that has no name-type attribute at all. In this case, however, there is a task name, but it is not guaranteed to be unique. Since the task name is user-friendly and useful, it is desirable to try to preserve and use it through the collection script. To preserve it,

the task name is used as the element name for task rows, but the “increment” option is selected for duplicate handling when creating a collection filter based on this script. This action allows the collection process to add an incremental entry to a list of multiple entries with the same task name: the first example of `GoogleUpdateTaskMachineCore`, while the second example will be relabeled as `GoogleUpdateTaskMachineCore_1`.

It is still possible that reordering the list among tasks that have the same name, will cause “extra” changes to be reported, but regardless of these changes, it is reasonable to have VCM display the friendly task names in the user interface. Because task names also can contain characters that would not be valid for XML element names, the task names, as with the column names, are encoded using the `ToCMBase64String` function.

Troubleshooting Custom PowerShell Filter Scripts

You can interactively test a custom PowerShell script using the following procedures.

Procedure

Verify the script runs correctly within a PowerShell shell.

1. Start PowerShell from the command line on a VCM-managed machine.
2. Paste the inspection script into the PowerShell shell window.
3. Depending on the last character, it may require one extra hit of the Enter key to start the script
4. The script should run to completion without throwing any errors (red text in the command line based powershell.exe environment).
5. Once completed, the script should return a set of XML, without any formatting white space (no CR LF at the end of elements, nodes, or attributes).
6. When this test is successful, run the script from a file.

Procedure

After you have verified the script runs correctly within PowerShell, run the script from a file:

1. Save the script to a .ps1 file.
2. From a command line run the script directly:
 - For PowerShell 2.0, execute: `PowerShell -command set-executionpolicy RemoteSigned -scope Process ; scriptname.ps1 > resultfile.xml`
 - For PowerShell 1.0 (with the execution policy already set to Remote Signed or less restrictive), execute: `PowerShell -file scriptname.ps1 > resultfile.xml`

When the script is complete, the XML result file should be created.

3. Verify that the XML file in question can be opened in Internet Explorer (you may have to allow blocked content in order to see the entire file). If the XML file cannot be parsed by Internet Explorer, the formatting errors in the XML from the script will need to be corrected before the script can be used as a collection filter script. Visual Studio can be a useful tool for finding formatting errors in larger XML files.

For details the job status reporting for WCI, see [Getting Started Collecting Windows Custom Information](#).

Discover, License, and Install UNIX/Linux Machines

The following steps must be performed before collecting data from UNIX/Linux machines:

1. Add UNIX/Linux machines.
2. License your UNIX/Linux machines.
3. Install the VCM Agent on your UNIX/Linux machines.
4. Perform an initial UNIX/Linux collection.
5. Explore the UNIX/Linux collection results.

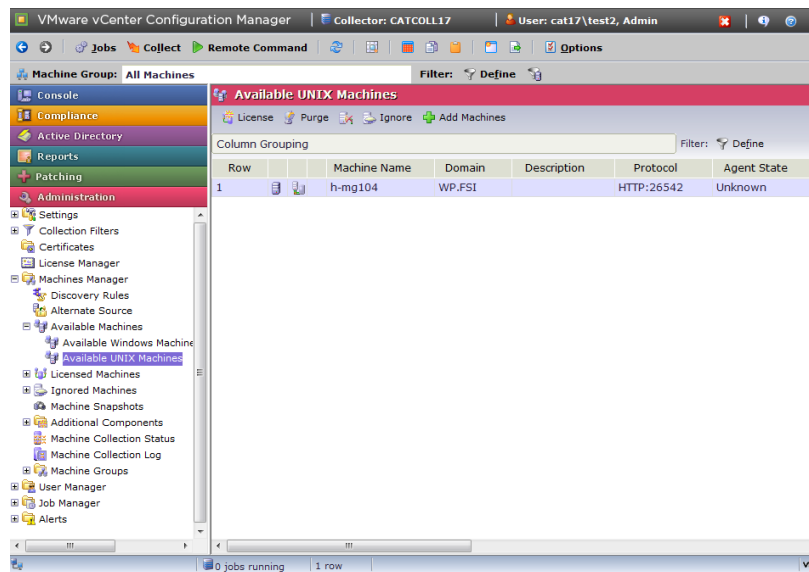
These steps are explained in the following subsections.

Adding UNIX/Linux Machines

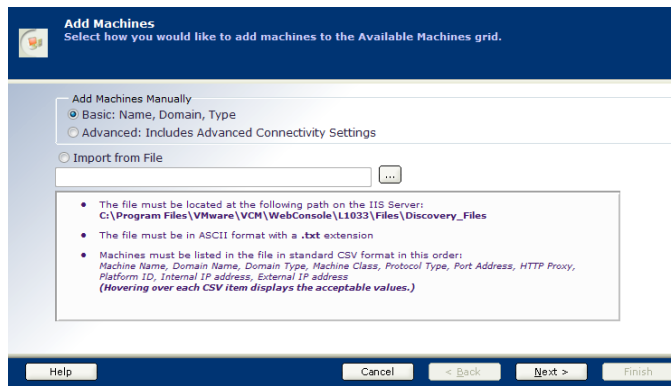
Before you can collect data from your UNIX/Linux machines, they must be displayed in the Available UNIX Machines list located in the Portal under **Administration > Machines Manager > Available Machines**.

NOTE A Discovered Machines Import Tool (DMIT) is available from VMware Customer Support to assist you with the following process. This tool imports machines discovered by the Network Mapper (Nmap) into the configuration database. To use the tool, contact VMware Customer Support; otherwise, use the following process.

1. Click **Administration > Machines Manager > Available Machines > Available UNIX Machines**.



2. Click **Add Machines**. The **Add Machines** page appears.



3. Select **Basic**, and then click **Next**. The **Manually Add Machines - Basic** page appears.

NOTE When you expand your UNIX/Linux collections to a broader set of machines, you may want to use other methods to add your UNIX/Linux machines. Refer to the online Help for the advanced features such as importing from a file or using IP Discovery.

4. Enter the **Machine** and the **Domain**, and then select **DNS** for **Type**. For **Machine Type**, select the appropriate operating system. Modify the port number if you are not using the default.

NOTE The port number specified must be the same number used when the Agent is installed on the managed UNIX/Linux machine.

5. Click **Add** to add the entry to the list.
6. Repeat for any other machines.
7. Click **Next** and accept the changes.

NOTE If your Collector cannot resolve a host name with a DNS Server, be sure to use an IP address in place of a Machine name for your machines as you enter them.

Licensing UNIX/Linux Machines

When the UNIX/Linux machines are displayed in your Available UNIX Machines list, you may begin licensing these machines.

Upgrading Red Hat Workstations

In previous versions of VCM, either Red Hat workstations or servers were licensed as Red Hat servers. Beginning with VCM version 5.2.0, Red Hat machines were licensed as either workstations or servers. When you upgrade to 5.2.0 or later, the workstations previously managed with server licenses will be unmanaged in VCM. The unmanaged Red Hat workstations should be listed in the Available UNIX Machines list. To manage the machines in VCM, select **Administration > Machines Manager > Available Machines > Available UNIX Machines** and re-license the machines using Linux/Mac Workstation licenses.

If you are not able to identify your unmanaged Red Hat machines, contact VMware Customer Support.

Use the following procedure to license your UNIX/Linux machines.

1. Click **Administration > Machines Manager > Available Machines > Available UNIX Machines**.

NOTE Remember, discovered machines with an indeterminate **Machine Type** will not be licensed if they are included in your selection.

2. Select the machine(s) you want to license. To select multiple machines, use **Shift-click** or **Ctrl-click**.
3. Click **License**. The **Machines** page appears.
4. The machines that you specified appear in the **Selected** area. Add or remove machines from the list as needed.
5. Click **Next**. The **Product License Details** page appears.
6. The licensed machine count has increased by the number of machines that you have selected to license.
7. Click **Next**. The **Important** page appears.
8. Review the information.
9. Click **Finish**.

Installing the Agent on UNIX/Linux Machines

Before collecting data from your UNIX/Linux machines, you must install the VCM Agent on each licensed UNIX/Linux machine. For information about upgrading existing Agents, see the online Help.

IMPORTANT The Collector should be installed before the Agents are installed. The configuration parameter `CSI_USER` assigns the account used to run the Agent daemon or service. If the parameter is changed, the user account must not have a valid login shell. You must be logged in to a target UNIX/Linux machine as root.

NOTE If you have copied your custom configuration file from a previous installation, follow the optional step provided in this procedure. If you are using a custom configuration file, perform the installation in Silent Mode.

Installing the Agent on UNIX/Linux machines is a manual operation.

NOTE A Deployment Tool is available from Customer Support to assist you with the following process for UNIX/Linux. To use the tool, contact support; otherwise, follow the steps in the following process.

IMPORTANT To install the UNIX Agent on SUSE and Red Hat machines, you may need to disable or reconfigure firewalls.

Platforms Not Supported for Upgrade to 5.4 Agent

Installing or upgrading on the following platforms is supported only to the 5.1.3 UNIX Agent. You can install the 5.4 Agent. However, these platforms are not tested with any additional 5.4 functionality.

Platform	Supported Agent Version	Agent File Name
AIX 4.3.3	5.1.3	CMAgent.5.1.0.AIX.4
Red Hat 2.1	5.1.3	CMAgent.5.1.0.Linux.2.1
Solaris 2.5	5.1.3	Contact VMware Customer Support if you are installing or upgrading the Agent on this platform.
Solaris 2.6	5.2.1	Contact VMware Customer Support if you are installing or upgrading the Agent on this platform.

Use the following steps to install the Agent.

1. Verify that the machine on which you intend to install the agent has enough free disk space. For more information, see the *VCM Hardware and Software Requirements Guide*.
2. When VCM is installed on the VCM Collector machine, the necessary Agent packages are created in the following locations:

\Program Files (x86)\VMware\VCM\Installer\Packages

or

The following agent binaries are available for the associated operating systems:

Operating System Version	Agent Binary
Red Hat (Enterprise) Linux Edition (Version 2.1)	CMAgent.<version>.Linux.2.1
Red Hat (Enterprise) Linux Edition (Version 3.0, 4.0, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5) SUSE Linux Enterprise Server (9, 10), Debian (4)	CMAgent.<version>.Linux
Solaris (Versions 8, 9, and 10 supported on Sparc)	CMAgent.<version>.SunOS
Solaris (Version 10 for x86)	CMAgent.<version>.SunOS.x86.5.10
HP-UX 11i Versions 1.0, 2.0, 3.0 (11.11, 11.23, and 11.31; Supported on PA-RISC)	CMAgent.<version>.HP-UX.11.pa
HP-UX 11i Version 2.0, 3.0 (11.23 and 11.31-Supported on Itanium)	CMAgent.<version>.HPUX.11.ia64
AIX Version 4.3.3	CMAgent.<version>.AIX.4
AIX Version 5L (5.1, 5.2, 5.3, and 6L (6.1))	CMAgent.<version>.AIX.5

3. Copy the installation package to the machine on which you want to install the agent. You can use **ftp**, **sftp**, or **cp** using an NFS share.

NOTE If you use ftp to copy the package to your machine, be sure to use binary mode.

4. Use `chmod u+x <filename>` to change the permissions on the agent binary file.
5. In the directory where you copied the file, execute the agent binary package to create the necessary directory structure and extract the files. The command and output will look similar to the following example, with differing file names depending on the operating system:

```
# ./CMAgent.<version>.SunOS
UnZipSFX 5.51 of 22 May 2004, by Info-ZIP (http://www.info-zip.org).
creating: CSIInstall/
creating: CSIInstall/packages/
inflating: CSIInstall/packages/Agent.1.0.SunOS
inflating: CSIInstall/packages/CFC.1.0.SunOS
inflating: CSIInstall/packages/ECMu.1.0.SunOS
inflating: CSIInstall/packages/ThirdParty.1.0.SunOS
inflating: CSIInstall/packages/cis.1.0.SunOS
extracting: CSIInstall/packages/package.sizes.SunOS
inflating: CSIInstall/packages/python.23.SunOS
creating: CSIInstall/scripts/
inflating: CSIInstall/scripts/checksum
inflating: CSIInstall/scripts/BootStrapInstall.sh
inflating: CSIInstall/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>

```

NOTE To force an overwrite of any existing files, include the `-o` option when executing the package. For example: `/CMAgent.<version>.SunOS -o`.

6. Change the directory to the location where the `InstallCMAgent` executable file was extracted. For example:


```
# cd <extractedpath>/CSIInstall
```
7. Use the `ls -la` command to validate that the following files are in this directory:
 - **InstallCMAgent:** The installation script.
 - **csi.config:** The configuration file for the installation, where you can modify the installation options.
 - **packages:** Contains the installation packages.
 - **scripts:** Contains the scripts needed for the install.
8. To customize the settings for the installation variables, modify the installation configuration file, `csi.config`, and then save your changes. If this file has only read permissions set, you will need to give the file write permissions with the `chmod u+x csi.config` command. See the following installation options for details.

Installation Options with Default Values	Description
<code>CSI_AGENT_RUN_OPTION</code>	<p>The Agent can be installed as a daemon process or installed to be run by <code>inetd/xinetd/launchd</code>.</p> <ul style="list-style-type: none"> • A value of <code>inetd</code> will install the Agent for execution by <code>inetd/xinetd/launchd</code>. • A value of <code>daemon</code> will install the agent for execution as a daemon process.
<code>CSI_NO_LOGIN_SHELL=</code> <code>+S:+A:+/sbin/noshell+/bin/false+</code> <code>/sbin/false+/usr/bin/false</code> <code>+/sbin/nologin</code>	<p>The <code>CSI_USER</code> account must not have a login shell. This parameter lists all valid no-login shells and is used to verify the <code>CSI_USER</code> has no-login shell.</p> <p>If your system has a valid no login shell that is not listed, then append a plus sign and add the no login shell to the list.</p> <p>The options available for this parameter include:</p> <ul style="list-style-type: none"> • <code>+S</code> means only for Solaris • <code>+A</code> means only for AIX • <code>+H</code> means only for HP-UX • <code>+L</code> means only for Linux • <code>+D</code> means only for Darwin (Mac OS X) • <code>+</code> means for all OS

Installation Options with Default Values	Description
CSI_CREATE_USER=Y Recommend keeping default value.	The user is being created. This value indicates whether or not the user is to be created. Note: When installing in trusted mode on HP-UX v1.0 (11.11), the user must already exist on the target machine. If you attempt to install and create the user, the installation of the Agent fails.
CSI_USER_ID=501 Recommend keeping default value.	This value is the integer value for the user ID of the created user.
CSI_USER_NO_LOGIN_SHELL=/bin/false Recommend keeping default value.	Indicates the desired no-login shell value to use when creating the user.
CSI_USER_PRIMARY_GROUP=csi_acct Recommend keeping default value.	Group name to use when creating 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 Recommend keeping default value.	This value indicates the need to create a low-security primary group for the CSI_USER.
CSI_USER_PRIMARY_GID=501 Recommend keeping default value.	Create user's primary Group ID.
CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID=Y Recommend keeping default value.	Setting this option to Y will allow the Group ID to be the next available local Group ID over CSI_USER_PRIMARY_GID.
CSI_USER=csi_acct Recommend keeping default value.	The user assigned to the cfgsoft group. The CSI listener process runs under this user.
CSI_CFGSOFT_GID=500 Recommend keeping 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.
CSI_CREATE_LOCAL_GROUP=Y Recommend keeping default value.	Setting this option to Y allows the cfgsoft group to be created. This setting allows the system call to groupadd.
CSI_USE_NEXT_AVAILABLE_LOCAL_GID=Y Recommend keeping default value.	Setting this option to Y will allow this Group ID to be the next available local Group ID starting at CSI_CFGSOFT_GID.
CSI_AGENT_PORT=26542 Recommend keeping default value.	This option specifies the port that the CM Agent will be listening on.

Installation Options with Default Values	Description
CSI_CREATE_LOCAL_SERVICE=Y Recommend keeping default value.	Setting CSI_CREATE_LOCAL_SERVICE to Y allows the system to create the local service (copy files to system directories).
CSI_REFRESH_INETD=Y 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	Setting this option to allows the system to refresh xinetd (Linux) or inetd (Solaris, AIX, and HP-UX).
CSI_NICE=10 Recommend keeping default value.	This option sets the nice value for the agent listener process.
CSI_CERTIFICATE_PATH=	This option 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 can use this option to have the certificates put in the Agent location (VMware encourages you to install the Enterprise Certificates so that multiple Collectors collecting from the same set of Agents can be supported). If this package was copied from a collector installation, this package already contains that Collector's Enterprise Certificate.
CSI_PARENT_DIRECTORY=/opt	This option specifies the parent directory of the CM Agent. The root directory of CMAgent will be CSI_PARENT_DIRECTORY/CMAgent.
CSI_PARENT_DATA_DIRECTORY=/opt	This option specifies the parent directory of the CMAgent data directory. The data directory will be CSI_PARENT_DATA_DIRECTORY/CMAgent/data
CSI_PARENT_LOG_DIRECTORY=default	This option specifies where agent operational log files are kept. The log directory is CSI_PARENT_LOG_DIRECTORY/CMAgent/log. The default value indicates to use the following: <ul style="list-style-type: none"> • Linux - /var/log • AIX, HP-UX, and Solaris - /var/adm • Mac OS X - log ->private/var/log/CMAgent/log
CSI_KEEP_CSIINSTALL=N Recommend keeping default value.	After a successful installation, the temp installation directory CSIInstall is deleted. To keep this installation directory, set this parameter to Y.

- If you modified and saved the csi.config installation file, copy the saved csi.config to the extracted location. For example:

```
# cp /<safelocation>/csi.config /<extractedlocation>/CSIInstall/csi.config
```
- Change the directory to the location where the InstallCMAgent executable file was extracted. For example:

```
# cd <extractedpath>/CSIInstall
```
- Execute InstallCMAgent in either silent mode or interactive mode, as described in the following options.

NOTE If you are using the custom configuration file, csi.config, proceed with the installation in Silent Mode.

Silent Mode:

If you execute InstallCMAgent in silent mode, the installation proceeds silently. It uses the

values specified in `csi.config` without prompting for input. To run the installation in silent mode, enter:

```
# ./CSIInstall/InstallCMAgent -s
```

You might use this method if you have manually edited the `csi.config` file, if you have 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.

When the silent installation completes, a summary of the installation process and status is displayed. Make sure the installation completed without errors.

You can check the installation status at anytime by viewing the installation log file at `<CSI_PARENT_DIRECTORY>/log/install.log`.

Interactive Mode:

If you execute the installation with no options, it runs in an interactive mode, prompting you to accept or change each parameter in the `csi.config` file.

NOTE When you use interactive mode, the `csi.config` file is modified.

To run the installation in interactive mode, enter:

```
# ./CSIInstall/InstallCMAgent
```

During the pre-installation stage of interactive mode, the check for a valid user (`CSI_USER`) is performed. If the user already exists (either the Administrator has manually added the account or is selecting an existing one), the following configuration values will not be requested (the questions will be skipped) by the installer:

- `CSI_USER_NO_LOGIN_SHELL`
- `CSI_USER_PRIMARY_GROUP`
- `CSI_USER_PRIMARY_GID`
- `CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID`

These prompts will be requested only when the `CSI_USER` user account is not found.

When the silent installation completes, a summary of the installation process and status is displayed. Make sure the installation completed without errors.

You can check the installation status at anytime by viewing the installation log file at `<CSI_PARENT_DIRECTORY>/log/install.log`.

NOTE If you selected `(x)inetd/launchd` for `CSI_AGENT_RUN_OPTION` and `(x)inetd/launchd` is not running, the agent will not install. A message appears indicating the service is not running. On some versions, when `(x)inetd/launchd` services are not configured, `(x)inetd/launchd` will not stay running. To allow the UNIX/Linux agent installation to complete successfully, pass a `- stayalive` option to `(x)inetd/launchd`.

12. In addition to creating the necessary user and groups, and configuring the machine to run the Agent, the installation also creates a new directory in the `<CSI_PARENT_DIRECTORY>` named `CMAgent` (unless this directory was changed in the configuration). This directory contains the following files and subdirectories:

```
# ls -la /CSI_PARENT_DIRECTORY/CMAgent
```



```

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
drwxr-xr-x 2 root root 4096 Jul 2 17:34 uninstall

```

- To verify the Agent was installed correctly and is listening on the port and ready to collect data, execute the following command:

```
# netstat -na | grep <port_number>
```

Where the default <port_number> is typically 26542 for VCM installations.

- For SUSE machines, after the installation completes, you may need to start xinetd using the command:

```
# ./etc/init.d/xinetd start
```

After you have installed the Agent on the UNIX/Linux machines, you are now ready to start collecting data from them. To do this, see "Performing a UNIX/Linux Collection". After selecting UNIX/Linux machines, note that UNIX/Linux data classes are available for collection.

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 execute jobs such as collections and remote commands will increase slightly. The time required will vary based on how much new or updated content needs to be synchronized between the Collector and the agent. This content push will happen when the first communication is initiated after installing the UNIX agent package, or when there is new patch content on the Collector that is applicable to the UNIX agent platform since the last agent/collector communication occurred.

Manually Uninstalling the UNIX/Linux Agent

Every installation generates an uninstall script, `UninstallCMAgent`, located at:

```
<path>/CMAgent/uninstall
```

Consider these points when uninstalling an Agent:

- 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. Refer to "Locating the Agent Directory" if necessary.
- After executing `UninstallCMAgent`, VMware recommends that you delete the remaining the `CMAgent` directory prior to running a new installation.

To uninstall the Agent, use the steps in the following procedure. If you want to use a custom configuration file, follow the optional step below before uninstalling the Agent.

1. (Optional) Copy `csi.config`, the file that contains all of the custom configuration settings, to a safe location. (This file can be found in `<path>/CMAgent/install.`)
2. Navigate up one level from the `uninstall` directory in the `CMAgent` directory.
3. Run the `uninstall` script using the following command:

```
# ./uninstall/UninstallCMAgent
```

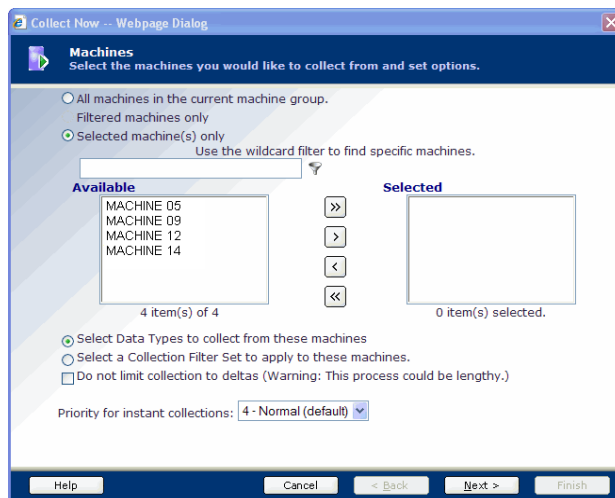
NOTE Consider these points when uninstalling an Agent:

- 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. Refer to "Locating the Agent Directory" later in this document if necessary.
 - After executing `UninstallCMAgent`, VMware recommends that you delete the remaining the `CMAgent` directory prior to running a new installation.
-

Performing a UNIX/Linux Collection

After the UNIX/Linux machines are added and licensed in VCM, and installed with the VCM Agent, you can perform a collection on those machines. The process for performing a UNIX/Linux collection is similar to other collections, including Windows, except that you select UNIX data types during your collection instead of Windows data types.

1. Click **Collect** on the Portal toolbar.
2. The **Collection Type** wizard page appears. Select **Machine Data**, and then click **OK**. The **Machines** page appears.

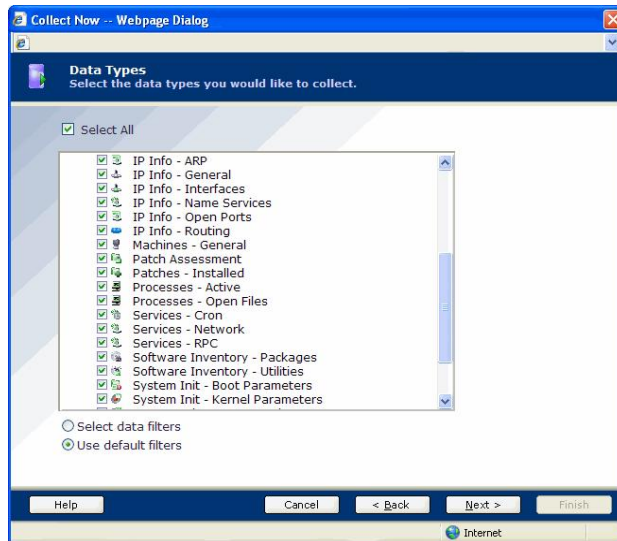


3. Select the machine(s) from which you want to collect data. To select multiple machines, use **Shift-click** or **Ctrl-click**. Use the double arrow to move all visible machines to the selection window, 500 at a time. Leave the default options selected, then click **Next**.

NOTE UNIX Patch Assessment is automatically licensed and enabled if you have licensed your UNIX/Linux Agent machines. If you are upgrading from a previous version of VCM, you will need a new license file to access this functionality.

In order to view Patch Assessment data, click **Select a Collection Filter Set to apply to these machines**

instead of the default collection options, and then select the UNIX Patch Assessment filter set. For more information, see the "UNIX Patch Assessment" Help topic.



4. The **Data Types** dialog box appears. Select the **Select All** check box, then confirm that the **Use default filters** option button is also selected. Click **Next**.
5. For initial collections, there should be no conflicts with previously scheduled or running jobs containing the same data types. Click **Finish**.
6. Verify that your collection job has completed before proceeding to the next step. To do so, click the **Jobs** button at the top of the Portal window to access the Jobs Summary.

NOTE You can also verify jobs for the past 24 hours if you think that you may have missed your collection job by going to **Administration > Job Manager > History > Instant Collections > Past 24 Hours**. Refer to the online Help for additional detail regarding Jobs.

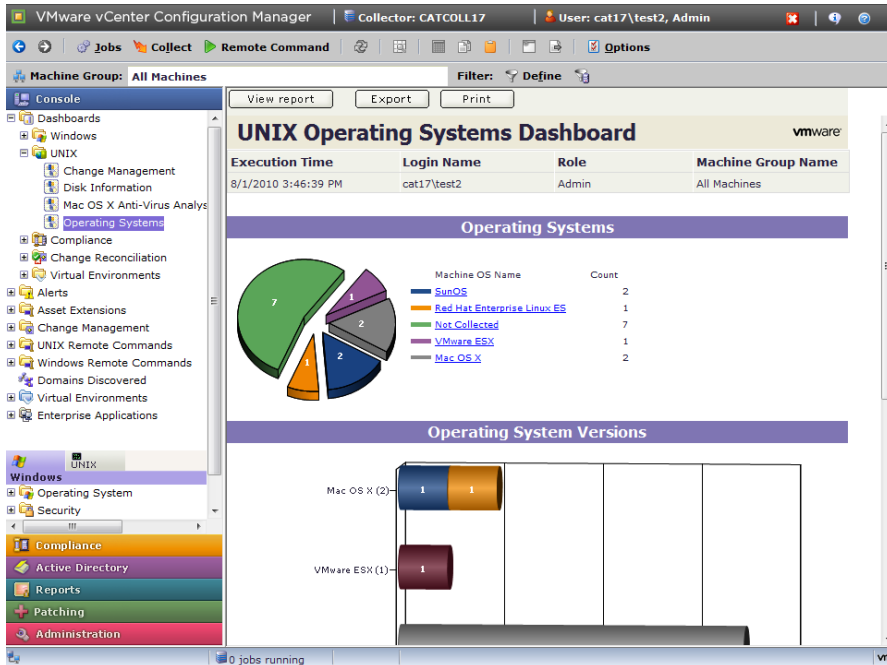
Exploring UNIX/Linux Collection Results

Now that you have performed an initial UNIX/Linux collection, you can explore that data in the Portal.

Dashboards

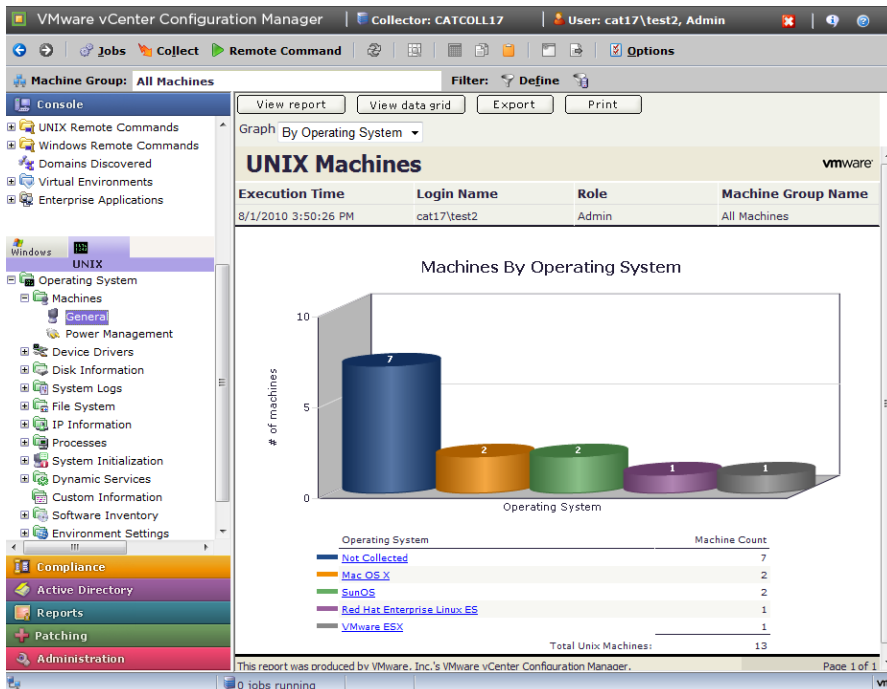
Each Dashboard is run only when the node is selected against the current data available in the CMDB for the machines in the active machine group. Therefore, Dashboard data is only current as of the time it was collected. In addition, it may take time for the data to display based on the volume or complexity of the data requested.

Begin by looking at the UNIX Operating System Dashboard under **Console > Dashboards > UNIX > Operating Systems**.



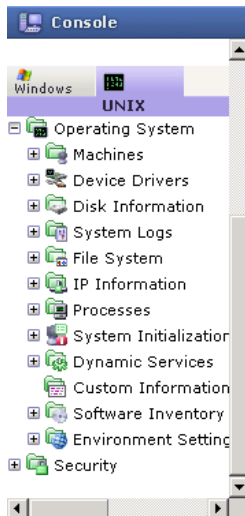
Note that several other UNIX Dashboards are also available. Take time to familiarize yourself with the remainder of the UNIX Dashboards. UNIX Collection Results are also available to you in a more “raw” format as well. This level of reporting is more relevant for day-to-day operations, troubleshooting, and analysis, and can be viewed in a Summary report or data grid format.

Look at your UNIX Operating System information by clicking the UNIX tab in the Console. Then, click **Operating System > Machines > General**.



When you select the node, you see a Summary Report as displayed above of the data type that you selected. Click **View data grid** to go directly to the data grid, or click an area of the Summary Report to filter the data before the data grid appears.

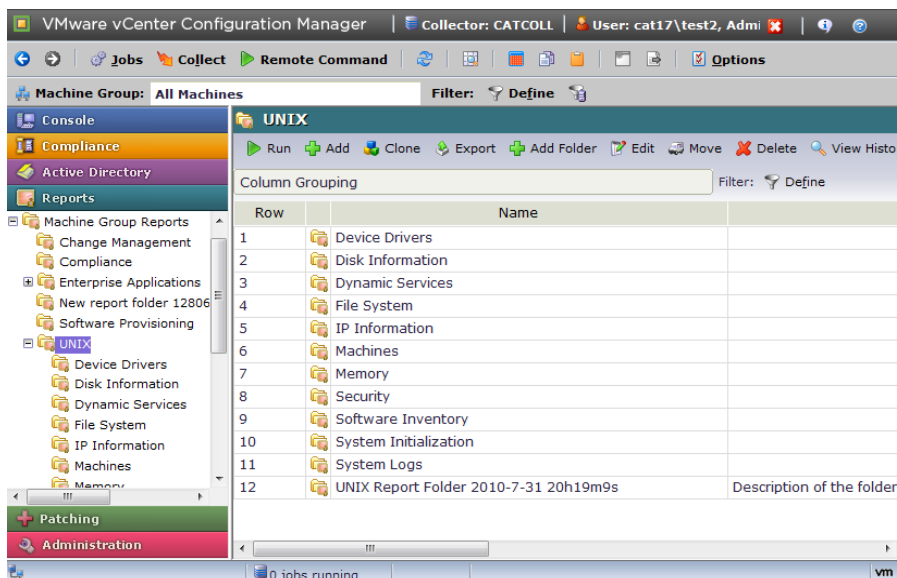
Several other categories (called “data classes”) of information regarding your UNIX/Linux Collection are available under the UNIX tab.



The UNIX tab is where the remainder of your collected UNIX/Linux data is visible through the Portal.

Reports

An alternate way to view your collected UNIX/Linux data is by running VCM Reports or creating your own custom reports using VCM’s reporting wizard. To begin exploring the reporting functionality, go to the **Reports** slider, then click **Machine Group Reports > UNIX**.



Like Dashboards, Reports are run real time against the current data available in the CMDB for the machines in the active machine group, and therefore they are only as current as the time of the last collection. In addition, it may require time for the report to generate based on the volume or complexity of the data requested. Refer to the online Help for more information on how to schedule and disseminate reports.

Compliance

You may now begin to check Compliance values for your collected data. To run a Compliance check, select the **Compliance** slider, then follow the steps described in the online Help to create rule groups, rules, filters, and templates.

Discover, License, and Install Mac OS X Machines

Getting Started with VCM for Mac OS X

The following steps must be performed before collecting data from Mac OS X machines:

1. Add Mac OS X machines.
2. License your Mac OS X machines.
3. Install the VCM Agent on your Mac OS X machines.
4. Perform an initial Mac OS X collection.
5. Explore the Mac OS X collection results.

These steps are explained in the following subsections.

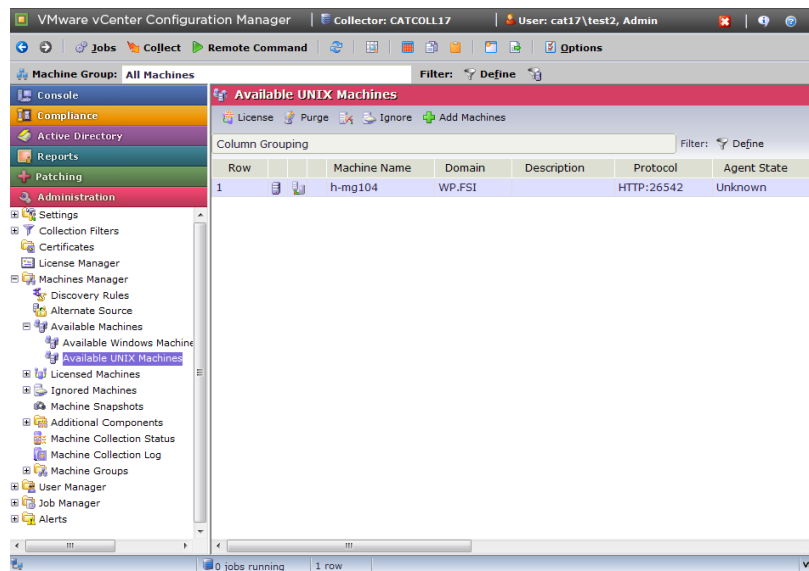
Mac OS X machines are managed in conjunction with UNIX machines.

Adding Mac OS X Machines

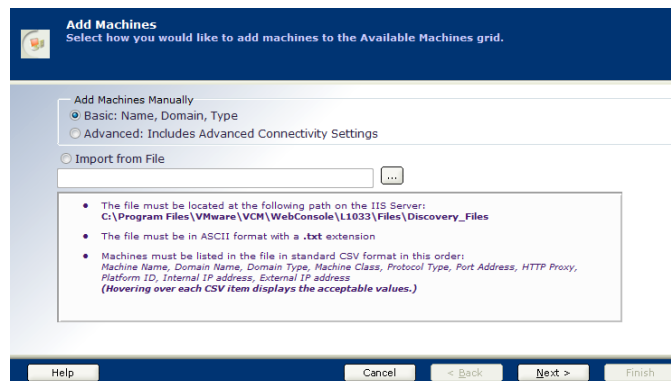
Before you can collect data from your Mac OS X machines, they must be displayed in the Available UNIX Machines list located in the Portal under **Administration > Machines Manager > Available Machines**.

NOTE A Discovered Machines Import Tool (DMIT) is available from VMware Customer Support to assist you with the following process. This tool imports machines discovered by the Network Mapper (Nmap) into the configuration database. To use the tool, contact VMware Customer Support; otherwise, use the following process.

1. Click **Administration > Machines Manager > Available Machines > Available UNIX Machines**.

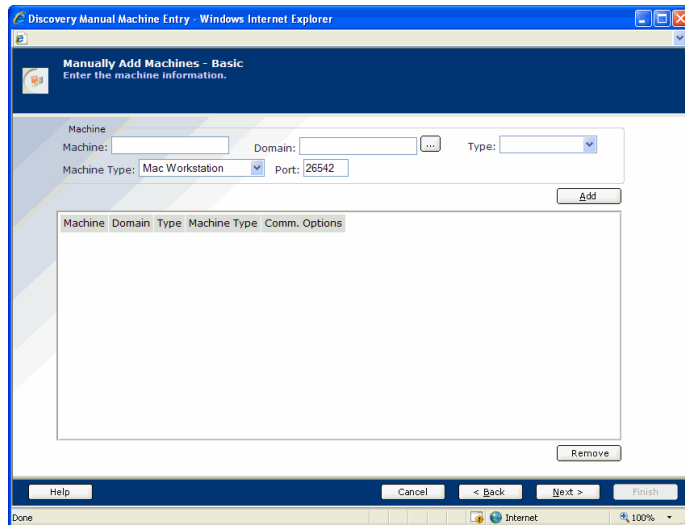


2. Click **Add Machines**. The **Add Machines** page appears.



3. Select **Basic**, and then click **Next**. The **Manually Add Machines - Basic** page appears.

NOTE When you expand your Mac OS X collections to a broader set of machines, you may want to use other methods to add your Mac OS X machines. Refer to the online Help for the advanced features such as importing from a file or using IP Discovery.



4. Enter the **Machine** and the **Domain**, and then select **DNS** for **Type**. For **Machine Type**, select the appropriate operating system. Modify the port number if you are not using the default.

NOTE The port number specified must be the same number used when the Agent is installed on the managed Mac OS X machine.

5. Click **Add** to add the entry to the list.
6. Repeat for any other machines.
7. Click **Next** and accept the changes.

NOTE If your Collector cannot resolve a host name with a DNS Server, be sure to use an IP address in place of a Machine name for your machines as you enter them.

Licensing Mac OS X Machines

When the Mac OS X machines are displayed in your Available UNIX Machines list, you may begin licensing these machines.

Use the following procedure to license your Mac OS X machines.

1. Click **Administration > Machines Manager > Available Machines > Available UNIX Machines**.

NOTE Remember, discovered machines with an indeterminate **Machine Type** will not be licensed if they are included in your selection.

2. Select the machine(s) you want to license. To select multiple machines, use **Shift-click** or **Ctrl-click**.
3. Click **License**. The **Machines** page appears.
4. The machines that you specified appear in the **Selected** area. Add or remove machines from the list as needed.

5. Click **Next**. The **Product License Details** page appears.
6. The licensed machine count has increased by the number of machines that you have selected to license.
7. Click **Next**. The **Important** page appears.
8. Review the information.
9. Click **Finish**.

Installing the Agent on Mac OS X Machines

Before collecting data from your Mac OS X machines, you must install the VCM Agent on each licensed Mac OS X machine.

IMPORTANT The Collector should be installed before the Agents are installed. The configuration parameter `CSI_USER` assigns the account used to run the Agent daemon or service. If the parameter is changed, the user account must not have a valid login shell. You must be logged in to a target Mac OS X machine as root, or have sudo as root.

NOTE If you have copied your custom configuration file from a previous installation, follow the optional step provided in this procedure. If you are using a custom configuration file, perform the installation in Silent Mode.

Installing the Agent on Mac OS X machines is a manual operation. The Agent is packaged as a Universal Binary Installer.

Use the following steps to install the Agent.

1. Verify that the machine on which you intend to install the agent has enough free disk space. For more information, see the *VCM Hardware and Software Requirements Guide*.
2. When VCM is installed on the VCM Collector machine, the necessary Agent packages are created in the following locations:

`\Program Files (x86)\VMware\VCM\Installer\Packages`

or

The following agent binaries are available for the associated operating systems:

Operating System Version	Agent Binary
Mac OS X (Version 10.4 and 10.5)	CMAgent.<version>.Darwin

3. Copy the installation package to the machine on which you want to install the agent. You can use **ftp**, **sftp**, or **cp** using an NFS share.

NOTE If you use ftp to copy the package to your machine, be sure to use binary mode.

4. Use `chmod u+x <filename>` to change the permissions on the agent binary file.
5. In the directory where you copied the file, execute the agent binary package to create the necessary directory structure and extract the files. The command and output will look similar to the following example, with differing file names depending on the operating system:

```
# ./CMAgent.<version>.Darwin
UnZipSFX 5.51 of 22 May 2004, by Info-ZIP (http://www.info-zip.org).
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
```

NOTE To force an overwrite of any existing files, include the `-o` option when executing the package. For example: `/CMAgent.<version>.Darwin -o`.

6. Change the directory to the location where the `InstallCMAgent` executable file was extracted. For example:


```
# cd <extractedpath>/CSIInstall
```
7. Use the `ls -la` command to validate that the following files are in this directory:
 - **InstallCMAgent:** The installation script.
 - **csi.config:** The configuration file for the installation, where you can modify the installation options.
 - **packages:** Contains the installation packages.
 - **scripts:** Contains the scripts needed for the install.
8. To customize the settings for the installation variables, modify the installation configuration file, `csi.config`, and then save your changes. If this file has only read permissions set, you will need to give the file write permissions with the `chmod u+x csi.config` command. See the following installation options for details.

Installation Options with Default Values	Description
<code>CSI_AGENT_RUN_OPTION</code>	<p>The Agent can be installed as a daemon process or installed to be run by <code>inetd/xinetd/launchd</code>.</p> <ul style="list-style-type: none"> • A value of <code>inetd</code> will install the Agent for execution by <code>inetd/xinetd/launchd</code>. • A value of <code>daemon</code> will install the agent for execution as a daemon process.
<code>CSI_NO_LOGIN_SHELL=</code> <code>+S:+A:+/sbin/noshell+/bin/false+</code> <code>/sbin/false+/usr/bin/false</code> <code>+/sbin/nologin</code>	<p>The <code>CSI_USER</code> account must not have a login shell. This parameter lists all valid no-login shells and is used to verify the <code>CSI_USER</code> has no-login shell.</p> <p>If your system has a valid no login shell that is not listed, then append a plus sign and add the no login shell to the list.</p> <p>The options available for this parameter include:</p> <ul style="list-style-type: none"> • <code>+S</code> means only for Solaris • <code>+A</code> means only for AIX

Installation Options with Default Values	Description
CSI_CREATE_USER=Y Recommend keeping default value.	<ul style="list-style-type: none"> • +H means only for HP-UX • +L means only for Linux • +D means only for Darwin (Mac OS X) • + means for all OS
CSI_USER_ID=501 Recommend keeping default value.	This value is the integer value for the user ID of the created user.
CSI_USER_NO_LOGIN_SHELL=/bin/false Recommend keeping default value.	Indicates the desired no-login shell value to use when creating the user.
CSI_USER_PRIMARY_GROUP=csi_acct Recommend keeping default value.	Group name to use when creating 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 Recommend keeping default value.	This value indicates the need to create a low-security primary group for the CSI_USER.
CSI_USER_PRIMARY_GID=501 Recommend keeping default value.	Create user's primary Group ID.
CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID=Y Recommend keeping default value.	Setting this option to Y will allow the Group ID to be the next available local Group ID over CSI_USER_PRIMARY_GID.
CSI_USER=csi_acct Recommend keeping default value.	The user assigned to the cfgsoft group. The CSI listener process runs under this user.
CSI_CFGSOFT_GID=500 Recommend keeping 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.
CSI_CREATE_LOCAL_GROUP=Y Recommend keeping default value.	Setting this option to Y allows the cfgsoft group to be created. This setting allows the system call to groupadd.
CSI_USE_NEXT_AVAILABLE_LOCAL_GID=Y Recommend keeping default value.	Setting this option to Y will allow this Group ID to be the next available local Group ID starting at CSI_CFGSOFT_GID.
CSI_AGENT_PORT=26542 Recommend keeping default value.	This option specifies the port that the CM Agent will be listening on.
CSI_CREATE_LOCAL_SERVICE=Y Recommend keeping default value.	Setting CSI_CREATE_LOCAL_SERVICE to Y allows the system to create the local service (copy files to system directories).

Installation Options with Default Values	Description
CSI_REFRESH_INETD=Y 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	Setting this option to allows the system to refresh xinetd (Linux) or inetd (Solaris, AIX, and HP-UX). This option does not apply to Mac OS X.
CSI_NICE=10 Recommend keeping default value.	This option sets the nice value for the agent listener process.
CSI_CERTIFICATE_PATH=	This option 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 can use this option to have the certificates put in the Agent location (VMware encourages you to install the Enterprise Certificates so that multiple Collectors collecting from the same set of Agents can be supported). If this package was copied from a collector installation, this package already contains that Collector's Enterprise Certificate.
CSI_PARENT_DIRECTORY=/opt	This option specifies the parent directory of the CM Agent. The root directory of CMAgent will be CSI_PARENT_DIRECTORY/CMAgent.
CSI_PARENT_DATA_DIRECTORY=/opt	This option specifies the parent directory of the CMAgent data directory. The data directory will be CSI_PARENT_DATA_DIRECTORY/CMAgent/data
CSI_PARENT_LOG_DIRECTORY=default	This option specifies where agent operational log files are kept. The log directory is CSI_PARENT_LOG_DIRECTORY/CMAgent/log. The default value indicates to use the following: <ul style="list-style-type: none"> • Linux - /var/log • AIX, HP-UX, and Solaris - /var/adm • Mac OS X- log ->private/var/log/CMAgent/log
CSI_KEEP_CSIINSTALL=N Recommend keeping default value.	After a successful installation, the temp installation directory CSIInstall is deleted. To keep this installation directory, set this parameter to Y.

- If you modified and saved the csi.config installation file, copy the saved csi.config to the extracted location. For example:

```
# cp /<safelocation>/csi.config /<extractedlocation>/CSIInstall/csi.config
```
- Change the directory to the location where the InstallCMAgent executable file was extracted. For example:

```
# cd <extractedpath>/CSIInstall
```
- Execute InstallCMAgent in either silent mode or interactive mode, as described in the following options.

NOTE If you are using the custom configuration file, csi.config, proceed with the installation in Silent Mode.

Silent Mode:

If you execute InstallCMAgent in silent mode, the installation proceeds silently. It uses the values specified in csi.config without prompting for input. To run the installation in silent

mode, enter:

```
# ./CSIInstall/InstallCMAgent -s
```

You might use this method if you have manually edited the `csi.config` file, if you have 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.

When the silent installation completes, a summary of the installation process and status is displayed. Make sure the installation completed without errors.

You can check the installation status at anytime by viewing the installation log file at `<CSI_PARENT_DIRECTORY>/log/install.log`.

Interactive Mode:

If you execute the installation with no options, it runs in an interactive mode, prompting you to accept or change each parameter in the `csi.config` file.

NOTE When you use interactive mode, the `csi.config` file is modified.

To run the installation in interactive mode, enter:

```
# ./CSIInstall/InstallCMAgent
```

During the pre-installation stage of interactive mode, the check for a valid user (`CSI_USER`) is performed. If the user already exists (either the Administrator has manually added the account or is selecting an existing one), the following configuration values will not be requested (the questions will be skipped) by the installer:

- `CSI_USER_NO_LOGIN_SHELL`
- `CSI_USER_PRIMARY_GROUP`
- `CSI_USER_PRIMARY_GID`
- `CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID`

These prompts will be requested only when the `CSI_USER` user account is not found.

NOTE The User and the Group are created in the local directory service storage.

When the silent installation completes, a summary of the installation process and status is displayed. Make sure the installation completed without errors.

You can check the installation status at anytime by viewing the installation log file at `<CSI_PARENT_DIRECTORY>/log/install.log`.

NOTE If you selected `(x)inetd/launchd` for `CSI_AGENT_RUN_OPTION` and `(x)inetd/launchd` is not running, the agent will not install. A message appears indicating the service is not running. On some versions, when `(x)inetd/launchd` services are not configured, `(x)inetd/launchd` will not stay running. To allow the UNIX/Linux agent installation to complete successfully, pass a `- stayalive` option to `(x)inetd/launchd`.

12. In addition to creating the necessary user and groups, and configuring the machine to run the Agent, the installation also creates a new directory in the `<CSI_PARENT_DIRECTORY>` named `CMAgent` (unless this directory was changed in the configuration). This directory contains the following files and subdirectories:

```
# ls -la /CSI_PARENT_DIRECTORY/CMAgent
```

```

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
drwxr-xr-x 2 root root 4096 Jul 2 17:34 uninstall

```

- To verify the Agent was installed correctly and is listening on the port and ready to collect data, execute the following command:

```
# netstat -na | grep <port_number>
```

Where the default <port_number> is typically 26542 for VCM installations.

After you have installed the Agent on the Mac OS X machines, you are now ready to start collecting data from them. To do this, see "Performing a Mac OS X Collection". After selecting Mac OS X machines, note that Mac OS X data classes are available for collection.

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 execute jobs such as collections and remote commands will increase slightly. The time required will vary based on how much new or updated content needs to be synchronized between the Collector and the agent. This content push will happen when the first communication is initiated after installing the UNIX agent package, or when there is new patch content on the Collector that is applicable to the UNIX agent platform since the last agent/collector communication occurred.

Manually Uninstalling the Mac OS X Agent

Every installation generates an uninstall script, `UninstallCMAgent`, located at:
<path>/CMAgent/uninstall

Consider these points when uninstalling an Agent:

- 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. Refer to "Locating the Agent Directory" if necessary.
- After executing `UninstallCMAgent`, VMware recommends that you delete the remaining the CMAGENT directory prior to running a new installation.

To uninstall the Agent, use the steps in the following procedure. If you want to use a custom configuration file, follow the optional step below before uninstalling the Agent.

- (Optional) Copy `csi.config`, the file that contains all of the custom configuration settings, to a safe location. (This file can be found in <path>/CMAGENT/install.)
- Navigate up one level from the uninstall directory in the CMAGENT directory.
- Run the uninstall script using the following command:

```
# ./uninstall/UninstallCMAgent
```

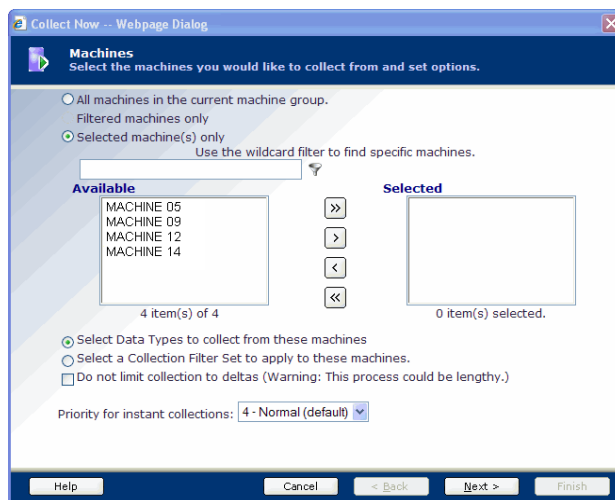
NOTE Consider these points when uninstalling an Agent:

- 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. Refer to "Locating the Agent Directory" later in this document if necessary.
 - After executing UninstallCMAgent, VMware recommends that you delete the remaining the CMAgent directory prior to running a new installation.
-

Performing a Mac OS X Collection

After the Mac OS X machines are added and licensed in VCM, and installed with the VCM Agent, you can perform a collection on those machines. The process for performing a Mac OS X collection is similar to other collections, including Windows, except that you select Mac OS X data types during your collection instead of Windows data types.

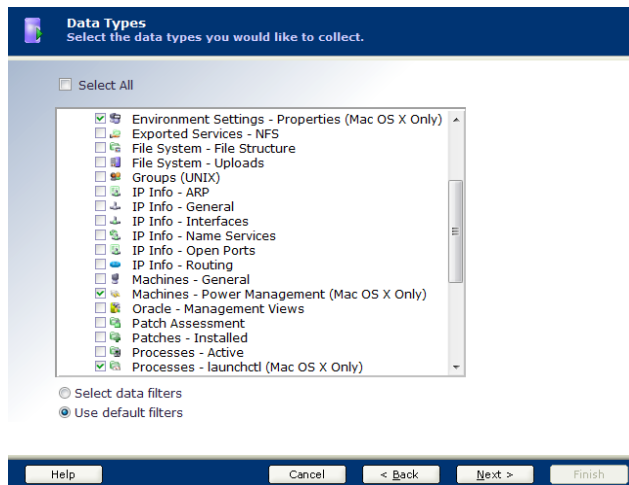
1. Click **Collect** on the Portal toolbar.
2. The **Collection Type** wizard page appears. Select **Machine Data**, and then click **OK**. The **Machines** page appears.



3. Select the machine(s) from which you want to collect data. To select multiple machines, use **Shift-click** or **Ctrl-click**. Use the double arrow to move all visible machines to the selection window, 500 at a time. Leave the default options selected, then click **Next**.

NOTE UNIX Patch Assessment is automatically licensed and enabled if you have licensed your UNIX/Linux Agent machines. If you are upgrading from a previous version of VCM, you will need a new license file to access this functionality.

In order to view Patch Assessment data, click Select a Collection Filter Set to apply to these machines instead of the default collection options, and then select the UNIX Patch Assessment filter set. For more information, see the "UNIX Patch Assessment" Help topic.



The data classes and filters for Mac OS X include the following:

- Machines > General
- File System > File Structure
- System Logs > syslog events
- IP Information > General
- IP Information > Routing
- IP Information > Interfaces (IF)
- IP Information > Open Ports
- Security > Users > Current
- Security > Users > Information
- Security > Groups
- Custom Information – subset of CITs
- Properties files (.plist)
- Machines > General
- File System > File Structure
- System Logs > syslog events
- IP Information > General
- IP Information > Routing
- IP Information > Interfaces (IF)
- IP Information > Open Ports
- Security > Users > Current
- Security > Users > Information
- Security > Groups
- Custom Information – subset of CITs
- Properties files (.plist)

4. The **Data Types** dialog box appears. Select the **Select All** check box, then confirm that the **Use default filters** option button is also selected. Click **Next**.
5. For initial collections, there should be no conflicts with previously scheduled or running jobs containing the same data types. Click **Finish**.
6. Verify that your collection job has completed before proceeding to the next step. To do so, click the **Jobs** button at the top of the Portal window to access the Jobs Summary.

NOTE You can also verify jobs for the past 24 hours if you think that you may have missed your collection job by going to **Administration > Job Manager > History > Instant Collections > Past 24 Hours**. Refer to the online Help for additional detail regarding Jobs.

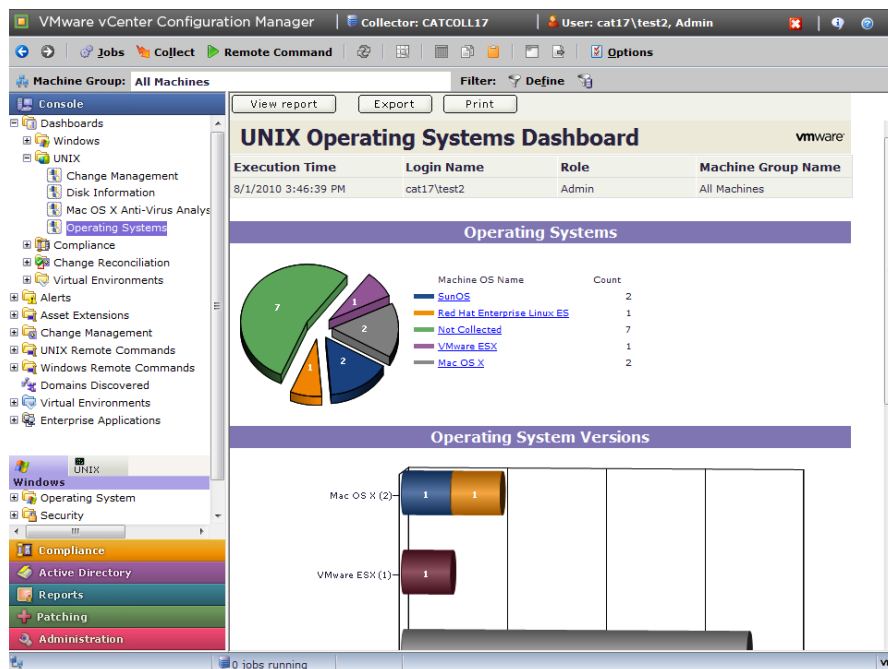
Exploring Mac OS X Collection Results

Now that you have performed an initial Mac OS X collection, you can explore that data in the Portal.

Dashboards

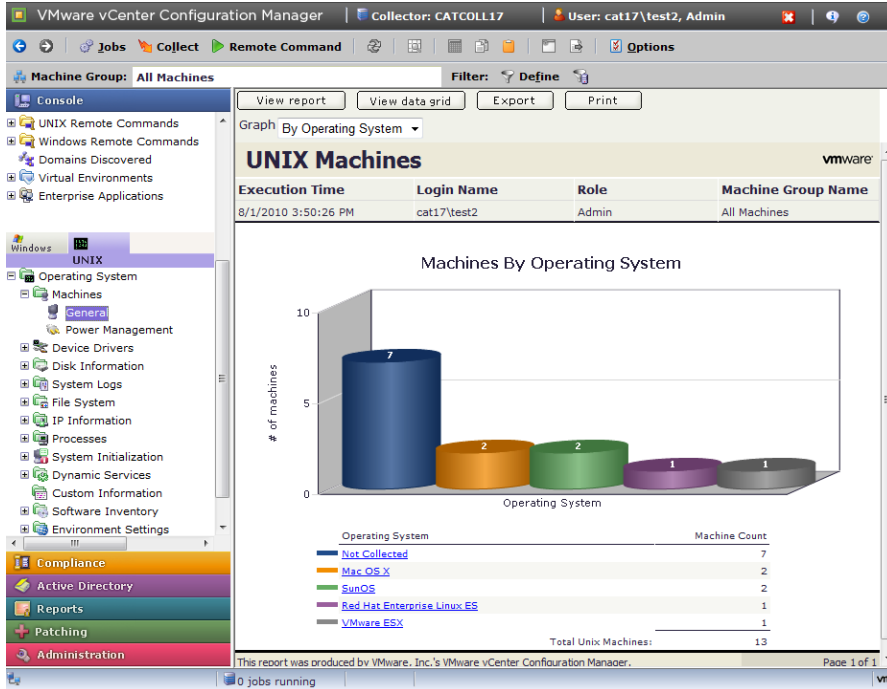
Mac OS X data is displayed in the UNIX Dashboards. Each Dashboard is run only when the node is selected against the current data available in the CMDB for the machines in the active machine group. Therefore, Dashboard data is only current as of the time it was collected. In addition, it may take time for the data to display based on the volume or complexity of the data requested.

To view Mac OS data, begin by looking at the UNIX Operating System Dashboard under **Console > Dashboards > UNIX > Operating Systems**.



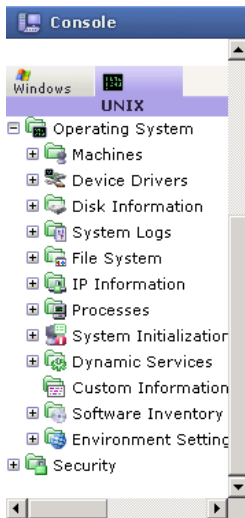
Note that several other UNIX Dashboards are also available. Take time to familiarize yourself with the remainder of the UNIX Dashboards. UNIX Collection Results are also available to you in a more “raw” format as well. This level of reporting is more relevant for day-to-day operations, troubleshooting, and analysis, and can be viewed in a Summary report or data grid format.

Look at your Mac OS X Operating System information by clicking the **UNIX** tab in the Console. Then, click **Operating System > Machines > General**.



When you select the node, you see a Summary Report as displayed above of the data type that you selected. Click **View data grid** to go directly to the data grid, or click an area of the Summary Report to filter the data before the data grid appears.

Several other categories (called “data classes”) of information regarding your Mac OS X Collection are available under the UNIX tab.

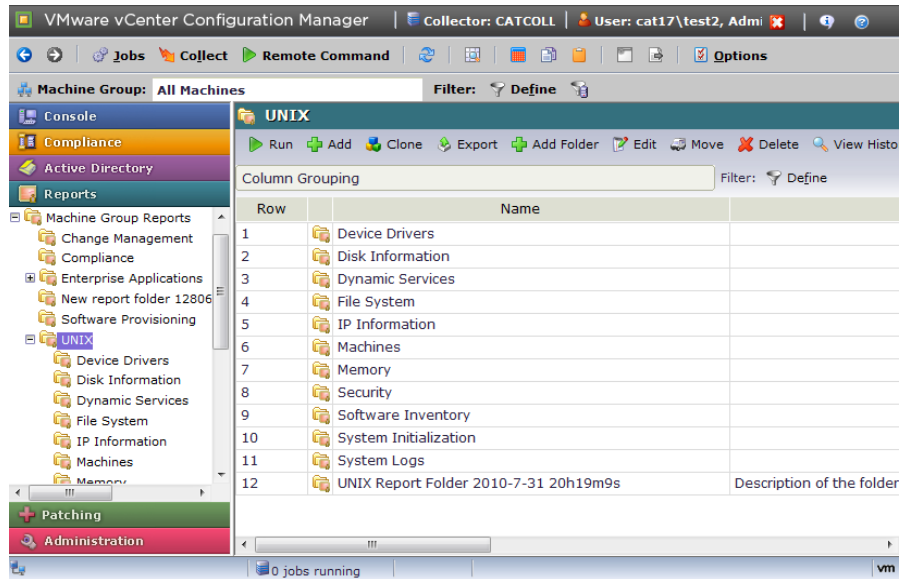


The UNIX tab is where the remainder of your collected Mac OS X data is visible through the Portal.

NOTE The displayed data is based on the collected Mac OS X data classes, also known as data types. See the Help for a list of currently collected data types.

Reports

An alternate way to view your collected Mac OS X data is by running VCM Reports or creating your own custom reports using VCM's reporting wizard. To begin exploring the reporting functionality, go to the **Reports** slider, then click **Machine Group Reports > UNIX**.



Like Dashboards, Reports are run real time against the current data available in the CMDB for the machines in the active machine group, and therefore they are only as current as the time of the last collection. In addition, it may require time for the report to generate based on the volume or complexity of the data requested. Refer to the online Help for more information on how to schedule and disseminate reports.

Compliance

You may now begin to check Compliance values for your collected data. To run a Compliance check, select the **Compliance** slider, then follow the steps described in the online Help to create rule groups, rules, filters, and templates.

Discover, License, and Collect Oracle Data from UNIX Machines

Welcome to VCM for Oracle. Now that you have installed VCM successfully, use the following steps to discover, collect, and work with Oracle data in VCM.

When getting started, you will first add the Oracle Instance, and then configure the Oracle Collection User account for database access. If you will be creating the Oracle Collection User account on Oracle 10g, see the following section about setting permissions on this account.

NOTE VCM uses the OS-authenticated Oracle Collection User account to connect to the Oracle database so that Oracle collections can be performed. This account can be created in two ways: 1) using the [Config User](#) action, or 2) using the [Oracle Account Setup remote command](#).

To get started with VCM for Oracle, follow these steps:

1. Add UNIX machines hosting Oracle and install the Agent.
2. Discover Oracle Instances.
3. Create the Oracle Collection User Account.
4. Perform an Oracle collection.
5. Explore Oracle collection results.
6. Explore reference information about Oracle.

For instructions on removing access to the Oracle database, see ["Removing Access to the Oracle Database" on page 127](#).

Adding UNIX Machines Hosting Oracle and Installing the Agent

1. Add UNIX machines in **Administration > Machines Manager > Available Machines > Available UNIX Machines > Add Machines**.
2. License UNIX machines in **Administration > Machines Manager > Available Machines > Available UNIX Machines > License**.
3. Install the Agent on one or more UNIX machines. See ["Installing the Agent on UNIX/Linux Machines" on page 99](#).

Discovering Oracle Instances

An Oracle Instance is a structure of memory and background processes used to interact with the Oracle database to access data. The Oracle Instance contains stored information that is shared by various Oracle processes, and private information used for particular processes.

The Oracle database includes the physical files used to store information, including database engine data files, containing database metadata control files, and log files of data changes for backup and recovery.

Use this view to add and configure an Oracle Instance on a machine. After an Oracle Instance has been added, you must configure the database access for the Oracle Collection User that VCM will use to collect from that Oracle Instance.

TIP After you have configured the Oracle Instance, use the **Config User** action to configure database access for the Oracle Collection User account.

1. Run a full collection on UNIX machines using the **Machines - General** and **Oracle - Management Views** data types. This process includes a discovery of Oracle Instances from the oratab file on Solaris machines. See ["Performing a UNIX/Linux Collection" on page 106](#) for more information about running collections on UNIX machines.
2. To edit or to manually add an Oracle Instance, see ["Adding Oracle Instances" on page 124](#).

Adding Oracle Instances

During the collection performed in the [previous section](#), the Agent retrieves **ORACLE_HOME**, **ORACLE_SID** and **Oracle Software Owner** from the oratab file, and displays the data in VCM. Review the list of Oracle instances populated in **Administration > Machines Manager > Additional Components > VCM for Oracle**.

Add an Oracle Instance

To add an Oracle Instance to a UNIX machine, follow these steps:

1. In **Administration > Machines Manager > Additional Components > VCM for Oracle**, click **Add**. The **Add Oracle Instances** wizard opens.
2. Select the machine(s) on which you want to add an Oracle Instance. Click **Next**. The **Configuration Values** wizard page appears.

NOTE On UNIX Machines, a **Machines - General** collection is necessary to see machines in the wizard. Supported UNIX machines displayed in the wizard include Solaris versions 9 and 10.

3. Enter the configuration values for each Oracle Instance (**Oracle SID**, **Oracle Home**, **Oracle SW Owner**, **DBA Group**, and **Oracle Collection User**). See the VCM for Oracle data grid for definitions of these values. Click **Next**, and then click **Finish**.

NOTE If VCM already contains the machine and **Oracle SID** that are added, a conflict screen appears showing the machine and Instance that are in conflict. If other values exist, which were changed for the conflicting machine and Instance, the "Update the existing Instances" check box appears. If you want to update the existing Instance, check this box. Otherwise, the Instance will not be updated.

Edit an Oracle Instance

1. In **Administration > Machines Manager > Additional Components > VCM for Oracle**, click **Edit**. The Edit Oracle Instances wizard opens.
2. Select the machine(s) on which you want to edit an existing Oracle Instance. Click **Next**. The **Configuration Values** wizard page appears.
3. Check the box next to a configuration value you want to modify. See the VCM for Oracle data grid for definitions of these values. Click **Next**, and then click **Finish**.

Creating the Oracle Collection User Account

After the Oracle Instance has been added, use one of these methods to configure the Oracle Collection User account for database access to Oracle Instances:

- [Create the Oracle Collection User Account with the Config User Action](#)
- [Create the Oracle Collection User Account with a Remote Command](#)

If you are working with Oracle 10g, see ["Permissions for Oracle Collection User Account on Oracle 10g" on page 128](#) for more information.

Creating the Oracle Collection User Account with the Config User Action

The **Configure Oracle User** action configures database access to Oracle Instances for the Oracle user. You can create the Oracle Collection User account on Oracle 10g. If you are working with Oracle 10g, see ["Permissions for Oracle Collection User Account on Oracle 10g" on page 128](#) for more information.

To create the OS-authenticated Oracle Collection User account with the **Config User** action, follow these steps:

1. Click **Config User**. The **Select Oracle Instances** wizard opens.
2. Select one or more **Oracle Instances**. You can set a filter on these items. Click **Next**, and then click **Finish**.

Filter the Oracle Instances based on:

- Machine Name
 - Oracle Home (Collected)
 - Oracle Home (Override)
 - Oracle SID
 - Oracle Software Owner (Override)
 - Oracle Software Owner (Override)
 - Oracle User
3. In the **Schedule** wizard page, set the job timing schedule. You can run the action immediately or schedule it to run later. Click **Next**.

You can remove access to the Oracle database. See ["Removing Access to the Oracle Database" on page 127](#).

Creating the Oracle Collection User Account with a Remote Command

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 so that Oracle collections can be performed.

The preferred method is to create the Oracle Collection User account using the [Config User action](#). Or, you can use the UNIX Remote Command, as described in the instructions below.

NOTE You can add Oracle Instances and create Oracle Collection User accounts on supported 64-bit and 32-bit UNIX machines.

For instructions on removing access to the Oracle database, see [Removing Access to the Oracle Database](#).

Setting Account Permissions on Oracle 10g

If you will be creating the Oracle Collection User account on Oracle 10g, see ["Permissions for Oracle Collection User Account on Oracle 10g" on page 128](#) for information about setting permissions on this account.

Create the Oracle Collection User Account with a Remote Command

To create the OS-authenticated Oracle Collection User account with a remote command, follow these steps:

1. Edit the **Install Oracle Collection User Account** remote command in **Console > UNIX Remote Commands > Oracle Account Setup**. Click the **Install Oracle Collection User Account** remote command, and then click **Edit**. The Remote Commands wizard appears.
2. Review the default values for the remote command and edit them with the correct values for your environment. Example values are shown here.
 - a. Type the **ORACLE_SID** (Oracle instance).
 - b. Type the **ORACLE_HOME** (path).
 - c. Type the **ORACLE_COLLECTION_USER_ACCOUNT**. If an account is not specified, the **ORACLE_COLLECTION_USER_ACCOUNT** named "csiora" will be created by default.
 - d. Type the **ORACLE_SOFTWARE_OWNER_ACCOUNT**. If left blank, VCM will attempt to derive it by determining the owner of the **ORACLE_HOME** directory. This account is used to log into the Oracle database to create the Oracle OS-authenticated User account (Oracle Collection User account).

3. On the **Files Wizard** page, select the **InstallOracleCollectionUserAccount.sh** file.
4. Run the job as root. If desired, select the option of storing results on the VCM Collector.
5. Select the machine(s) on which to create the Oracle Collection User account.
6. Select to run the remote command now. As the remote command is running, the following actions will be performed:
 - a. Action will be run with root privileges (for example, **Setuid – RunHigh**).
 - b. If the local user does not exist, a non-privileged OS user account will be created and the password will be locked.
 - c. Switch or "su" to the **ORACLE_SOFTWARE_OWNER_ACCOUNT** that was provided.
 - d. Connect to the Oracle database using the sqlplus binary.
 - e. Create the Oracle OS-authenticated User account if it does not exist.
 - f. Grant the Oracle OS-authenticated User account the **SELECT_CATALOG** role (privilege necessary for accessing data dictionary views and packages).
 - g. If the option was chosen to store results in a local directory, the job status (success or failure) will be returned here.

If you no longer want to collect from an Oracle database, you can remove access to the Oracle database.

Removing Access to the Oracle Database

To remove access to the Oracle database, follow these steps:

1. Edit the **Uninstall Oracle Collection User Account** remote command in **Console > UNIX Remote Commands > Oracle Account Setup**. Click the **Uninstall Oracle Collection User Account** remote command, and then click **Edit**. The Remote Commands wizard appears.
2. Review the default values for the remote command and edit them with the correct values for your environment. Example values are shown here.
 - a. Enters the **ORACLE_SID** (Oracle instance)
 - b. Enter the **ORACLE_HOME** (path).
 - c. Enters the **ORACLE_COLLECTION_USER_ACCOUNT** that should be removed.
 - d. Either enter the **ORACLE_SOFTWARE_OWNER_ACCOUNT**. If left blank, VCM will attempt to derive it by determining the owner of the **ORACLE_HOME** directory.
3. In the Files wizard page, select the **UninstallOracleCollectionUserAccount.sh** file.
4. Run the job as root. If desired, select the option of storing results on the VCM Collector.
5. Select the machine(s) on which to remove the Oracle account.
6. Select to run the remote command now. As the remote command is running, the following actions will be performed:
 - a. Action will be run with root privileges (for example, **Setuid - RunHigh**)
 - b. The non-privileged OS user account will be deleted.
 - c. Switch or "su" to the **ORACLE_SOFTWARE_OWNER_ACCOUNT** that was provided.
 - d. Connect to the Oracle database using the sqlplus binary.
 - e. The Oracle OS-authenticated account will be removed for Oracle database.

- f. If the option was chosen to store results in a local directory, the job status (success or failure) will be returned here.

1 After the Oracle OS-authenticated account is removed, VCM will not be able to collect Oracle data unless an account is recreated.

Permissions for Oracle Collection User Account on Oracle 10g

For Oracle 10g installations, permissions are set by default to prevent users who are not part of the Oracle DBA Group from accessing and executing files in the Oracle Home directory. Because the Oracle Collection User account typically does not belong to the Oracle DBA Group, problems may arise when executing SQL*Plus using the Oracle Collection User account.

Consequently, if this account does not have access to the necessary directories and files in Oracle Home to execute SQL*Plus, Oracle - Management View data will not be collected. Therefore, you must ensure that the Oracle Collection User account that is created has appropriate access to the required binaries.

For the Oracle Collection User account to execute SQL*Plus, you must grant Oracle directories read/read-execute permission grant Oracle directories read/read-execute permission.

Grant Permission to the Oracle Collection User Account to Execute SQL*Plus

The following Oracle directories must be granted permission:

`chmod o+rx <top level oracle install>` (for example, `/opt/oracle`, `/oracle`, etc.)

```
- repeat for every directory level from the top level install down to
$ORACLE_HOME

- Example: If the top level is /oracle, and $ORACLE_HOME is
/oracle/app/product/10.20.0/db_1, then:

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

- Continue, after verifying the $ORACLE_HOME environment variable is set:

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/lx1boot.nlb
chmod o+r $ORACLE_HOME/nls/data/*
chmod o+rx $ORACLE_HOME/oracore
chmod o+rx $ORACLE_HOME/oracore/zoneinfo
chmod o+r $ORACLE_HOME/oracore/zoneinfo/timezlrq.dat

```

Alternate Approach to Modify Permissions in Oracle

Oracle has provided a change permissions script, `changePerm.sh`, which is included with most Oracle 10g installations. This script is typically located in `$ORACLE_HOME/install` by default.

An alternate approach is to run the `changePerm.sh` script. Running this script relaxes permissions on several directories and files in Oracle Home so that users who are not part of the Oracle DBA Group can access parts of Oracle, such as SQL*Plus. However, because running this script grants every UNIX account read and execute permissions to most, if not all, directories and files in Oracle Home, this option is not recommended.

Performing an Oracle Collection

Run a collection on UNIX machines using the **Oracle - Management Views** data class. Any fields that were modified in the Oracle administration data grid will be used in collections of data performed during the discovery process.

NOTE To limit the amount of data stored in the change log, from collections performed using the **Oracle - Management Views** data class before the **Oracle Collection User** account was defined, ensure that you check the option, **Do not limit collection to deltas** for this collection.

Exploring Oracle Collection Results

After collecting Oracle data, view the data in the **Management Views** in **Console > Enterprise Applications > Oracle > Management Views**.

The Oracle Management Views display security information, including users, roles, and privileges; configuration settings; and database parameters for Oracle Instances. The data in these views is collected from views within each Oracle Instance on supported Solaris machines. Each **Oracle Management View** displays the Oracle data, the Machine Name, Instance Name (Oracle SID), and the date the data was last updated.

Reference Information about Oracle

For a list of supported Solaris machines, see the *VCM Hardware/Software Requirements Guide*.

The following views show additional VCM data. For additional information, see the online Help.

- VCM for Oracle data grid in **Administration > Machines Manager > Additional Components > VCM for Oracle**
- Management Views in **Console > Enterprise Applications > Oracle > Management Views**
- Oracle Management View Data Types
- Oracle Mgmt View – Audit Table Privs

For Oracle 9i Online Documentation, see:

(<http://www.oracle.com/pls/db92/db92.docindex?remark=homepage>)

For Oracle 10g Online Documentation, see:

(<http://www.oracle.com/pls/db102/homepage>)

Customize VCM for your Environment

You have now completed the preliminary setup procedures. For more information about how to use VCM, refer to online Help, available in the Portal. As always, if you have any questions or problems using VCM, contact VMware Customer Support. Customization of your environment is essential to fine-tune the visibility of configuration information so that the policies you develop and the actions you take are appropriate for your IT infrastructure.

As you learn more about VCM, it is highly advised that you take advantage of the organization of machines in your environment by creating a relevant machine group structure. These machine groups allow you to manage specific machines in your environment (for example, all SQL Servers in Ohio) and to apply specific changes or create Roles/Rules for those machines independently of other machines in your environment. This also ensures that access to critical machines can be restricted to appropriate personnel with rights to VCM. Additionally, you can customize the following options specifically for your environment:

- **Alerts:** The alerting system allows you to define the objects and types of changes that you are alerted to when they are detected in VCM. For example, you could set up an alert to notify you if a registry setting changes in your environment. Refer to the online Help on Alerts for more information.
- **Collection Filters and Filter Sets:** Use Collection Filters to specify the data that you want to collect from the machines that VCM manages. A default Collection Filter is provided for each data type. You can choose to add custom Collection Filters that are specific to your enterprise. Filters can be applied during Instant Collections and during Scheduled Collections if they are included as part of a filter set. Once you have created Collection Filters, organize them into Filter Sets. You might want to create specific Filter Sets or Filter Set Groups for different Machine Groups. Filter Sets can also be applied during Instant or Scheduled Collections. Refer to the online Help about Collection Filters for more information.
- **Compliance Templates and Rule Groups:** Use Compliance Templates and Rule Groups to define desired settings and check whether or not machines match those ideals. VCM comes with pre-packaged templates and rules that let you immediately start checking your machines' compliance to regulatory, industry, and vendor standards. Refer to the online Help for more information. Additionally, other compliance packages are available from VMware that can be imported into VCM post-installation. Refer to [Import/Export and Content Wizard](#) for more information.
- **Reports:** Use Reports to create and print tailored reports of information not shown specifically in VCM. VCM comes with pre-packaged reports that you can run as soon as you have collected data from your licensed machines. Refer to the online Help for more information.
- **Roles and Rules:** VCM roles and access rules work together to control a user's access to VCM. For example, you may create a role that allows a user to view all data, but not allow the user to make changes to the environment. Alternatively, you can create a role that can be used only to run certain reports, or a role that allows unlimited access to a single Machine Group. Refer to the online Help about User Manager for more information.

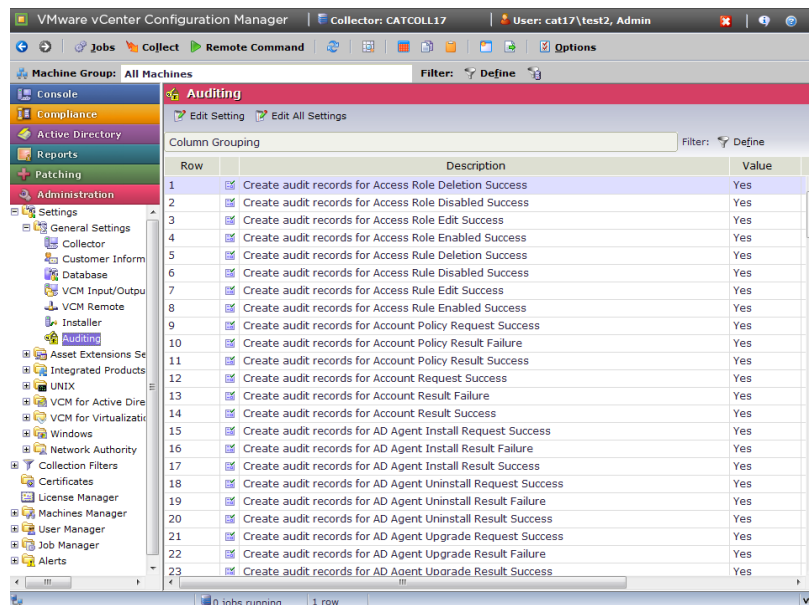
How to Set Up and Use VCM Auditing

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, independent of the VCM application. The format of the event log prohibits any modifications to the recorded entries, making it a secure, tamper-proof auditing record of changes in security.

When a user performs 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. Examples of VCM user actions that cause events to be written to the event log include user logon/logoff, session timeouts, changes in managing users, changes to passwords and administration settings, changes in network accounts and authority, collection requests, and service and registry changes.

NOTE Auditing settings can be enabled or disabled only by users who are assigned and logged in with the Admin role.

1. To view the VCM Auditing settings, navigate to the **Administration** slider. Select **Settings > General Settings > Auditing**.
2. To change an auditing setting, highlight a setting and then click **Edit Setting**. When a user changes an auditing setting, the VCM Auditing data grid displays the user's name in the Last Modified By column.



For details about the Auditing settings, and viewing the Windows Event Log, see the Administration: Auditing Settings topic in the online Help.

Getting Started with VCM for Virtualization

7

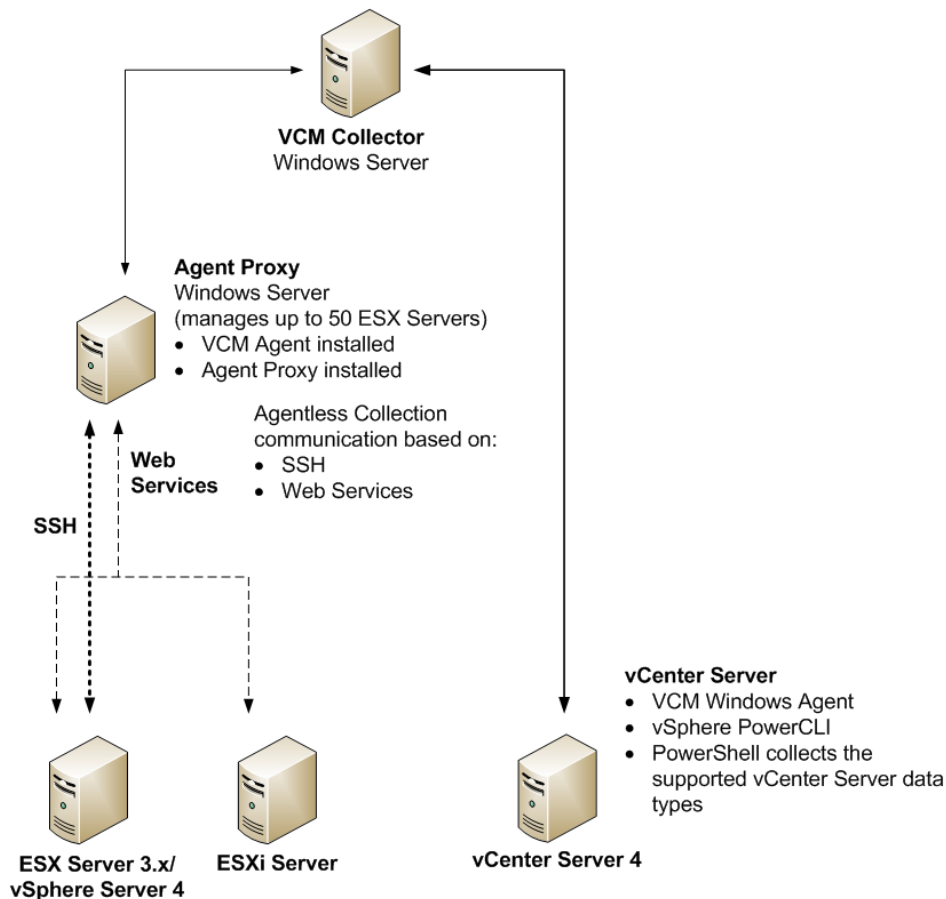
VCM collects virtualization configuration information for virtual machine hosts, their guest operating systems, and VMware vCenter Servers™.

The collected data is displayed in the Console slider under the Virtual Environments node. The information is organized in a logical grouping of the configurations of VM hosts, VM guest operating systems, and vCenter servers. Using the grouping, you can view your virtual environments at an enterprise level based on collected data.

Virtual Environments Configuration

To collect virtual environment data from VMware ESX® and VMware ESXi® servers and vCenter servers, you must configure different communication options for each target source.

- To collect ESX and ESXi data, you use an Agent Proxy rather than installing the VCM Agent directly on the ESX and ESXi servers.
- To collect data from VirtualCenter and vCenter servers, the VCM Agent is installed on the Windows machines running vCenter server.

Figure 1. Virtual Environments Configuration Diagram

ESX/ESXi Server Collections

When collecting from ESX and ESXi servers, you must configure at least one VCM Agent Proxy machine. You can configure the Collector as the Agent Proxy or configure standalone Agent Proxy machines. The Collector communicates with the Agent Proxy and the Agent Proxy then directly communicates with the ESX and ESXi servers using SSH and/or Web Services for necessary data collection actions. The data is processed by the Agent Proxy and relayed to the Collector.

The Agent Proxy machine must be a Windows server that meets the minimum hardware and software requirements specified in the *VCM Hardware and Software Requirements Guide*. A single Agent Proxy machine supports up to 50 ESX or ESXi servers.

VCM Support of ESXi

VCM supports collecting VM guest operating system and VM host data from ESXi machines. ESXi does not support SSH communication. Therefore, you cannot run UNIX remote commands or collect UNIX and Linux data types data on ESXi machines. Only Web service settings are required for ESXi machines. The License VM Host wizard for the ESXi machines includes SSH settings, but you should not configure them.

IMPORTANT When you collect data from ESXi servers, attempting to collect data other than VM hosts or VM guest operating data from the ESXi servers results in a collection failure. This restriction includes collection filters for ESX3.x and vSphere4 that are supplied with VCM. Running such collections on all the All VM Hosts Machine fails on the ESXi machines.

vCenter Server Collections

When collecting data from vCenter Server, you must license the Windows machine running the vCenter Server and install a VCM Agent (version 5.4 or later), PowerShell, and vSphere PowerCLI. The Agent runs the vCenter Server collection by using vSphere PowerCLI to access the vSphere API on vCenter server. The data is relayed to the Collector and added to the database.

Configuring vCenter Server Data Collections

Collecting vCenter server data is based on a process that extends beyond the standard Windows collection. The configuration of the process has several prerequisites. When the prerequisites are met, data is collected from vCenter Server by using default collection filters.

The configuration process includes several tasks.

- ["vCenter Server Collection Prerequisites" on page 135](#)
- ["Collect vCenter Server Data" on page 137](#)
- ["Reviewing Collected vCenter Server Data" on page 137](#)
- ["Troubleshooting vCenter Server Data Collections" on page 138](#)

vCenter Server Collection Upgrade Considerations

A new method for collecting vCenter Server data is introduced in VCM 5.4 that is simpler to implement and manage. The older method (5.3 and earlier), implemented using Windows remote commands, has been replaced with this new method.

Data that you previously collected by using the vCenter Server remote commands is no longer available. You must recreate scheduled collections to accommodate the new method. However, previously configured compliance rules, reports, and alerts based on the previously collected data are automatically redirected to the data in the new data grids.

vCenter Server Collection Prerequisites

The vCenter Server collection prerequisites prepare your environment for collecting data from vCenter Servers.

- ["Configure the VCM Agent with HTTP Communication" on page 135](#)
- ["Add vCenter Server User with Administrator Role" on page 136](#)
- ["Remove PowerShell v1.x from vCenter Servers" on page 136](#)
- ["Download and Install PowerShell v2.0 " on page 136](#)
- ["Download and Install VMware vSphere PowerCLI" on page 137](#)

Configure the VCM Agent with HTTP Communication

You must configure the VCM Agent (5.4 or later) on the vCenter server with HTTP communication. You cannot collect vCenter Server data if the Agent is not configured to use HTTP.

Prerequisites

Install the Agent (5.4 or later) on the vCenter server. See ["Discover, License, and Install Windows Machines" on page 69](#).

Procedure

1. Select **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines**.
2. Select the vCenter Server machines and verify that the **Protocol** field displays HTTP.
3. If HTTP is not displayed, change the protocol.
 - a. Click **Change Protocol**.
 - b. On the Machines page, verify the list of selected machines and click **Next**.
 - c. On the Change Protocol page, select **Switch to HTTP** and click **Next**.
 - d. On the Important page, review the number of selected machines, the type of change, and click **Finish**.

You can view the status of the change protocol job in Job Manager.

Add vCenter Server User with Administrator Role

The VCM Agent Network Authority Account must be added as a vCenter Server user with an Administrator Role. See the vCenter Client online help for information about adding users to vCenter.

Remove PowerShell v1.x from vCenter Servers

Before you can collect from vCenter Servers, you must first uninstall PowerShell 1.x from those machines. PowerShell 1.x is often installed by other applications and must be removed.

Procedure

1. Go to **Add/Remove Programs**.
2. Select **Show Updates**.

The list displays updates associated with installed programs.
3. Look for any of the following knowledge base numbers, which indicate earlier versions of PowerShell.

Versions of v1.x prior to RC2 are MS-based installations. These versions will appear as Windows PowerShell in the programs list.

 - KB926139 - Windows PowerShell v1.0 RTM - English Language Version
 - KB926140 - Windows PowerShell v1.0 RTM - Localized Installation Package
 - KB926141 - Windows PowerShell v1.0 RTM - MUI pack
 - KB925228 - Windows PowerShell v1.0 RC2
4. Uninstall any occurrence of PowerShell v1.x.

Download and Install PowerShell v2.0

Before you can collect data from vCenter Servers, you must install PowerShell 2.0 on those machines.

Prerequisites

- Uninstall previous versions of PowerShell. See ["Remove PowerShell v1.x from vCenter Servers" on page 136](#).
- Locate the PowerShell download page at <http://support.microsoft.com/kb/968929>.

Procedure

1. Download and install the appropriate version of PowerShell 2.0 included in the Windows Management Framework.
2. Reboot the vCenter Server machine.

Download and Install VMware vSphere PowerCLI

Before you can collect from vCenter Servers, you must install VMware vSphere PowerCLI 4.1 on those machines.

Prerequisites

Locate the VMware vSphere PowerCLI 4.1 download page at <http://www.vmware.com/support/developer/PowerCLI/index.html>. You must be registered on the VMWare Web site.

Procedure

1. Download and install VMware vSphere PowerCLI 4.1.

Collect vCenter Server Data

When you collect vCenter Server data, the collection is based on default collection filters for vCenter Host Profiles, vCenter Host Status, and vCenter Inventory.

Prerequisites

- Verify that you completed all the pre-collection prerequisites. See ["vCenter Server Collection Prerequisites" on page 135](#).
- Collect the Machines data type from the Windows machines on which vCenter Server is installed. This action identifies the machines as a vCenter Servers. See ["Performing an Initial Collection" on page 83](#).

Procedure

1. Click **Collect**.
2. On the Collection Type page, select **Machine Data** and click **Next**.
3. On the Machines page, select one or more vCenter Server machines and click **Next**.
4. On the Data Types page, expand **Windows**, select the **vCenter** data type, and click **Next**.
5. On the Important page, review and resolve any conflicts and click **Finish**.

What to do next

After you collect vCenter data, the vCenter servers and any VCM-managed Host machines are automatically added to the Virtual Environments machine groups. Using the machine group, you can schedule regular collection jobs to collect vCenter data. See ["Reviewing Collected vCenter Server Data" on page 137](#).

Reviewing Collected vCenter Server Data

You review collected vCenter Server data in the Console in the Virtual Environments node. The collected vCenter Server data helps you identify and manage VM Host machines.

Option	Description
Console	To view the collected vCenter data, select Console > Virtual Environments > vCenter > Host Profiles .

Troubleshooting vCenter Server Data Collections

If you encounter problems with vCenter collections, review the troubleshooting options.

vCenter Data Missing

Data does not appear in the vCenter server data grids.

Problem

After you collect vCenter data, the data grids do not display the new data.

Cause

The required VMware Web Services are not running on the vCenter machine

Solution

On the vCenter server machine, verify that the VMware VirtualCenter Management Web Services is running.

Configuring VM Host Collections

To manage your VM Host machines, ESX and ESXi servers, VCM uses an Agent Proxy rather than installing the VCM Agent directly on the ESX and ESXi machines. However, you must install other required files and certificates on the ESX and ESXi servers to manage the data collection from those machines.

After you configure the Agent Proxy, you should license, configure, and copy files as separate tasks, performing the tasks first for ESX servers and then for ESXi servers.

The configuration process includes the following tasks.

1. ["Configure the Collector as an Agent Proxy" on page 138](#)
2. ["License and Configure VM Hosts" on page 139](#)
3. ["Copy Files to the ESX/ESXi Servers" on page 141](#)
4. ["Perform an Initial Virtualization Collection" on page 142](#)
5. ["Reviewing Virtualization Collection Results" on page 143](#)

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 requirements to be an Agent Proxy and must only be configured for use by first licensing the Collector and then collecting the Machines data type.

NOTE If you manage more than fifty VM 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 for more information about configuring other Windows machines as Agent Proxies.

Procedure

1. Determine if the Collector is licensed by selecting **Administration > Machines Manager > Available Machines > Available Windows Machines**.
If the Collector is licensed, the machine is displayed in the Licensed Windows Machines data grid.
2. If the Collector is not listed in the Licensed Windows Machines data grid, license the Collector.
 - a. Select the Collector in the data grid and click **License**.
 - b. On the Machines page of the Available Machines License wizard, verify the Collector machine name is displayed in the Selected list and click **Next**.
 - c. Review the Product License Details page and click **Next**.
 - d. Review the Important page and click **Finish**.
 - e. Select **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines** to verify the Collector is now licensed.
 - f. Click **Refresh** on the Console toolbar to update the displayed data.
3. Select the Collector in the Licensed Windows Machines data grid and click **Collect** on the Console toolbar.
4. On the Collection Type page, click **Machine Data** and click **OK**.
5. On the Machines page, verify the Collector machine name is displayed in the Selected list, click **Select Data Types to collect from these machines** and click **Next**.
6. On the Data Types page, expand the Windows tree and select **Machines**.
7. Select **Use default filters** and click **Next**.
8. Review the Important page and click **Finish**.
The collection job starts. You can use the Job Manager to determine when the collection is completed.
9. When the collection is completed, select **Administration > Machines Manager > Agent Proxies** and verify the Collector machine Agent Proxy State equals Current Agent.

What to do next

License and configure the target VM Host machines. See ["License and Configure VM Hosts" on page 139](#).

License and Configure VM Hosts

When you license a VM Host, the licensing process generates a file containing machine names and settings. You use the generated file to configure the ESX and ESXi 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. Web Services must be set up on your VM Hosts before data can be collected.

Prerequisites

- Verify that at least one Agent Proxy machine is configured. See ["Configure the Collector as an Agent Proxy" on page 138](#).
- License the ESX and ESXi machines as UNIX machines. See ["Licensing UNIX/Linux Machines" on page 98](#).
- Verify that vCenter Server data is collected. If using vCenter, the hostname in vCenter must match the configured hostname of the ESX server. If the name does not match, you must manually add the machine. See the online Help.

Procedure

1. To license and configure settings for VM Hosts, select **Console > Virtual Environments > vCenter > Inventory > Manage VM Hosts**.
2. Add the machines to be configured to the lower grid and click **Next**.
The selected machines will all use the same Agent Proxy and the same SSH and Web Services settings.
3. Configure the settings on the Agent Proxy and Communication Setting page.

Option	Description
Agent Proxy	The configured Agent Proxy used to manage the selected VM Host machines. This option is required when you are licensing VM Hosts but optional if you are modifying the settings.
SSH Settings	Select the check box to configure the settings for your ESX machines. Configure these settings if you plan to collect VM Logs data from the managed VM Host machines. <ul style="list-style-type: none"> ■ Port: Used by VMware's 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 Settings	Select the check box to configure the settings for your ESX and ESXi machines. Configure the settings to collect virtual environment data from a VM host. <ul style="list-style-type: none"> ■ 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.

Option	Description
	<ul style="list-style-type: none"> ▪ Ignore untrusted SSL Certificate: Connection allowed even when certificates are not verified as trusted.

4. 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.

5. Click **Finish**.

The machines are displayed in the Licensed VM Hosts.

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 141](#).

Copy Files to the ESX/ESXi Servers

Using the UNIX/ESX/vSphere Deployment Utility on your Agent Proxy machines, you can import machine information from VCM and copy 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 ["License and Configure VM Hosts" on page 139](#).
- Locate the UNIX/ESX/vSphere Deployment Utility file. The Deployment Utility file is located on the Collector in C:\Program Files (x86)\VMware\VCM\Tools\DeployUtility-<version number>.
- Consult the see 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 VMHosts configuration file generated when you licensed and configured the VM 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 you defined in VCM.

7. Select a configuration option:

Option	Description
Configure ESX 3.x	Configures the SSH certificate, the csiprep.py file, the csiprep.config file, and

Option	Description
Servers	passes the SSH and Web Services user information to the target machines.
Configure ESXi Servers	Passes the Web Services to the target machines

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.

If you configured the settings in VCM and want to modify them, 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 VM Hosts. See "[Perform an Initial Virtualization Collection](#)" on page 142.

Perform an Initial Virtualization Collection

An initial collection of Virtual Environments data identifies your VM Host machines and their VM Guest machines.

Procedure

1. On the Portal toolbar, click **Collect**.
2. Select either your ESX or ESXi Servers.

To avoid configuration conflicts, do not select both for one action. The selected machines are displayed in the Selected list.
3. Click **Select Data Types to collect from these machines** and click **Next**.
4. For ESX machines only, on the Collection Wizard Data Type page, expand the UNIX node and select the **Machines - General** data type.
5. Expand the Virtualization node and select the **VM Hosts** and **VM Guests** data types.
6. Click **Use default filters** and click **Next**.
7. Click **Finish**.

You can monitor the collection job in Job Manager. When the collection is completed, the data is available for reports and compliance assessments.

What to do next

You review the collected data in the Console, run reports, configure alerts, and use the machine groups. See ["Reviewing Virtualization Collection Results" on page 143](#).

Reviewing Virtualization Collection Results

You have several options for reviewing and using virtualization 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.

Option	Description
Console	ESX and ESXi server information is available in Console > UNIX (tab) > Operating System > Machines > General . VM Host and Guest Summary information is available in Console > Dashboards > Virtual Environments .
Reports	To view reports related to your Virtual Environments, select Reports > Machine Group Reports > Virtual Environments . Additional reports for ESX/ESXi Servers are available in Reports > Machine Group Reports > UNIX , which display information from UNIX and Linux data types.
Machine Groups	VM Host, VM Guest, and Virtual Environments vCenter machine groups are available in Administration > Machines Manager > Machine Groups > All Machines .
Alerts	Configurations are available in Administration > Alerts .

Configuring the vSphere Client VCM Plug-In

The vSphere Client VCM Plug-In provides contextual access to VCM's change, compliance, and management functions, in addition to direct access to collected vCenter, VM Host, and VM Guest data.

When using the vSphere Client VCM Plug-In, the VM Host name in vCenter must match the VM Host name in VCM exactly.

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.

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 automatically with VCM. To unregister a previous version of the plug-in, see [Upgrading the vSphere Client VCM Plug-in](#).

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 you are using VMware vCenter 4 Server.
- Verify the VMware vSphere Client is installed.
- Verify the VMware Tools are 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 VCVPIInstaller.exe.
2. In the VCVI Plug-in Registration dialog box, configure these options.

Option	Description
Register	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.
Server URL	Type the http or https path, where <server> is your vSphere Client server.
Administrator User Name	Type the name of a user with Administrator privileges in the vSphere Client.
Administrator Password	Type the associated password.
URL to vSphereClientVCMPlugin.xml	Type the http path, where <VCMserver> is the name or IP address for the VCM Collector. The xml file is located in \VMware\VCM \WebConsole\L1033\VCVPAnon\Xml\vSphereClientVCMPlugin.xml

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 and select the **Automatically log in using this role** check box.
6. Start the vSphere Client.
7. 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 144.

Configuring the vSphere Client VCM Plug-In Integration Settings

You must configure integration settings in VCM for vSphere Client VCM Plug-In users. The settings enable users to view the VCM reports.

Procedure

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

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

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 145](#).

Manage Machines from the vSphere Client

vSphere Client-managed machines are available in the vSphere Client VCM Plug-In when they are licensed and have the VCM Agent installed. Using the vSphere Client VCM Plug-In, you can continue to manage the machines. 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 ["Licensing Windows Machines" on page 75](#) and ["Licensing UNIX/Linux Machines" on page 98](#).
- Install the Agent on the virtual machine. See ["Installing the VCM Windows Agent on your Windows Machines" on page 77](#) and ["Installing the Agent on UNIX/Linux Machines" on page 99](#).

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.

Upgrade the vSphere Client VCM Plug-In

Upgrading the plug-in is necessary only if you have a vSphere Client VCM Plug-In version 5.3 or earlier, or if the URL to the VCM instance has changed.

Prerequisites

Unregister the previous version of the vSphere Client VCM Plug-In. See ["Unregister the Previous Version of the vSphere Client VCM Plug-In" on page 146](#).

Procedure

1. Upgrade VCM.

What to do next

Register the new vSphere Client VCM Plug-In by following the instructions in ["Register the vSphere Client VCM Plug-In" on page 143](#).

Unregister the Previous Version of the vSphere Client VCM Plug-In

You must unregister a previous version of the vSphere Client VCM Plug-In before you can upgrade to the new version provided when you upgraded VCM. The upgrade to VCM removes files for the previous plug-in and installs the new plug-in files in new locations and with new names, but it does not register the new plug-in with the vSphere Client.

Procedure

1. Go to `https://vCenter machine name/mob/?moid=ExtensionManager`.
vCenter machine name represents the name of your vCenter Server 4.0 instance.
2. In the **Methods** area, click the **UnregisterExtension** link.
3. Type the string value for **extensionKey**:
`com.CM.VirtualCenterCompliancePlugIn`
4. Click **Invoke Method**.
The plug-in is unregistered.

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.

Getting Started with VCM Remote

Getting Started with VCM Remote

Many workstations come and go from the network. This transient behavior is especially true of mobile workstations, such as laptops. From a mobile workstation, you can connect by dialing in, connect from a client site via a Virtual Private Network (VPN), or connect from an alternate location via a DSL line or cable modem. In these scenarios, these devices may connect over networks with variable available bandwidth such as:

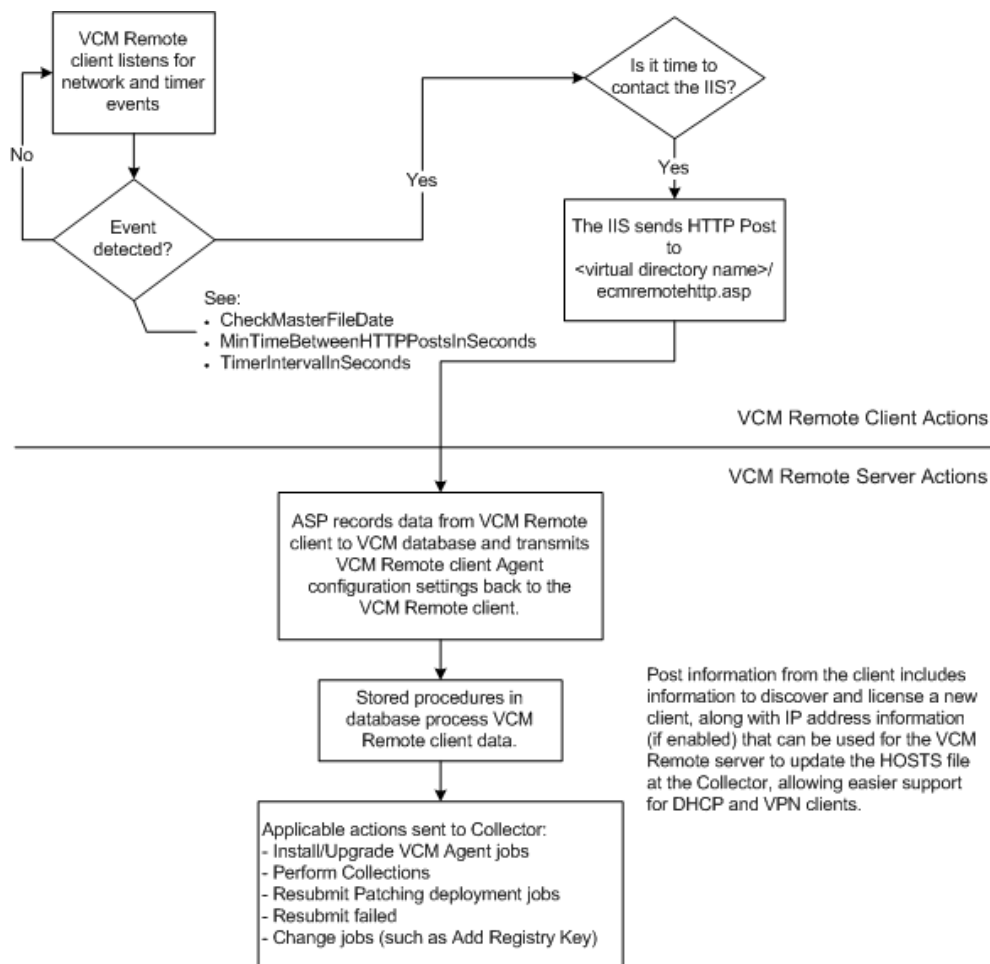
- **Broadband:** DSL and cable connections can be 156Kb to more than 1Mb
- **Dialup:** A dial-up connection could be 56Kb or less
- **LAN:** A local area connection to the network equal to or greater than 1Mb. A VPN connection may be at LAN speeds but connected over the Internet

Machines may not be, and often are not, on the network when the Collector initiates a collection. Consider patch management. You need up-to-date information to perform the Assessments to ensure your machines and production networks are protected from the latest vulnerability. Relying on data from mobile workstations can be risky.

The VCM Remote client provides support for mobile Windows workstations. VCM Remote is a service-based agent that “announces” itself when it is online. The agent sends this announcement over HTTP to a server-side component residing on the VCM Internet Information Services (IIS) server. Based on user-defined settings on the IIS server, the Collector creates immediate requests, such as collections, for the machine that just came online. The server-side processing is smart enough to batch work at periodic intervals. This technique avoids the problem of having 15,000 clients come online within ten minutes of one another and creating 15,000 individual requests.

Workflow Diagram

The basic sequence of actions is represented in the following diagram.



Before Collecting Remote Data

Begin using VCM Remote by following the steps outlined below. For more information, click any step to jump to the related section.

[Step 1: Installing VCM Remote Client](#)

[Step 2: Making VCM Aware of VCM Remote Clients](#)

[Step 3: Configuring the VCM Remote Settings](#)

[Step 3a: Creating Custom Collection Filter Sets](#)

[Step 3b: Specifying Custom Filter Sets in the VCM Remote Settings](#)

[Step 4: Performing a Collection Using VCM Remote](#)

[Step 5: Reviewing the VCM Remote Collection Results](#)

Installing the VCM Remote Client

Installing VCM Remote involves installation of both the VCM Remote server and VCM Remote Client. The VCM Remote server was installed when the VCM Installation Manager was run. The VCM Remote Client must be installed separately.

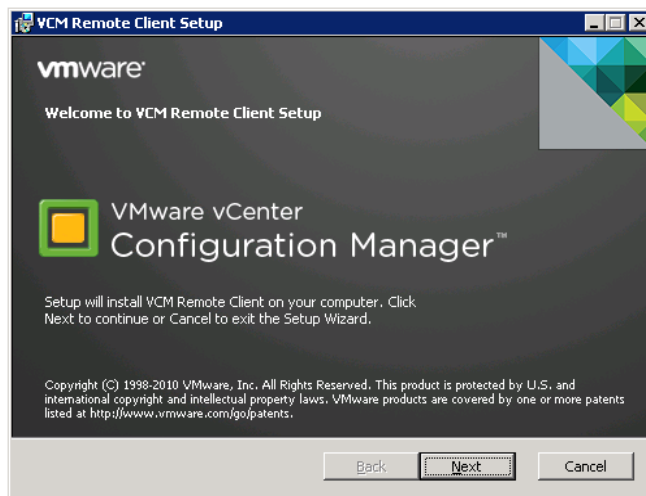
The VCM Remote Client can be installed using any of several methods, including a manual installation (provided below), ["Installing the Remote Client using a Command Line" on page 153](#), or ["Installing the Remote Client using Windows Remote Commands" on page 154](#). All the methods are described in this section.

Additionally, communication between the Collector and the Remote Client is secured using Transport Layer Security (TLS) certificates. You can use the Enterprise certificate generated by VCM or you can use an existing Enterprise certificate. The steps below include copying the VCM generated certificate to the Remote Client; however, if you have an existing Enterprise certificate in the certificate store with a known trust relationship with the Collector, you do not need to perform those steps. By default, the installation of a Windows VCM base agent in HTTP mode adds the Collector's Enterprise Certificate to the certificate store of the client system, and this certificate can also be used by the VCM Remote client.

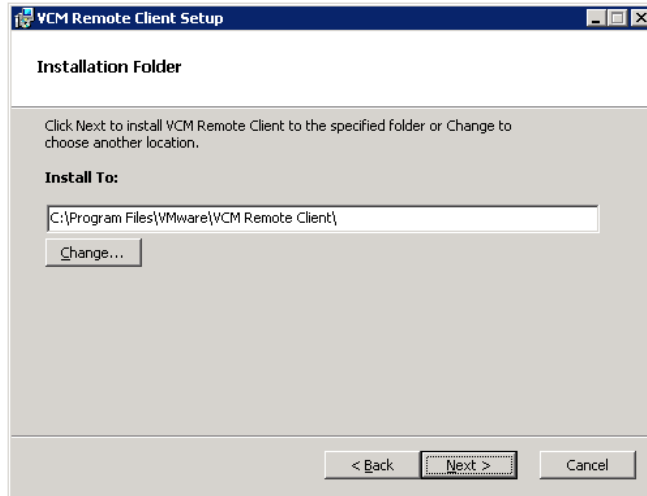
NOTE The VCM Remote Client can be deployed to multiple machines in your enterprise using VCM's Remote Command feature. See ["Installing the Remote Client using Windows Remote Commands" on page 154](#) for more information.

Installing the Remote Client manually

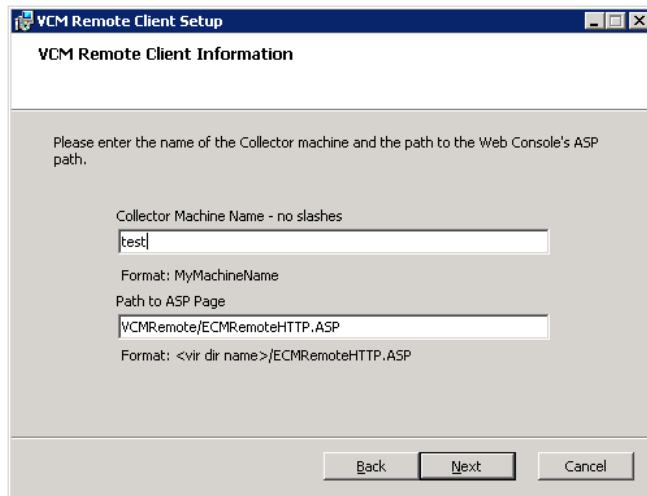
1. Create a folder on the target mobile workstation and copy the following files from the Collector to the target folder:
 - **CM Remote Client.msi:** Located on the Collector at [install path] \VMware\VCM\AgentFiles.
 - **CM_Enterprise_Certificate_xxx.pem:** Located on the Collector at [install path] \VMware\VCM\CollectorData.
2. Double click the **CM Remote Client.msi** copied to the mobile workstation. The **VCM Remote Client Setup** installation wizard appears.



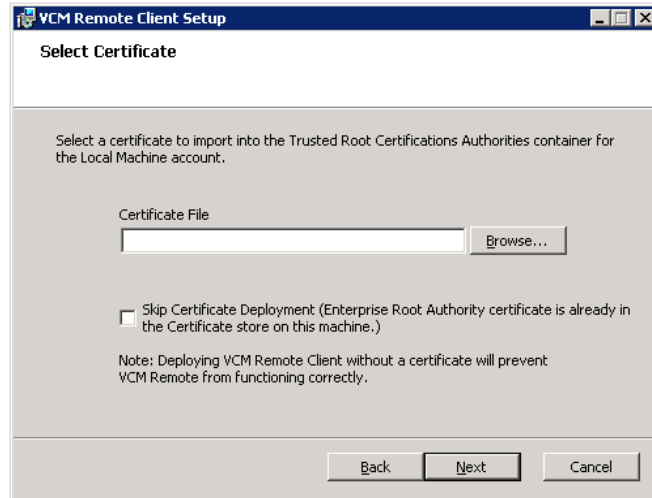
3. Click **Next**. The **Installation Folder** page appears.



4. Accept the default installation location, or click **Change** to enter a different location. Click **Next**.



5. Type the name of the Collector machine and the path to the Web Console's ASP path as follows:
 - **Collector Machine Name:** Type the name of the machine on which the VCM Collector and Microsoft IIS are installed.
 - **Path to ASP Page:** This path was created in the IIS default web site by the VCM Remote server installation. The <virtual directory name> must match the virtual directory name entered when you installed the server component.
6. Click **Next**. The **Select Certificate** page appears.



7. Configure or select one of the following certificate options:
 - If you copied the VCM-generated Enterprise certificate to the CM Remote Client, to locate the certificate (.pem), click **Browse**.
 - If you are using an existing Enterprise certificate in the client certificate store, select **Skip Certificate Deployment**.

IMPORTANT Do not select **Skip Certificate File Import** unless you are certain the Enterprise certificate exists in the client certificate store. If you select this option, the Remote Client will use the Enterprise certificate in the store. If the certificate does not exist in the store, any communication between the client and the Collector will fail.

8. Click **Next**. The **Ready to install CM Remote Client** page appears.
9. Click **Install** to begin the installation.
10. When the installation is completed, click **Finish**.

NOTE After the Remote Client is installed, the first time the Remote Client connects with the Collector, 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.

Installing the Remote Client using a Command Line

The VCM Remote Client can be installed using any of several methods, including ["Installing the VCM Remote Client" on page 150](#), Installing the Remote Client using a Command Line (provided below), or ["Installing the Remote Client using Windows Remote Commands" on page 154](#).

1. On the Collector, navigate to the path where you installed the software, which by default is `C:\Program Files (x86)\VMware\VCM\AgentFiles`.
2. Copy `CM Remote Client.msi` to the target mobile workstation.
3. On the Collector, navigate to the path where you installed the software, which by default is `C:\Program Files (x86)\VMware\VCM\CollectorData`.
4. Copy the certificate file (.pem) to the target mobile workstation.
5. On the workstation, open a command prompt and type the following command:

```
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" /! *v "[path\]filename.log"
```

NOTE If the names and paths contain spaces, you must use double quotation marks. See the example above.

Where:

/qn: No error messages are displayed.

[path]\cm remote client.msi: Specify the path to the CM Remote Client.msi on the target machine.

COLLECTOR=YourCollectorName: Replace <YourCollectorName> with the name of your VCM Collector.

PATHTOASP=VCMRemote/ecmremotehttp.asp: If necessary, replace VCMRemote (the default virtual directory name) with the name of the IIS Default Web Site virtual directory containing ecmremotehttp.asp.

INSTALLDIR:c:\Program Files (x86)\VCM\CM Remote Client: Specify the path where you want the Remote client files installed on the target machine. The directory will be created by the command.

CERTIFICATE_FILE=[path]\YourEnterpriseCertificateName.pem: Specify the path and the certificate name on the target machine.

NOTE If you are using an existing Enterprise certificate in the client certificate store, you can use `SKIP_CERTIFICATE_FILE=1` instead of `CERTIFICATE_FILE=YourEnterpriseCertificateName.pem`.

IMPORTANT Do not use this option unless you are certain the Enterprise certificate exists in the client certificate store. If you specify `SKIP_CERTIFICATE_FILE=1`, the Remote Client will use the Enterprise certificate in the store. If the certificate does not exist in the store, any communication between the client and the Collector will fail.

! *v [path]\filename.log: Any error messages are added to the log file. If a path is specified, the log file is saved to that location. If the path is not specified, the log file is saved in the directory from which the msiexec.exe was run. The log files are a useful troubleshooting tool.

Installing the Remote Client using Windows Remote Commands

The VCM Remote Client can be installed using any of several methods, including a ["Installing the VCM Remote Client" on page 150](#) (a manual installation), ["Installing the Remote Client using a Command Line" on page 153](#), or Installing the Remote Client using the Window Remote Commands (provided below).

Before you can run the Remote Command, you must have the VCM Agent installed on the target Remote machine.

NOTE Using this option, the VCM Remote Client can be deployed to multiple machines in your enterprise.

1. On your VCM Collector, copy ... \VMware\ VCM\AgentFiles\CM Remote Client.msi to... \VMware\ VCM\WebConsole\L1033\Files\Remote_Command_Files.
2. On your VCM Collector, copy ... \VMware\ VCM\CollectorData\<YourEnterpriseCertificate>.pem to the same location specified in step 1 (to... \VMware\ VCM\WebConsole\L1033\Files\Remote_Command_Files).
3. In VCM, select **Console > Windows Remote Commands**.
4. Click **Add**. The **Remote Commands** wizard appears.
5. Type the **Name** and **Description** of the your new command.
6. Click **Next**. The **Remote Command** page appears.
7. In the **Type** drop-down list, select VBScript.
8. In **Command Text** text box, copy and paste the following Script. Modify the script as specified in the comments of the script.

NOTE The script installs the 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 running the script.

```

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

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

sCertFile = "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

```

9. Select the **Certain file(s) are required to be on the target machine for this remote command** check box.
10. Click **Next**. The **Files** page appears.
11. Select the `CM Remote Client.msi` file and the `.pem` file then move them to the right box
12. Click **Next**. When you are ready to save the new remote command, click **Finish**. The command is saved and added to the **Windows Remote Commands** list.
13. To run the new remote command to install VCM Remote Client, select your new remote installation remote command and click **Run**. The **Windows** page of the **Remote Commands** wizard appears.
14. Select the machines on which you are installing VCM Remote.

NOTE The VCM Agent must already be installed on the target machines.

15. Click **Next**. The **Schedule** page appears. Select one of the following options:

- **Run Action now:** This option immediately installs VCM Remote Client on the target machines.
- **Schedule the Action to run later:** This option allows you to specify the **Time** and **Date** for the installation.

NOTE The job appears in the Instant Collection job history queue as **Install CM Remote Client**.

16. Click **Next**. When you are ready to proceed, click **Finish**.

Making VCM Aware of VCM Remote Clients

After the VCM Remote Client is installed, the client contacts the collector when connected to the network.

The default VCM Remote setup enables VCM Remote to automatically contact the Collector, auto-license the machine, install or upgrade the base VCM Windows Agent, and determine whether it should submit a VCM collection job for that machine. In addition, VCM Remote resubmits failed deployment jobs if you are using other VCM components for your patch management processing.

This process is automated based on VCM Remote Settings and other than configuring the settings, requires no operator interaction.

Configuring VCM Remote Settings

Once the VCM Remote client and server components have been installed successfully, you need to collect from, or push patches to, the mobile Windows workstations. You must configure the following:

- Create custom Collection filter sets to be used when a mobile workstation connects using Dial-up, Broadband, or LAN. We recommend a different Filter Set for each connection type. See ["Creating Custom Collection Filter Sets" on page 158](#) for more information.
- In the VCM Remote settings, enter the names of the filter sets to be used for each type of connection. See ["Specifying Custom Filter Sets in the VCM Remote Settings" on page 158](#) for more information.

Creating Custom Collection Filter Sets

If you have not created any Collection filter sets, you can specify the default set. However, this is an all-encompassing collection that would likely not be able to complete over a dial-up connection. Therefore, you should create filter sets customized to the type of connection that might be used by the mobile workstations: Dial-up, Broadband, or LAN. For example, the dial-up set might be limited to only a few high-importance items and would not include the File System Uploads or Emergency Repair Disk data classes.

1. In VCM, select **Administration > Collection Filters > Filter Sets**.
2. Select **Add Filter Set**.
3. Construct a filter set appropriate for the connection type. Use the Help available in the Filter Set Wizard to configure the filter set.

Specifying Custom Filter Sets in the VCM Remote Settings

For a Collection of the client machine to take place, a Collection Filter Set must be created and its name entered into VCM. You can, of course, enter Default for the automatically-created default set. The same or different Filter Set names can be assigned to each of the three connection types: Broadband, Dialup, and LAN. For instance, if the connection speed is only that of Dialup, you might want to create a smaller Filter Set. If a connection type does not have a Filter Set name assigned, no Collection will be initiated when the connection is at that speed.

1. In VCM, click **Administration > Settings > General Settings > VCM Remote**. The default selection for the Broadband, Dialup, and LAN collection filter settings that VCM Remote will use for connections require you to edit the setting and specify a collection filter.
2. To specify the name of the filter set for each connection, select the setting that you want to change, then click **Edit Setting**. The **General Settings Edit Setting** wizard appears.
3. In the drop-down list, select the name of the filter set to use for the connection. Click **Next**.
4. Confirm that you want to change the name as specified, then click **Finish**.

Performing a Collection Using VCM Remote

After VCM Remote is installed, it will contact the Collector, auto-license the machine, install or upgrade the VCM Windows Agent, and determine whether it should submit a VCM Collection job for that machine.

Exploring VCM Remote Collection Results

Collection results gathered by VCM Remote are displayed in the same way as other data collected from your VCM-managed Windows machines. Refer to ["Exploring Windows Collection Results" on page 84](#) for more information.

In addition to the general Windows data collected using the VCM Remote Client, you should be aware of the data displayed in the **Administration > Job Manager > History > VCM Remote** node. Refer to the information displayed in the node to verify communication between VCM and the VCM Remote Clients running on your Windows machines. Refer to the online Help for more details on the unique capabilities and features of the VCM Remote Client.

Getting Started with VCM Patching

VCM Patching for Windows and UNIX/Linux

VCM Patching is the VCM patch assessment, deployment, and verification module, which ensures continuous enterprise security through proactive compliance of the IT infrastructure. VCM Patching ensures that your machines have the latest security patches and other software downloads. You can evaluate each licensed machine in your network for the current Microsoft Security Bulletins or supported UNIX/Linux Vendor Bulletins and deploy the recommended patches to each machine.

Before you patch Windows 2008 servers and Windows 7 machines, make sure the Windows Update service is running (set to something other than Disabled) or the patch deployment will fail.

IMPORTANT For VCM Patching to correctly assess Windows systems, you must have a current collection of File System, Hotfixes, 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 Hotfixes data to determine which patches are already installed on which machines. VCM Patching for UNIX/Linux collects the data when you perform an assessment.

VCM Patching for Windows

VCM Patching for Windows provides several features that help you deploy patches to remediate Windows machines:

- **Bulletins:** The Bulletins section contains a list of Microsoft bulletins available to VCM Patching. These bulletins can be listed by bulletin and by affected product.
- **Assessment Templates:** An Assessment Template contains one or more bulletins and, when run, dynamically shows which machines require the patches described by each bulletin. You can create templates easily in the Bulletin section by selecting bulletins or product names.
- **Imported Templates:** An imported template is a user-defined template that associates machines with patches for deployment of those patches to the selected machines. Imported templates are available for Windows and UNIX/Linux machines.
- **VCM Patching Administration:** Use VCM Patching Administration to configure patch deployment, proxy server settings, and the conditions under which you want to receive an e-mail alert. You can select the machines that VCM Patching will manage, add and update your VCM Patching license, and view the status of jobs that are currently running, scheduled, and completed.

VCM Patching for UNIX/Linux

VCM Patching for UNIX/Linux provides several features that help you deploy patches to remediate UNIX/Linux machines:

- **Bulletins:** The Bulletins section contains a list of vendor bulletins available to VCM Patching.
- **Assessment Templates:** An Assessment Template contains one or more bulletins that dynamically show which machines require the patches described by each bulletin. You can create templates easily in the Bulletin section by selecting bulletins or product names.
- **Imported Templates** An imported template is a user-defined template associates machines with patches for deployment of those patches to the selected machines. Imported templates are available for Windows and UNIX/Linux machines.
- **Assessment Results:** The Assessment Results node displays the results of your assessment for all bulletins or for specific bulletins.
- **VCM Patching Administration:** Use VCM Patching Administration to configure patch deployment, proxy server settings, and the conditions under which you want to receive an e-mail alert. You can select the machines that VCM Patching will manage, add and update your VCM Patching license, and view the status of jobs that are currently running, scheduled, and completed.

Minimum System Requirements

VCM Patching must be installed on the same machine as the VCM application software, because it depends on the VCM database. VCM data must have been collected, otherwise the VCM Patching does not have the necessary information. Although you should collect all data types, as a minimum, you must have a current collection of Hotfixes, File System, Registry and Services data.

About UNIX Patch Assessment and Deployment

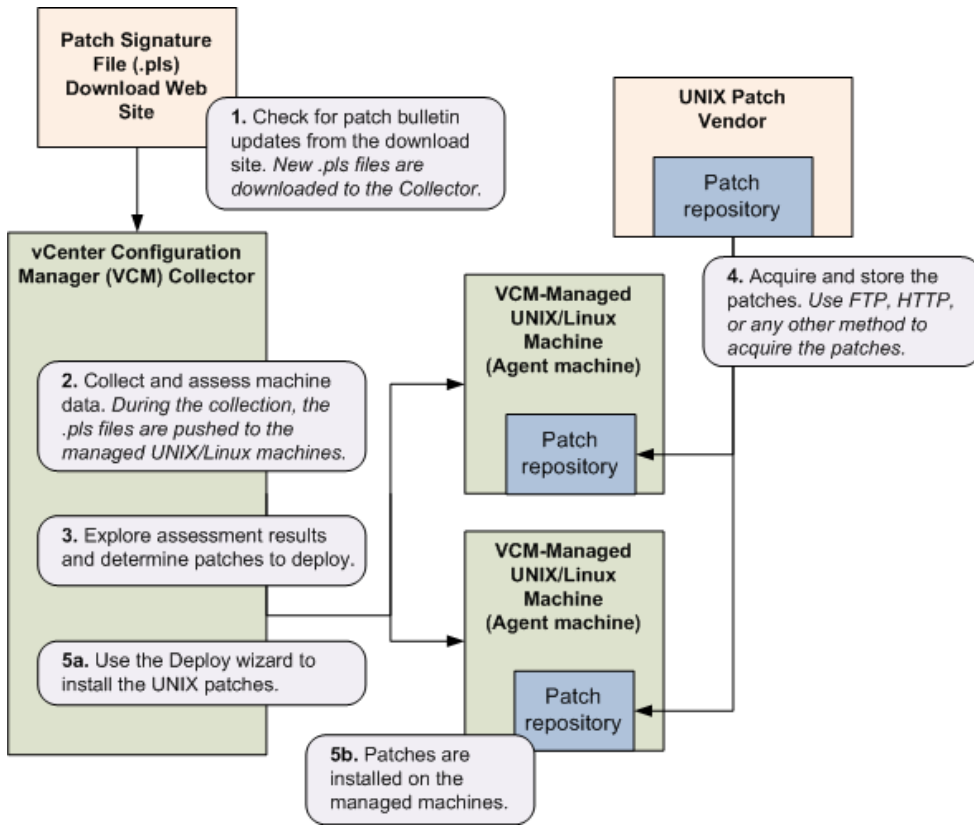
UNIX Patch Assessment and Deployment is a VCM Patching feature. When UNIX Patch Assessment is licensed, you can assess UNIX/Linux machines to determine their patch status.

Verify that your UNIX and Linux machines and operating systems are supported for patch deployment. See the *VCM Hardware and Software Requirements Guide*.

VCM Patching for UNIX/Linux machine patching involves the following process.

Before using VCM Patching to install the patches UNIX/Linux machines, you must always collect assessment data from those machines.

NOTE Assessments of UNIX and Linux-based machines operate differently from Windows assessments. UNIX and Linux assessments require new data to be collected, while Windows assessments are performed against previously collected data.



Getting Started with VCM Patching

You can use VCM Patching to assess the state of managed Windows and UNIX/Linux machines and deploy patches to those machines.

[Getting Started with VCM Patching for Windows Machines](#)

[Getting Started with VCM Patching for UNIX/Linux Machines](#)

For information about other VCM Patching functionality, such as Windows Patch Staging or creating filters for UNIX Patch Assessment results, see the online Help.

Getting Started with VCM Patching for Windows Machines

You can use VCM Patching to determine the patch status of Windows machines and deploy patches to those machines.

[Step 1: Check for updates to bulletins.](#)

[Step 2: Perform a collection using the appropriate filters.](#)

[Step 3: Assess Windows machines.](#)

[Step 4: Explore the results.](#)

[Step 5: Deploy the patches.](#)

[Step 6: Perform another collection.](#)

[Step 7: Run another assessment.](#)

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. To view bulletins, select **Patching > Windows > Bulletins**.
2. To obtain a comprehensive view of all released bulletins, click **By Bulletin**.
3. To find a bulletin for an installed software product, click **By Affected Product**.
4. In the By Bulletin or By Affected Product views, select **Check for Update**.
5. If updates exist, download the updates.

VCM displays a dialog box communicating the status of your request. Follow the prompts to update your bulletins, force an update to the bulletins, or cancel the request.

6. Click **Finish** to submit the download job to the pending job queue.

When the job finishes, the content is available in VCM.

Collect Data from Windows Machines by Using the VCM Patching Filter Sets

VCM Patching requires that you collect current information about the File System, Hotfixes, Registry, and Services Windows data types.

1. On the toolbar, click **Collect**.
2. Select the Windows machines from which to collect data.
3. Mark **Select a Collection Filter Set to apply to these machines** and click **Next**.
4. Select the **Patching - Windows Security Bulletins** filter set and click **Next**.

The Patching - Windows Security Bulletins filter set for Windows machines gathers information for all bulletins. Bulletin filter sets are available by month, and you can select any of the monthly filter sets to filter the bulletins released in that 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.

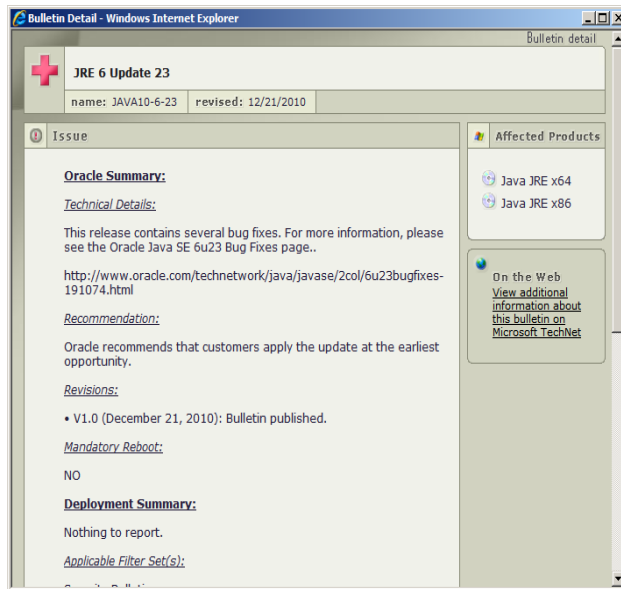
When run, the template checks data collected from machines to confirm whether the patches referenced by the bulletins must be installed on those machines. For example, a template might contain all bulletins related to Internet Explorer 7 to ensure that all of the instances installed have the latest security 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 in several ways: based on bulletins, based on 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.

Procedure

1. Review the collected patching data and determine which machines must be patched.
2. Select **Patching > Windows > Bulletins > By Bulletin** and select a bulletin.
3. Click **Details** and read the technical details about the bulletin, including the affected products and vendor recommendations.
4. Read the Deployment Summary to identify any issues that might interfere with the distribution of the bulletin.
5. Select **On the Web** to link to vendor information about the bulletin.



6. Review all of the bulletins to include in the assessment template.
7. To create a template that includes all of the bulletins for patches to deploy, select all of the relevant bulletins and click **Create Template**.
8. Verify that the bulletins are automatically selected, and click **Finish** to create the template.
9. On the VCM toolbar, verify that the correct Machine Group is selected.
10. Select **Patching > Windows > Assessment Templates**.
11. In the node tree, select the template to run and select **Assess**.
12. When the assessment completes, indicated by the Assessment Results pop-up dialog box, click the **Refresh** button on the toolbar and view the assessment results in the data grid.

Explore VCM Patching Windows Assessment Results

Data for the assessed Windows machines appears in the data grid for the assessment template. The patch status is indicated for each machine.

Prerequisite

You must have run an assessment template.

Procedure

1. In the Assessment Templates node tree, select the template and view the results in the data grid.
2. View the Patch Status column to determine the state of each machine for the patches listed.
3. If the assessment results provide multiple pages of data, click the **Patch Status** column heading and drag it up to **Column Grouping**.
4. In the Column Grouping view, expand the **Not Patched** status to view all of the machines that are not patched.
5. To display the graphical representation of the patch assessment status, in the template data grid view,

select **Enable/Disable Summary** to enable the Summary view, and click the template node again.

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 drill down directly to the affected machines.

Deploy Patches to Windows Machines

You can deploy patches on Windows machines that are managed by VCM Patching. These machines appear in Patching > VCM Patching **Administration** > **Windows** > **Machines Manager** > **Licensed Machines**.

Before you patch Windows 2008 servers and Windows 7 machines, make sure the Windows Update service is running (set to something other than Disabled) or the patch deployment will fail.

If you have VCM Service Desk Integration licensed, the Service Desk Connector dialog box appears prior to the VCM Patching Deploy Patches wizard.

If you licensed and activated VCM Service Desk Integration, the deployment job must be approved through VCM Orchestrator before it can run.

Procedure

1. In the Patching > **Windows** > **Assessment Templates** node, select the template used for the assessment.
2. Make sure the data grid view is visible so that you can view the machines and bulletins.
3. Locate the rows that display the StatusNotPatched status.

To easily identify the machines that must be patched, group the Patch Status column.

4. Highlight the row containing the machine to be patched and select **Deploy**.
5. (Optional) Although the Deploy wizard automatically selects the machine and the patch to be deployed, you can select additional machine and patch combinations to include.
6. Select the machines and patches to deploy and click **Next**.

The Deploy wizard attempts to detect the patch by first checking the Collector, and if found, uses the downloaded patch. If the patches are not found on the Collector, 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.

7. Click **Next**.
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 installation, and click **Next**.
10. On the Patch Staging and Deployment Schedule page, select to copy the patches to the agent 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 automatically runs a delta collection of the VCM Patching Security Bulletins filter set to update the assessment information.
15. To view the status of the deployment job, select **Patching > VCM Patching Administration > Windows > Job Manager > Running** .
16. If you scheduled the job to run later, to view the status of the scheduled deployment, select **Patching > VCM Patching Administration > Windows > Job Manager > Scheduled > Deployments**.
17. 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.

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.

For more information about scheduled patch deployments for Windows machines, see the online Help.

Getting Started with VCM Patching for UNIX and Linux Machines

Welcome to VCM Patching for UNIX and Linux. When licensed, you can use VCM Patching for UNIX and Linux to determine the patch status of UNIX and Linux machines and deploy patches to those machines.

NOTE Assessments of UNIX and Linux-based machines operate differently from Windows assessments. UNIX and Linux assessments require new data to be collected, while Windows assessments are performed against previously collected data.

UNIX and Linux patching change actions are saved in the VCM change log in Console > 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 machines.
- Verify that VCM Patching for UNIX is licensed on the UNIX or Linux machine.
- Verify that your UNIX and Linux machines and operating systems are supported for patch deployment. See the *VCM Hardware and Software Requirements Guide*.

Procedure

[Step 1: Check for updates to bulletins.](#)

[Step 2: Collect assessment data.](#)

[Step 3: Explore the results, and acquire and store the patches.](#)

[Step 4: Install the patches.](#)

Check for Updates to Bulletins

Before you assess the patching state of UNIX and Linux machines, you must check for updates to VCM Patching bulletins.

Prerequisite

Place patch bulletin files on the local machine to load the bulletin updates from a local file.

Procedure

1. Select **Patching > UNIX/Linux Platform > Bulletins > By Bulletin**.

2. Select **Check for Update**.

You can check for updates on the Internet or load the updates from patch bulletin files on the local machine.

3. Select **Check for Updates via the Internet** and click **Next**.

If updates are found, they are downloaded to the local machine.

Collect Assessment Data from UNIX/Linux Machines

You can collect UNIX/Linux assessment data using bulletins, an assessment template, or the Collect wizard.

- **Bulletins:** Collect using the Patch Assessment collection filter. Because UNIX/Linux assessments are VCM collections, you can schedule these assessments.
- **Assessment template:** Collect using a template that filters the patch assessment results.
- **Collect wizard:** Collect using the Patch Assessment Data Class filter.

NOTE Assessments of UNIX and Linux-based machines operate differently from Windows assessments. UNIX and Linux assessments require new data to be collected, while Windows assessments are performed against previously collected data.

Assessments of UNIX/Linux machines are run against the patches known by VMware at the time the assessment is performed.

Patch assessments of UNIX/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.

For a patch assessment that did not return any results, see the troubleshooting section.

If machine data has not been collected, the assessment results might not appear and the machine will not be available for deployment. If this situation occurs, a patch-machine mismatch status will result. You can display or hide the patch-machine mismatch status in **Patching > VCM Patching Administration > UNIX > Settings > Bulletin and Update**.

Prerequisites

- Assessments must have finished successfully.
- The patch signature files (.pls files) must reside on the Collector.

The .pls files determine whether required patches are installed on the machine. By default, VCM Patching downloads the .pls files automatically every 4 hours.

Patch files appear in **Console > 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 pushed from the Collector to the machine. A delay might

- The VCM Agent must be installed on the machine.
- The machine must be licensed for VCM Patching.
- If you choose **Filters** in the following procedure, you must already have pre-configured Filters.

The following procedure runs the assessment using patch bulletins.

Procedure

1. Select the All UNIX Machines machine group.
2. Select **Patching > UNIX/Linux Platform > Bulletins > By Bulletin**.
3. Select **Assess**.
4. In the UNIX Patch Assessment wizard, select **Default Filter** or **Filters**.
If you selected **Filters**, select a specific filter.
5. Click **Next** and **Finish** to begin the assessment on all machines in the selected machine group.
6. Click the **Jobs** button on the toolbar 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. The results are reported in the Assessment Results node.

7. Select **UNIX/Linux Platform > Assessment Results > All Bulletins** and view the results.

Create UNIX/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. Select **Administration > Collection Filters > Filters**.
2. In the Collection Filters data grid, select **Add Filter**.
3. On the Name and Description page, name the filter and click **Next**.
4. On the Data Type page, select **UNIX/Linux**.
5. Select **Patch Assessment** and click **Next**.
6. On the **UNIX Patch Assessment Filters** page, to create a subset of the available bulletins, select **Include Bulletin(s) that match this criteria**.
7. Define the filter criteria using the available settings.
For example, you can create a filter where **Platform = Red Hat** and **Severity = Critical**.
8. Click **Next** and **Finish** to create the filter.
9. 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.


Use the new filter when you run an assessment.


Explore Assessment Results and Acquire the Patches


The Assessment Results data grid displays the UNIX/Linux machines that were assessed, the patch status for each machine, and details about the patches.


Procedure


1. Select **Patching > UNIX/Linux Platform > Assessment Results > All Bulletins** to display the patch status of all of the machines that were assessed.
2. To display the assessment results for a single bulletin, select **By Specific Bulletin** and select a bulletin in the center pane.
3. Review the patch status for each machine.


 **Patched:** The patch has been applied to the machine.


 **Patch-Machine Mismatch:** The patch OS version or hardware architecture does not match the machine.


 **Patch Not Needed:** The machine is up-to-date or the intended software product is not installed on the machine.

 **Not Patched:** The patch was not applied to the machine.

 **Error Occurred:** An unexpected condition occurred during the assessment of the machine. Additional information about the root cause of the exception can be determined by running the Debug Event Viewer at `C:\Program Files (x86)\VMware\VCM\Tools\ecmDebugEventViewer.exe`.

 **Signature Not Found:** The .pls patch file does not exist on the machine, and therefore the patch status cannot be determined.

 **Incorrect MD5:** The MD5 Hash generated from the patch signature (.pls) file, which contains the content and signature, does not match the expected value on the UNIX/Linux Agent. Be aware that MD5 is NOT validated against the vendor MD5 hash data.

 **Patch Status Unknown:** The patch status of the machine cannot be determined.

If machine data has not been collected, the assessment results might not appear and the machine will not be available for deployment. If this situation occurs, a patch-machine mismatch status will result. You can display or hide the patch-machine mismatch status in **Patching > VCM Patching Administration > 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 **Patching > VCM Patching Administration > 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 Patching > VCM Patching Administration > Machine Group Mapping > Local Patch Path.

Default Location for UNIX/Linux Patches

If you do not define an alternate location for the patches using Machine Group Mapping, the default location of `/tmp` is used. A temporary expansion of the patches occurs in the `/tmp` directory.

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 User-created Assessment Template, Imported Template, or Assessment Results for All Bulletins.

Prerequisites

- Verify that your UNIX and Linux machines and operating systems are supported for patch deployment. See the *VCM Hardware and Software Requirements Guide*.
- VCM Patching for UNIX is licensed on the machines.
- Patch assessments have run successfully.
- Patches are available locally to the machine.
- Prerequisites are complete.

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. 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. If you need to specify commands to deploy the patches, on the Command Line Options page, specify the options to use.
8. 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.

UNIX and Linux patching change actions are saved in the VCM change log in Console > 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.

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 pre-install 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 post-install script (remote command) if specified.
- Assesses whether the patch was installed on the VCM-managed machine.

The pre-install and post-install 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. However, if you choose to deploy a patch using a user-created remote command, be aware that 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.

Real-time assessment reports allow you to generate SQL reports for machines assessed against bulletins and affected software products. The patch deployment history report allow you to report on the history of patch deployments using VCM Patching assessment results.

You can generate these 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 generating reports, you can:

- 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 to fine-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 you are retaining 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.

Getting Started with Operating System Provisioning

11

Operating system (OS) provisioning is the process of deploying operating system to physical or virtual machines. As part of the process, you can add newly provisioned machines to VCM.

About OS Provisioning

Some provisioned machines, for example Servers, are brought up quickly to meet expanding business needs. These machines may have limited use and lifespan, and may be re-provisioned for other purposes. Other machines are provisioned and distributed for long term use.

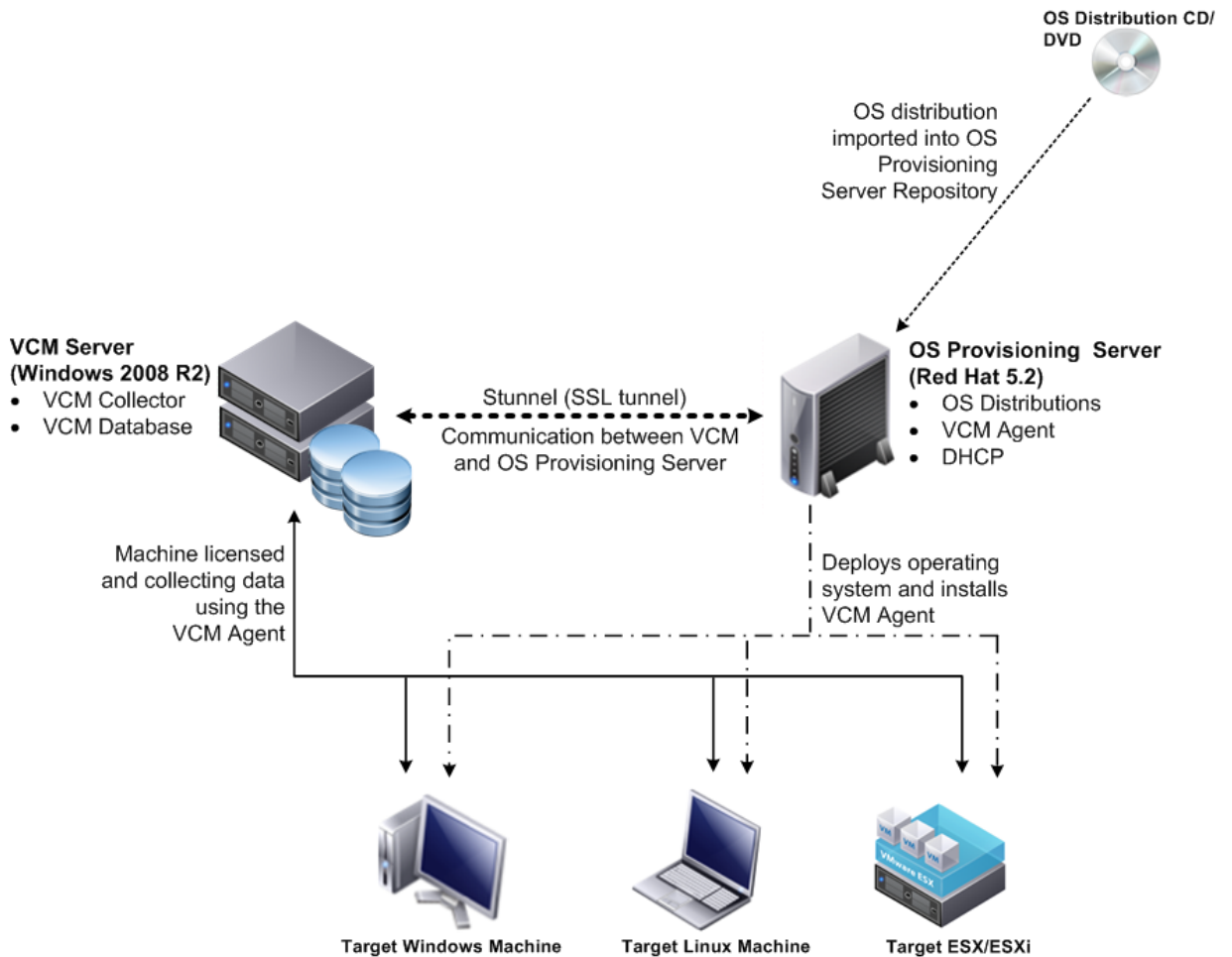
The provisioning process installs the operating system and the VCM Agent. When the machines are licensed, you can collect machine data, monitor the machines' state and status, and manage the security and compliance of the machines.

OS Provisioning Components

The OS provisioning components include the Collector, the OS Provisioning Server, and the target machines.

The OS Provisioning Server, when it is installed and configured for the network, serves as the engine for OS provisioning; however, the process of initiating provisioning actions is managed through the VCM Console.

The installation and configuration information for the OS Provisioning Server is provided in ["Installing the Operating System Provisioning Server" on page 23](#).



Provision Machines Workflow

The process of provisioning operating systems to target machines includes the following general tasks, underlying actions, and results:

1. Set the BIOS on the target machines to network boot.
2. Connect the machines to the network and turn them on. The OS Provisioning Server discovers the machines.
3. VCM collects the discovered machines from the OS Provisioning Server and displays them by MAC address in the Provisionable Machines data grid.
4. In VCM, you select the target machines, the operating system distribution, configure the OS-related settings, and send the command to the OS Provisioning Server to build an installation session for each selected machine.

5. Reboot the target machines. As each machine requests an IP address from the DHCP server and then requests a PXE boot, OS Provisioning Server checks the machine MAC address to determine if a machine has an installation session waiting. If an installation session is found, the download process begins.
6. The OS Distribution and the VCM Agent are downloaded to the target machines using TFTP.
7. When the installation is completed, the machines are licensed or available to license in VCM. If the machine is not licensed, you must license it to manage the machine.
8. As each machine is licensed, you can begin managing it in VCM.

Collect OS Distributions

OS Distributions are operating system images that have been imported into the OS Provisioning Server repository.

Prerequisites

- The operating system distributions are imported into the OS Provisioning Server repository. To import OS distributions, see ["Importing Distributions into the OS Provisioning Server Repository" on page 29](#).
- To collect OS Provisioning Server data, the OS Provisioning Integration Enabled setting must be configured with a value greater than 0. If the value is 0, VCM will never collect data from the OS Provisioning Server, even when manually requested. Select **Administration > Settings > OS Provisioning Settings > OS Provisioning Server** to verify or modify the setting.

Procedure

1. Select **Administration > Machines Manager > OS Provisioning > OS Distributions**.
2. Click **Refresh**.

The Refresh option starts a collection of data from the OS Provisioning Server. You can view the status of the collection in Jobs Manager. When the collection is completed, the data grid displays all available operating systems distributions.

Discover Provisionable Machines

Provisionable machines are machines the OS Provisioning Server has identified as eligible for provisioning. To be identified as provisionable, the machines' BIOS are set to network boot, and then the machines are connected to the network and booted. When they attempt to PXE boot they are identified by the OS Provisioning Server. When the list of provisionable machines is collected by VCM from the OS Provisioning Server, the machines are displayed in **Administration > Machines Manager > OS Provisioning > Provisionable Machines**.

Procedure

1. On target machines, configure the BIOS to network boot.
2. Start the machines on your provisioning network.
3. In VCM, select **Administration > Machines Manager > OS Provisioning > Provisionable Machines**.
4. If the target machines are not displayed, click **Refresh**.

The Refresh action starts a collection from the OS Provisioning Server. The data grid updates when the action is completed.

The data grid displays the provisionable machines, usually identified by MAC address.

Alternately, you can manually add machines to the list rather than use the OS Provisioning Server discovery process. To manually add machines, select **Administration > Machines Manager > OS Provisioning > Provisionable Machines** and click **Add**. Use the wizard to add machines to the data grid. You will need to know the machine MAC addresses. See the online Help for information about using the wizard.

Provision Machines

Provisioning machines installs the selected operating system on the selected 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

- Target machines have a minimum of 1 GB RAM and meet the minimum RAM requirements for the operating system.
- On target machines with multiple network cards, you must configure the primary network interface with a connection to the OS Provisioning Server deployment network. If you use a different network on the primary interface, the deployment process appears to start, but you may receive communication errors and the process ultimately fails.
- The operating system you are installing is compatible with the hardware of the target machines. For example, the operating system supports the drivers required by the hardware.
- OS Distributions are collected and displayed in **Administration > Machines Manager > OS Provisioning > OS Distributions**.
- Eligible machines are discovered or added manually, and displayed in **Administration > Machines Manager > OS Provisioning > Provisionable Machines**.

Procedure

1. Select **Administration > Machines Manager > OS Provisioning > Provisionable Machines**.
2. Select the machines.
3. Click **Provision**.
4. On the **Select Machines** page, add or remove machines and click **Next**.
5. On the **Select OS Distribution** page, select the operating system you are installing on the selected machines and click **Next**.
6. On the **Settings** page, configure the options and click **Next**.

The options on the Settings page vary depending on the OS Distribution you selected. To facilitate managing the machines in VCM, select **Use DHCP to determine IP Address** and **License these machines for VCM after deployment**. See the online Help for more information about the settings.

NOTE Static IP addressing is recommended when deploying ESX or ESXi hosts. If DHCP is used, the ESX or ESXi machine's host name will be set to `localhost` rather than the host name provided during deployment.

7. On the **IP Settings** page, configure the **HostName** and click **Next**.

If you did not select **Use DHCP to determine IP address** on the previous page, you will also need to configure the IP Address, Subnet, Default Gateway, and DNS. See the online Help for more information about the settings.

8. (Optional) (Available only for Windows, Red Hat, and SUSE Linux Enterprise Server) On the **Post-install Script** page, type a **Script Name** and the script, and then click **Next**.

See the online Help for more information about the options.

9. (Available only for Windows) On the **Disk Configuration** page, select one of the options and click **Next**.

You can either install the operating system without partitioning the disk, or you can create a partition and specify the size. See the online Help for more information about the options.

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 OS Provisioning Server. If a session is waiting on the OS Provisioning Server, the installation begins. If the session does not exist, then the machine remains provisionable and will not be provisioned until the session is created.

When the provisioning process begins, the machines are displayed in the **Administration > Machines Manager > OS Provisioning > Provisionable Machines** data grid. The machines are also displayed in the appropriate Available Machines or Licensed Machines data grid, with an OS provisioning status of **OS Provisioning Queued**.

When the provisioning is completed, the machines are added to the **Administration > Machines Manager > OS Provisioning > Provisioned Machines** data grid.

The machines are ready to use when the **Provisioned Machines** data grid, and the **Available Machines** or **Licensed Machines** data grid, display an OS provisioning status of **OS Provisioning Succeeded** or **OS Provisioning Overwritten**.

Post-Provisioning Action

Windows 2008 SP1, SP2, and R2, and Windows 7 machines require Internet access to complete the license activation. After provisioning these Windows machines, you must configure the machines on a public network with access to the Internet and manually complete the Windows activation on the provisioned machines.

Configure ESX and ESXi Machines

After using the OS Provisioning Server to install the ESX or ESXi operating system, you must configure the Agent Proxy settings and continue with a standard virtualization configuration.

Depending on whether you selected **License these machines...** during provisioning, your actions will vary.

- If licensed during OS provisioning, the machines are displayed in **Administration > Machines Manager > Licensed Machines > Licensed VM Hosts** data grid.
- If not licensed during OS provisioning, the machines are displayed in **Administration > Machines Manager > Available Machines > Available VM Hosts** data grid.

Change Agent Communication

The VCM Agent is installed by the OS Provisioning Server with default settings. After the machine is provisioned, you can change the settings or install a new Agent.

Windows Agents are installed with DCOM as the communication protocol. If you want to change the protocol, see the online Help for more information.

The UNIX/Linux Agents are installed with inetd or xinetd, as appropriate, with a default communication port of 26542. If you want to change any Agent settings, you must uninstall the Agent from the machine, and then reinstall with the settings you require. See ["Installing the Agent on UNIX/Linux Machines" on page 99](#) for more information about installing the Agent.

Working with Provisioned Machines

The OS Provisioning Server data is automatically collected and added to **Administration > Machines Manager > OS Provisioning > Provisioned Machines**.

After the machines are provisioned and licensed, either automatically or manually, they are managed machines. As managed machines, you can collect data, add necessary software, run assessments, and apply rules to maintain machine compliance in your environment.

Re-Provision Machines

Machines that have been provisioned once using operating system provisioning in VCM are eligible to be re-provisioned.

Re-provisioning overwrites the existing disk with a new operating system. All existing data is lost.

When machines are re-provisioned, you can change the machine name.

Prerequisite

The machine is listed in the **Administration > Machines Manager > OS Provisioning > Provisioned Machines** data grid.

The machine BIOS is set to network boot.

Procedure

1. Select **Administration > Machines Manager > OS Provisioning > Provisioned Machines**.
2. Select the machines.
3. Click **Re-provision**.
4. On the **Select Machines** page, add or remove machines and click **Next**.
5. On the **Select OS Distribution** page, select the operating system you are installing on the selected machines and click **Next**.
6. On the **Settings** page, configure the options and click **Next**.

The options on the Settings page vary depending on the OS Distribution you selected. To facilitate managing the machines in VCM, select **Use DHCP to determine IP Address** and **License these machines for VCM after deployment**. See the online Help for more information about the settings.

NOTE Static IP addressing is recommended when deploying ESX or ESXi hosts. If DHCP is used, the ESX or ESXi machine's host name will be set to `localhost` rather than the host name provided during deployment.

7. On the **IP Settings** page, configure the **HostName** and click **Next**.

If you did not select **Use DHCP to determine IP address** on the previous page, you will also need to configure the IP Address, Subnet, Default Gateway, and DNS. See the online Help for more information about the settings.

8. (Optional) (Available only for Windows, Red Hat, and SUSE Linux Enterprise Server) On the **Post-install Script** page, type a **Script Name** and the script, and then click **Next**. See the online Help for more information about the settings.

9. (Windows only) On the **Disk Configuration** page, select one of the options and click **Next**.

You can either install the operating system without partitioning the disk, or you can create a partition and specify the size. See the online Help for more information about the options.

10. If you are certain that the selected machines are those you want to re-provisioning, select the **Proceed with re-provisioning...** check box.

11. 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.

12. 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.

When the provisioning process begins, the machines are displayed in the **Administration > Machines Manager > OS Provisioning > Provisionable Machines** data grid. The machines are also displayed in the appropriate Available Machines or Licensed Machines data grid, with an OS provisioning status of **OS Provisioning Queued**.

When the provisioning is completed, the machines are added to the **Administration > Machines Manager > OS Provisioning > Provisioned Machines** data grid.

The machines are ready to use when the **Provisioned Machines** data grid, and the **Available Machines** or **Licensed Machines** data grid, display an OS provisioning status of **OS Provisioning Succeeded** or **OS Provisioning Overwritten**.

Post-Provisioning Action

Windows 2008 SP1, SP2, and R2, and Windows 7 machines require Internet access to complete the license activation. After provisioning these Windows machines, you must configure the machines on a public network with access to the Internet and manually complete the Windows activation on the provisioned machines.

Introduction to VCM Software Provisioning

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.

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 unattended 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.

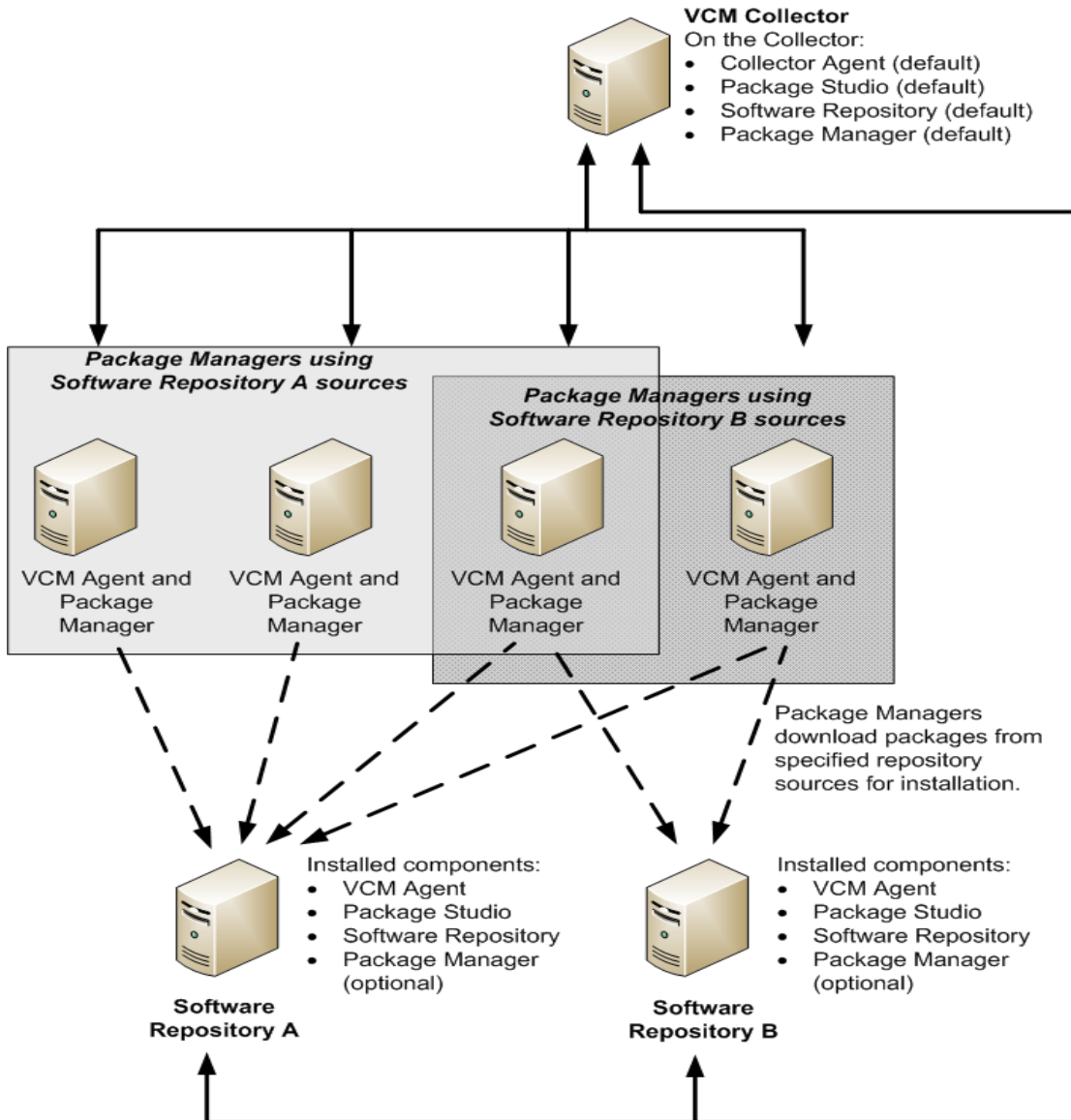


Figure 1. Software Provisioning Diagram

Installing the Software Provisioning Components

The software provisioning components should be installed on machines with these relationships:

NOTE By default, all the components are installed on the VCM Collector; however, it is recommended you install the Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio on a machine other than the Collector.

- **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 above 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.

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

- Target machine meets the supported hardware requirements, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.
- Access to the `Repository.msi`, which is available on the VMware website or in the vCenter Configuration Manager application files. The default location in the VCM application files is `C:\Program Files (x86)\VMware\VCMAgentFiles\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.
When the path is correct, 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\VCMAgentFiles\Tools\Repository` (on 32-bit machines) or `C:\Program Files (x86)\VMware\VCMAgentFiles\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 following command line syntax, you can run an unattended uninstall the software repository.

Prerequisites

- To uninstall the application, you must 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

The VMware vCenter Configuration Manager Package Studio and the repository must be installed on the same machine. The process installs the application files and specifies the repository to which Package Studio will publish packages.

Prerequisites

- Target machine meets the supported hardware requirements, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.
- Access to the PackageStudio.msi, which is available on the VMware website 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.
- (Recommended) Software Repository for Windows is installed. Installing the repository before installing Package Studio will reduce 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**.
7. On the Setup Complete page, click **Finish**.

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, select **Start > 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

- Target machine meets the supported hardware requirements, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.
- Access to the PackageStudio.msi, which is available on the VMware website 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`.
- (Recommended) Software Repository for Windows is installed. Installing the repository before installing Package Studio will reduce 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.
You can also run the `.msi` from a shared location.
3. On the target machine, run the `.msi` file using the following command line syntax.

```
msiexec /i [path]\PackageStudio.msi /qn /l*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, select **Start > 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. You can also run it from a shared location.
2. Run the `.msi` file using the following command line syntax:

```
msiexec /x [path]\PackageStudio.msi /l*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 is automatically installed on target machines when the 5.3 VCM Agent or later is installed.

On the target machine, the Package Manager 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. It is from this location that Package Manager upzips the files to the %TMP% directory and runs the configured installation.

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. It is from this location that 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 ["Installing the VCM Windows Agent on your Windows Machines" on page 77](#) for complete instructions. By default, the VCM Agent installation installs the agent extensions for provisioning and the Package Manager for Windows. This default action is based on the settings in **Administration > Settings > General Settings > Installer**.

Prerequisites

- Target machine meets the supported hardware requirements, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.

Verifying the Installation of the Agent Extensions for Provisioning

If you do not know if the machines are ready to use provisioning or not, you can verify the version of the Agent Extensions for Provisioning. The Agent Extensions for Provisioning include the Package Manager.

- Select **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines**.
- In the data grid, locate the machines on which you are verifying the existence of the necessary Agent Extensions, and then 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 unattended or quietly using command line options, response files, or other similar methods.

Creating Packages

A software package provides the files and metadata necessary to install and remove programs. One of the most useful features of a package is the metadata regarding dependencies, conflicts, and other relationships that are not represented by software installation files. This metadata is used to determine if the necessary dependencies are in place so that an installation is successful, and if not, what is necessary to make the installation successful. This use of metadata is similar to rpm on Linux.

Packages support commercial and custom software that may be installed using any Windows installation technology, including .msi, .exe, or scripts (Python, VBScript, PowerShell, and others).

Once a package is created and ready for distribution, it is published to a software repository. You then use Package Manager to download the package from the repository to the local machine and install it on your Windows systems.

Creating a software package includes creating and saving a project. Projects can be used to create variations based on platform or version that can then be published as separate packages.

General Process

Detailed steps for creating and publishing packages are provided in the Package Studio online Help and in the *VCM Software Provisioning Installation and User's Guide*.

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 192](#) for more information.

2. Click **Manage Packages**. Configure the package contents based on the options on the following tabs:
 - a. Click **Properties**. Type a **Name**, **Version**, and **Description**. Select the **Architecture**. These are required fields. You have the option to update the other fields, depending on your requirements.
Configuring the package with Depends, Conflicts, Provides, and adding and configuring the installation and removal files.
 - b. Click **Files**. 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**. Sign the package with a signing certificate.
 - a. Click **Open** to select a package (*.crate file).
 - b. Click **Sign**. Select a certificate from the certificate store or from a file.
4. Click **Manage Repositories**. 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 then click **Open**. The **Publish Package** dialog box appears.
 - 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**. 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 list.
 - d. Click **Select Attribute Name** and select a registry property or WMI attribute in the drop-down list.
 - 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 can collect and view Repository and Package Manager data, and then install, update, or remove packages.

Prerequisites

The following prerequisites must be met before you can begin using VCM Software Provisioning:

- You have created software provisioning packages using VMware vCenter Configuration Manager Package Studio and published the packages to the repositories.
- Package Manager is installed on the target machines. Package Manager is automatically installed when you install the VCM 5.3 Agent or later.

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.

As you work with provisioning, you will want to regularly collect Package Manager data to determine if your machines are remaining current with the necessary software packages.

Procedure

1. Click **Collect**.
The **Collection Type** page of the **Collection Wizard** appears.
2. Select **Machine Data**.
3. Click **OK**. The **Machines** page appears.
4. Verify that the **Selected** pane displays all the machines from which you are collecting package manager data. Add any machines as needed.
5. Click **Next**. The **Data Types** pages appears.
6. Expand **Windows**, and then select **Software Provisioning - Package Managers**.
7. Click **Next**. The **Important** page appears.
8. Review the information, resolve any conflicts, and then click **Finish**. You can monitor the process in the **Jobs Manager**. See "[Viewing Provisioning Jobs in the Job Manager](#)" on page 196 for more information.

When the collection is completed, select **Console > Windows tab > Operating System > Software Provisioning > Package Managers**. The data grid displays the packages and their current status.

Collect Software Repository Data

A collection of repository data will include the software packages in the repository, allowing you to determine which repositories to assign to machines based on the available packages.

TIP Create a Machine Group containing all machines on which the software repository is installed.

Procedure

1. Click **Collect**.
The **Collection Type** page of the **Collection Wizard** appears.
2. Select **Machine Data**.
3. Click **OK**. The **Machines** page appears.
4. Verify that the **Selected** pane displays all the machines from which you are collecting repository data. Add any machines as needed.
5. Click **Next**. The **Data Types** pages appears.
6. Expand **Windows**, and then select **Software Provisioning - Repositories**.
7. Click **Next**. The **Important** page appears.

- Review the information, resolve any conflicts, and then click **Finish**. You can monitor the process in the **Jobs Manager**. See "[Viewing Provisioning Jobs in the Job Manager](#)" on page 196 for more information.

When the collection is completed, select **Console > Windows tab > Operating System > Software Provisioning > Repositories**. The data grid displays the packages in the repositories.

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.

Procedure

- Select **Console > Windows tab > Operating System > Software Provisioning > Package Managers** data grid.

- Select one or more machines, and then click **Add Source**.

The **Select Machines** page of the **Add Source** wizard appears.

- Verify that the machines displayed in the lower pane are the machines to which you want to add the source. Add or remove machines as needed.

- Click **Next**.

The **Enter or Select Source** page appears.

- Select either **Add source at the beginning of existing source lists** or **Add source at the end of the existing source list**.

- Type the **URI** or click **Browse Sources**. If you click **Browse Sources**, the **Browse Sources** page appears. In the Show Sources from drop-down list, select one of the following:

- 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 automatically populates the **Platform** and **Section** field 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.

- Type a **Platform** name and a **Section** name. The names must be typed exactly as they are used in the repository.

- Click **Next**.

The **Schedule** page appears.

- Select one of the scheduling options and configure as needed.

- Click **Next**.

The **Confirmation** page appears.

- Review the information. If it is correct, click **Finish**.

You can monitor the status of the process using **Jobs Manager > Running**.

The added source is displayed in the **Package Manager - Sources** data grid.

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 then running any specified post-scripts. You can also remove packages.

Procedure

1. Select **Console > Windows tab > Operating System > Software Provisioning > Package Managers**
2. Click **Install**.

The **Select Machines** page of the **Install Package** wizard appears.

3. Verify that the machines displayed in the lower pane are the machines to which you want to install the package. Add or remove machines as needed.
4. Click **Next**.

The **Select Package to Install** page appears.

5. In the **Package Name** list, select the package to install.
6. Select one of the following version options:
 - **Install Version:** 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.
 - **Install latest available version on all platforms:** Installs the latest version of the package available from the sources configured for the Package Manager.
7. Configure the **Security Options**.

This option determines if a package is installed or removed based on the state of the signature. Select one of the following options:

- **Install secure signed package only:** 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.
 - **Skip signature validation when installing a signed package:** (Not Recommended) The package is installed or removed without attempting to verify the signature.
 - **Allow unsigned package to be installed:** (Not recommended) The package is installed or removed even if it is unsigned.
8. Click **Next**.
- The **Schedule** page appears.
9. Select one of the scheduling options and configure as needed
 10. Click **Next**.
- The **Confirmation** page appears.
11. Review the information. If it is correct, click **Finish**.
 12. Review the information, resolve any conflicts, and then click **Finish**. You can monitor the process in the **Jobs Manager**. See ["Viewing Provisioning Jobs in the Job Manager" on page 196](#) for more information.

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:

- **Job Manager:** Displays current jobs running, and job history. Use the job history when troubleshooting the processing of a job. See ["Viewing Provisioning Jobs in the Job Manager" on page 196](#) for more information.
- **Compliance:** You can create compliance rules based on software provisioning data types, and you can add provisioning remediation actions to rules.
 - ["Creating Compliance Rules based on Provisioning Data" on page 196](#)
 - ["Creating Compliance Rules containing Provisioning Remediation Actions" on page 197](#)
- **User Rules and Roles:** You can define user access rules and roles to specify what level of access users have to the Software Provisioning data and actions in VCM. Select **Administration > User Rules and Roles > User Manager > VCM Access** to configure the Access Rules and Roles.
- **Reports:** You can run reports on collected Software Provisioning data. Select **Reports > Machine Group Reports > Software Provisioning** to run the default reports, or you can create your own.
- **Change Management:** All Software Provisioning are available for auditing as part of Change Management. Select **Console > Change Management > VCM Initiated** or **Non VCM Initiated** to view the data.

Software Provisioning actions are not eligible for rollback through Change Management. The undoing of any unwanted changes can be handled using Compliance enforcement remediation actions. See ["Creating Compliance Rules containing Provisioning Remediation Actions" on page 197](#) for general information about remediation.

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.

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:

- Change Request: Add Source
- Change Request: Remove Source
- Change Request: Install Package
- Change Request: Remove Package

Creating Compliance Rules based on Provisioning Data

A Compliance rule based on Provisioning data can detect any packages or sources that are out of compliance. You can also configure remediation actions to bring the machines back into compliance.

In this example the Compliance rule checks whether the source, where 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. Select **Compliance > Machine Group Compliance > Rule Groups**. Either add a rule to an existing rule group or create a new rule group.
2. To add a rule to a Rule Group, expand your rule group, and then select **Rules**. The **Rules** data grid appears.
3. Click **Add**. The **Rule and Name** page of the **Rule Wizard** appears.
4. Type a **Name** and **Description** for your rule.
5. Click **Next**. The **Data Type** page appears.
6. Expand **Windows** and select the data type on which you are basing the rule. The data type does not need to be software based, you will later configure the software provisioning remediation. In this example, select **Services**.
7. Click **Next**. The **Rule Type for Services** page appears.
8. Select **Conditional (if/then)**, and then click **Next**. The **Conditional Data** properties for **Services** page appears.
9. In the **IF** area, click **Add**.
10. Select Source Repository = YourRepository.
11. Select **Must Exist**.
12. In the **THEN** area, select Platform = Any and Section = Release.
13. **Next**. The **Options** page appears.
14. Select a **Severity** in the drop-down list.
15. Select **Make available for enforcement where possible**.
16. Select **Software Provisioning action**.
17. Select **Add Source** in the drop-down list, and then click **Define Action**. The **Software Provisioning Compliance Remediation** page appears.
18. Select **Add source to the beginning of existing source list**.
19. Click **Browse Sources** to select the repository URI where the Platform=Any and Section=Release exist. The **Platform** and **Section** update with Any and Release respectively.
20. Click **OK** to close the page, and then click **Next**. The **Collection filters** page appears.
21. Select the Provisioning - Package Managers collection filter.
22. Click **Next**. The **Important** page appears.
23. Review the information, and then click **Finish** to save your rule.

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.

Creating Compliance Rules containing Provisioning Remediation Actions

When configuring a Compliance rule, you can configure the rule to perform a remediation based on a software provisioning action -- Install Package, Remove Package, Add Source, Remove Source.

In this example, you want to determine if a software application named XSoftware is correctly 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. Select **Compliance > Machine Group Compliance > Rule Groups**. Either add a rule to an existing rule group or create a new rule group.
2. To add a rule to a Rule Group, expand your rule group, and then select **Rules**. The **Rules** data grid appears.
3. Click **Add**. The **Rule and Name** page of the **Rule Wizard** appears.
4. Type a **Name** and **Description** for your rule.
5. Click **Next**. The **Data Type** page appears.
6. Expand **Windows** and select the data type on which you are basing the rule. The data type does not need to be software based, you will later configure the software provisioning remediation. In this example, select **Services**.
7. Click **Next**. The **Rule Type for Services** page appears.
8. Select **Conditional (if/then)**, and then click **Next**. The **Conditional Data** properties for **Services** page appears.
9. In the **IF** section, click **Add**.
10. Select `Services Name = XService`.
11. Select **Must Exist**.
12. In the **THEN** section, click **Add**.
13. Select `State = Running`.
14. Click **Next**. The **Options** page appears.
15. Select a **Severity** in the drop-down list.
16. Select **Make available for enforcement where possible**.
17. Select **Software Provisioning action**.
18. Select **Install Package** in the drop-down list, and then click **Define Action**. The **Software Provisioning Compliance Remediation** page appears.
19. Select the XSoftware package to install if the rule you are configuring fails.
20. Configure the version options to use the selected version, specify a different version, or install the latest version.

21. Select one of the following **Security Options**:

This option determines if a package is installed or removed based on the state of the signature. Select one of the following options:

- **Install secure signed package only:** 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.
- **Skip signature validation when installing a signed package:** (Not Recommended) The package is installed or removed without attempting to verify the signature.
- **Allow unsigned package to be installed:** (Not recommended) The package is installed or removed even if it is unsigned.

22. Click **OK** to close the page, and then click **Next**. The **Collection filters** page appears.

23. Select the `Services` collection filter.

24. Click **Next**. The **Important** page appears.

25. Review the information, and then click **Finish** to save your rule.

When the Compliance Template is run, if the check for XService running fails, the XSoftware package is installed.

Further Reading

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.

Getting Started with VCM Management Extensions for Assets

13

Getting Started with VCM Management Extensions for Assets

VCM Management Extensions for Assets (VCMMA) facilitates the storage of asset data across multi-platform enterprises into a single repository. With VCMMA, you can integrate and manage data not collected by VCM. This data appears in the VCM Console.

To get started using VCMMA, follow these steps.

[Step 1: Add, Edit, or Delete Hardware and Software Configuration Item Fields.](#)

[Step 2: Add Hardware Configuration Items.](#)

[Step 3: Add Software Configuration Items.](#)

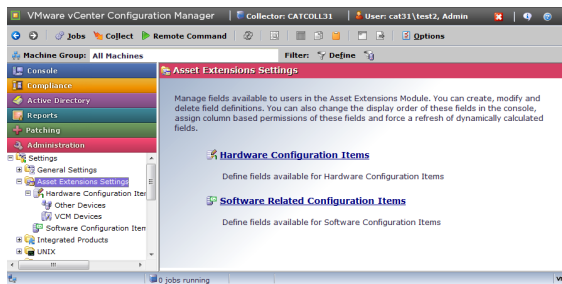
Review Hardware and Software Configuration Item Fields

Before you begin to add asset data to VCM, you should review the default hardware and software fields in VCMMA and determine if they satisfy the needs of your organization. If not, create, modify, or delete the fields according to your needs.

NOTE VCMMA Administration functionality is available only to users logged in with the Admin role.

To view the fields, follow these steps.

1. Click **Administration > Settings > Asset Extensions Settings**. The VCMMA navigation window appears.



3. Consider whether the fields are listed in the order in which you want them to appear in the Console. If not, click **Column Order** in the data grid view to reorder the fields to your specifications.
3. Consider whether the fields are listed in the order in which you want them to appear in the Console. If not, click **Column Order** in the data grid view to reorder the fields to your specifications.
4. By default, dynamic fields are refreshed every six hours. To force a refresh of dynamic fields at any time, click **Refresh Dynamic Fields** in the data grid view.

Modifying Hardware Configuration Item Fields

Use VCMMXA to manage your hardware assets. Add, edit, and delete the hardware configuration items to maintain asset data for the following types of hardware devices:

- **VCM Devices:** Include machines that are currently licensed and managed by VCM. These machines are listed in **Administration > Machines Manager > Licensed Machines**.
- **Other Devices:** Include machines that are not managed by VCM, as well as other hardware devices, such as bridges, routers, or fax machines.

View Available Fields

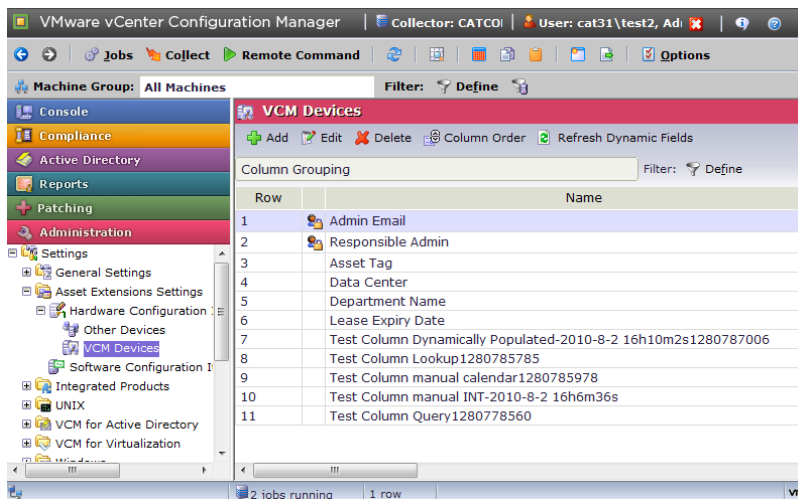
To view the fields available for both VCM Devices and Other Devices, follow these steps.

1. Click **Administration > Settings > Asset Extensions Settings > Hardware Configuration Items > VCM Devices or Other Devices**. The data grids in these views contain a list of fields that are available for the type of device you are configuring (VCM Device or Other Device). Each of these fields appears as a column in **Console > Asset Extensions > Hardware Configuration Items**.
2. Before users populate these fields with asset data, review the fields, and then add, edit, or delete them as desired.

Add or Edit a Hardware Configuration Item Field

To add or edit a hardware configuration item field, follow these steps.

1. Click **Administration > Settings > Asset Extensions Settings > Hardware Configuration Items**. The Hardware Configuration Items view appears.



2. Click **VCM Devices** or **Other Devices**, depending on the type of field you want to delete.
3. If you are editing an existing field, select the field, and then click **Edit**. Otherwise, to add a field, click **Add**. The **Add/Edit Fields** wizard appears.

4. Enter the name and description of the field, and then click **Next**. This name appears as the column heading in **Console > Asset Extensions > Hardware Configuration Items**.

5. If you are adding a field, determine how you want this field to be populated. Click the appropriate option button: **Manually** (free-form text), **Lookup** (pick from list of predetermined values), or **Dynamically** (population from another source), and then click **Next**. If you are editing a field, you cannot change the population method. For more information, click **Help**. Otherwise, click **Next**.
6. If you have defined this field as a lookup, the wizard prompts you to define or edit the lookup values. Enter the required information, and then click **Next**.
7. Assign the roles that should have edit access to this field, and then click **Next**. Users with these roles can then edit the values of the field from **Console > Asset Extensions > Hardware Configuration Items**.
8. Confirm your addition or edit, and then click **Finish**. The field now appears in the **Administration > Settings > Asset Extension Settings > Hardware Configuration Items > VCM Devices** or **Other Devices** data grid, and as a column in the **Console > Asset Extensions > Hardware Configuration Items > VCM Devices** data grid.

Delete a Hardware Configuration Item Field

To delete a hardware configuration item field, follow these steps.

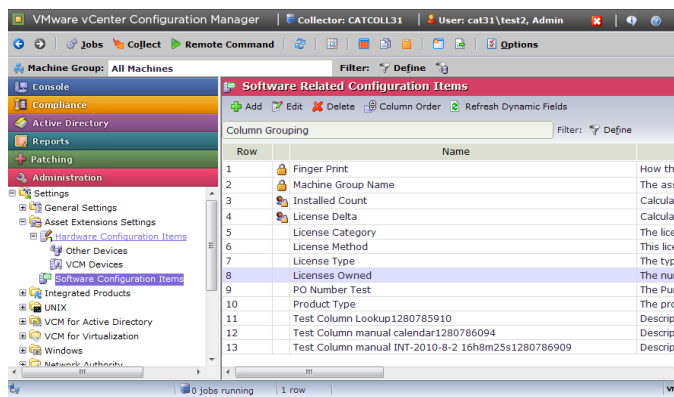
1. Click **Administration > Settings > Asset Extension Settings > Hardware Configuration Items**.
2. Click **VCM Devices** or **Other Devices**, depending on the type of field you want to delete.
3. Select the field, and then click **Delete**. You cannot delete fields marked with a Locked icon.
4. Click **OK** to confirm. VCM deletes the field from VCMMXA.

Modifying Software Configuration Item Fields

Use VCMMXA to manage your software assets. Add, edit, and delete the software configuration items to maintain asset data for your software.

Add or Edit a Software Configuration Item Field

1. Click **Administration > Settings > Asset Extension Settings > Software Configuration Items**. The Software Related Configuration Items view appears.



2. Review the available fields, and then determine whether you want to add, edit, or delete any of the existing fields. If you are editing an existing field, select the field, and then click **Edit**. Otherwise, to add a field, click **Add**. The **Add/Edit Fields** wizard appears.

Name & Description
Enter a name and description for the field.

Name:
Finger Print

Description:
How the Assets module determines if the software is installed

Help Cancel < Back Next > Finish

3. Enter the name and description of the field. This name appears as the column heading in **Console > Asset Extensions > Software Configuration Items**. Click **Next**.
4. If you are adding a field, determine how you want this field to be populated. Click the appropriate option button, and then click **Next**. If you are editing a field, you cannot change this information. For more information, click **Help**. Otherwise, click **Next**.

- If you have defined this field as a lookup, the wizard prompts you to define or edit the lookup values. Enter the required information, and then click **Next**.
- Assign the roles that should have edit access to this field. Users with these roles can then edit the values of the field from **Console > Asset Extensions > Software Configuration Items**. Click **Next**.
- Confirm your addition or edit, and then click **Finish**. The field now appears in the **Administration > Settings > Asset Extension Settings > Software Configuration Items > VCMDevices** or **Other Devices** data grid, and as a column in the **Console > Asset Extensions > Software Configuration Items** data grid.

Delete a Software Configuration Item Field

Use the following procedure to delete a Software Configuration Item field from VCMMXA.

- Click **Administration > Settings > Asset Extension Settings > Software Configuration Items**.
- Click **VCM Devices** or **Other Devices**, depending on the type of field you want to delete.
- Select the field, and then click **Delete**. You cannot delete fields marked with a Locked icon.
- Click **OK** to confirm. VCM deletes the field from VCMMXA.

Adding Hardware Configuration Items

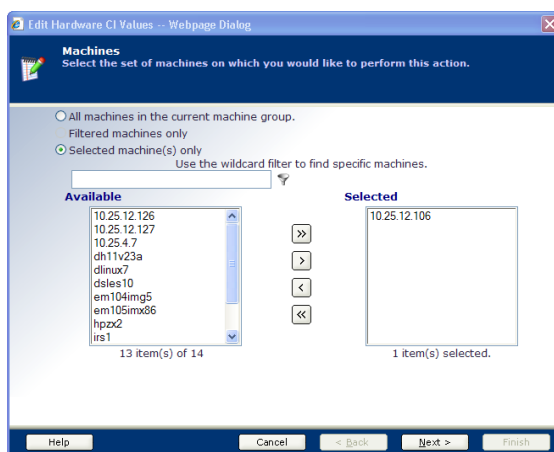
Now that you have configured your VCMMXA fields for both VCM managed and non-managed devices, you can populate those fields with machine-specific data. To begin populating the fields, use the following procedures.

Editing Values for Devices

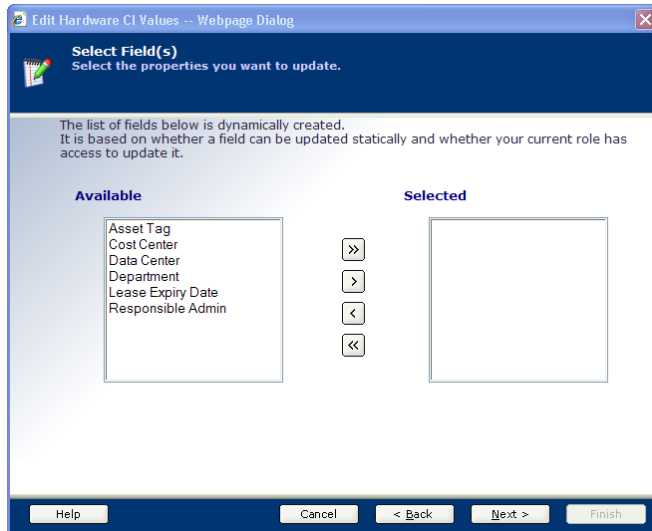
Use the VCM Console to view a list of licensed, VCM-managed machines. Machines appear in this data grid when they are licensed (see [Licensing Windows Machines](#) or [Licensing UNIX/Linux Machines](#) in the online Help). Machines are removed from this data grid when they are removed from the list of licensed machines in Machines Manager (**Administration > Machines Manager > Licensed Machines**).

To add information specific to the VCM-managed machines:

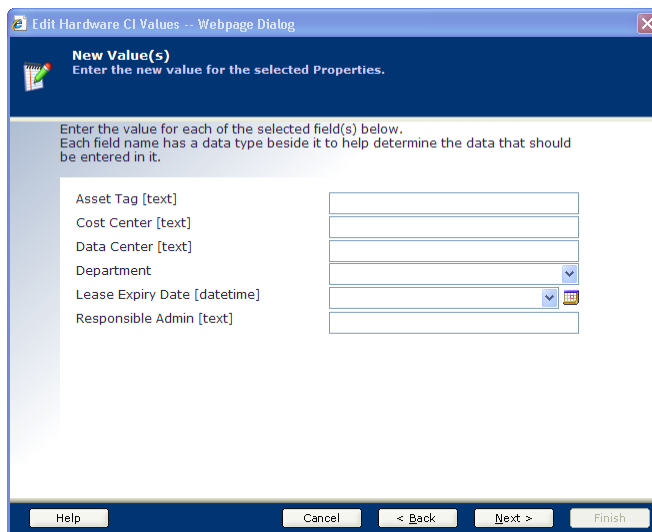
- Click **Console > Asset Extensions > Hardware Configuration Items > VCM Devices**.
- Select the machine or group of machines to edit, and then click **Edit Values**. VCM launches the **Edit Hardware CI Values** wizard.



- Verify the machines you want to edit appear in the **Selected** pane. Click **Next**.



4. Select the fields to edit, and then click **Next**.



5. Enter a value for each of the fields displayed, and then click **Next**.
6. Confirm your change, and then click **Finish**. The **VCM Devices** data grid updates the values of the fields for the machines you edited and displays the resulting data.

Modifying Other Devices

In addition to accommodating VCM-licensed machines, VCM MXA also allows you to add up to 135,000 non-VCM managed assets. Use the **Other Devices** node to add, edit, or delete these assets.

To add or edit information specific to other devices, follow these steps.

1. Click **Console > Asset Extensions > Hardware Configuration Items > Other Devices**.
2. If you are adding a device, click **Add**. If you are editing an existing device, select that device, and then click **Edit**.

NOTE If you want to change only the values for that device, and not the device name or description itself, click **Edit Values**, instead of **Edit**. The Edit Values Wizard allows you to quickly edit the specific field values that you select. The **Edit Device** wizard is a longer wizard designed to let you edit the entire device asset record.

3. Follow the prompts through the wizard to complete the action. Click **Help** at any time for more information.
-

NOTE Use the **Clone** and **Edit Values** functionality to generate a large number of near-identical records. For example, if you are adding more than one record for a specific device type (50 telephones, for example), you can create one record for that device type, and then clone it 50 times. Once you have generated 50 identical records, you can individually select each of the records, then click **Edit Values** to change the fields that distinguish the records from one another (example: Location, or Serial Number). Navigate to **Console > Asset Extensions > Hardware Configuration Items > Other Devices**, and then click **Help** for more information.

To delete a record from the **Other Devices** data grid, follow these steps.

1. Select a record, and then click **Delete**.
2. Click **OK** to confirm your deletion. VCM MXA deletes the requested record from the Other Devices data grid.

Adding Software Configuration Items

Use the **Software Configuration Items** node to build a list of software assets. You can add values to the inventory and manage other aspects of software, such as license counts, license expiration dates, or even custom fields that support your organization's processes.

When you configure the values for these fields, they are available in Compliance also, where you can create rules to actively check inventory. For example, use options in VCM Compliance to verify that your install count for licensed software is below your overall purchase license count. For more information about VCM MXA-specific issues in Compliance, click **Console > Asset Extensions**, and then click **Help**.

To add or edit Software Configuration Items, follow these steps.

1. Click **Console > Asset Extensions > Software Configuration Items**.
 2. If you are adding software, click **Add**. If you are editing an existing software asset record, select that row, and then click **Edit**.
 3. If you want to change the values for that software entry, and not the software asset name or description itself, click **Edit Values**, instead of **Edit**. The **Edit Values** wizard allows you to select the field values you want to edit, and then change them. The **Edit** wizard is designed to let you edit the entire software asset record.
-

NOTE Use the **Clone** and **Edit Values** functionality to generate a large number of near-identical records. For example, if you are adding more than one record for a specific software item, you can create one record for that item, and then clone it 50 times. Once you have generated 50 identical records, you can individually select each of the records, then click **Edit Values** to change the fields that distinguish the records from one another. Navigate to **Console > Asset Extensions > Software Configuration Items**, and then click **Help** for more information.

To delete a record from the Software Configuration Items data grid, follow these steps.

1. Select the record, and then click **Delete**.
2. Click **OK** to confirm your deletion. VCMMXA deletes the requested record from the **Software Configuration Items** data grid.

Further Reading

For information on how to customize for your environment, refer to [Customizing VCM](#). Each of these areas regarding customization also applies to VCMMXA. You can also read [Maintaining VCM after Installation](#) for important information regarding additional data retention settings and database maintenance steps that you should take.

When using VCMMXA, refer to the online Help for specific information.

Getting Started with Service Desk Integration

VCM Service Desk Integration allows you to track planned and unplanned changes to managed machines in your organization, and to integrate these changes with your organization's change management process.

When Service Desk Integration is licensed, integrated with VCM Service Desk Connector, and activated, it temporarily halts any requested change to a VCM-managed machine while VCM integrates with the Service Desk application to pass the change through a predefined change management process or workflow. Once the change is approved through the workflow, VCM reinstates the change requested on the Agent machine(s), based upon machine criticality.

VCM Service Desk Connector communicates with both VCM and your Service Desk application to help users track and manage all VCM-initiated planned and unplanned changes across an organization. Any change to a VCM-managed machine that is requested in VCM must advance through the defined workflow before being executed. The workflow definition varies by customer and is dependent upon the configuration implemented during the VMware services engagement and as determined by the customer's change management process.

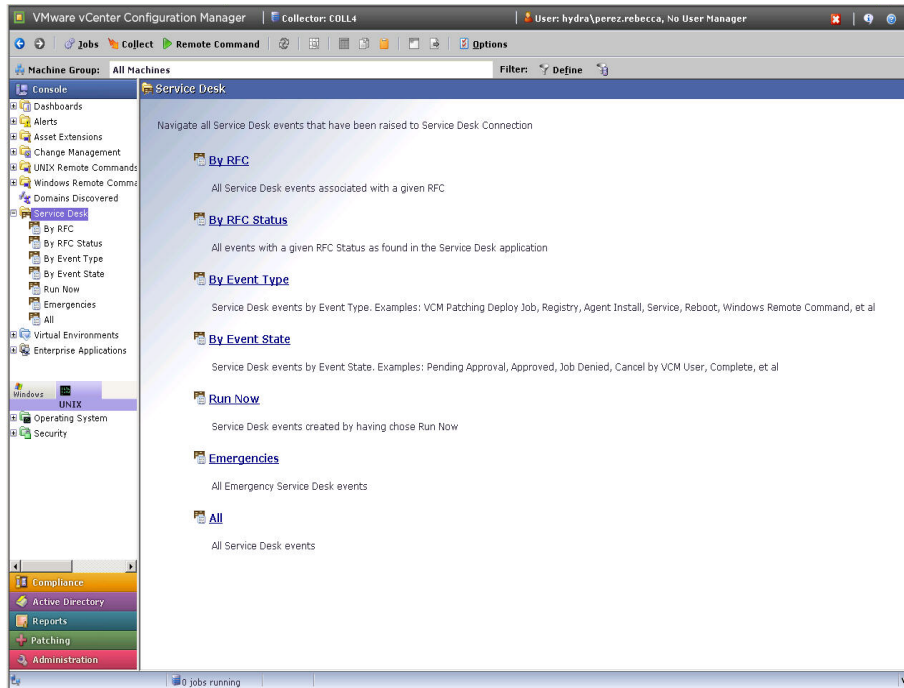
If you have licensed VCM Service Desk Integration, will you be able to see the Service Desk nodes. However, you must arrange a services engagement to "turn on" Service Desk functionality, and configure and implement this component. Contact VMware Customer Support to determine the requirements for your integration. Once VMware Customer Support has enabled VCM Service Desk Integration, they will give you an overview of how to use the product in your organization. You may also refer to the online Help for more information on how to use VCM Service Desk Integration.

Service Desk Integration in the Console

The Service Desk node provides a single entry point for viewing all VCM-related Service Desk events. Click any sub-node beneath the Service Desk node to view data by that variable. For example, click **By RFC** to view the data for a single Request For Change (RFC). In the By RFC sub-node, select any of the listed RFCs to view the data for that item only.

The data views shown below are the default VCM Service Desk Integration views. Your configuration may differ, based on your organizational requirements and specific implementation.

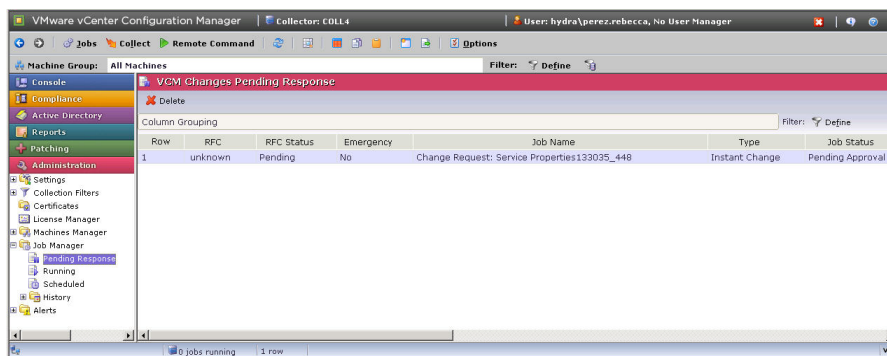
Click **Console > Service Desk** to display the VCM Service Desk Integration node.



Service Desk Integration in Job Manager

When VCM Service Desk Integration is licensed and activated, it suspends any requested change to a VCM-managed machine while VCM integrates with the Service Desk application to pass the change through a change management process. If a job was suspended in VCM, it appears in **Administration > Job Manager > Pending Response**. Once the job is approved, it is released to run, thereby appearing in either the **Job Manager > Running** or **Job Manager > Scheduled nodes**. Jobs integrated with VCM Service Desk Integration are listed by RFC in the Job Manager data grids.

Click **Administration > Job Manager** to display the VCM Job Manager node.



NOTE Jobs for VCM Patching-managed machines appear in the Patching Job Manager, not the VCM Job Manager. Locate these jobs at: **Patching > Administration > Job Manager**. Click **VCM Patching Administration > Job Manager > Pending Response** to locate jobs that are currently awaiting approval. Click **VCM Patching Administration > Job Manager > Running or VCM Patching Administration > Job Manager > Scheduled** to locate approved jobs that are currently running, or are scheduled to run.

Further Reading

Refer to [Customizing VCM](#) for information on how to customize for your environment. Each of these areas regarding customization also applies to VCM for Service Desk Integration. You can also read [Maintaining VCM after Installation](#) for important information regarding additional data retention settings and database maintenance steps which should be taken.

When using VCM for Service Desk Integration, refer to the Help for specific task information. To access the Help, click the **Help** button, located on the Portal toolbar.

VCM for Active Directory (AD) collects AD objects across Domains and Forests, and displays them through a single console. This data is consolidated and displayed under the Active Directory slider, providing a logical grouping of AD object and configuration information, allowing you to view your AD structure, troubleshoot issues, and detect change.

Data can be filtered, sorted, and grouped to allow you to pinpoint the specific area in which you are interested. You can also view a subset of your AD (a Forest, Domain, or specific OU branch) by setting the AD Location in the global zone at the top of the VCM Portal. Dashboards display high-level roll up information in graphical form, Alerts can be configured to notify you when there is a problem or misconfiguration, and Change Management tracks changes to the AD objects or configuration by data class.

Before you begin collecting Active Directory data with VCM for Active Directory, you must complete the following required steps. These steps are explained in this chapter.

1. [Making VCM aware of your Domain Controllers](#)
2. [Configuring VCM for Active Directory as an additional product](#)
3. [Performing an Active Directory data collection](#)
4. [Exploring Active Directory collection results](#)

Making VCM Aware of Domain Controllers

The first step in using VCM for Active Directory (AD) is to make VCM aware of the Domain Controllers (DCs), and license them as Windows servers. Once they are licensed, you can then perform an initial machines collection to make them available to VCM for Active Directory (AD).

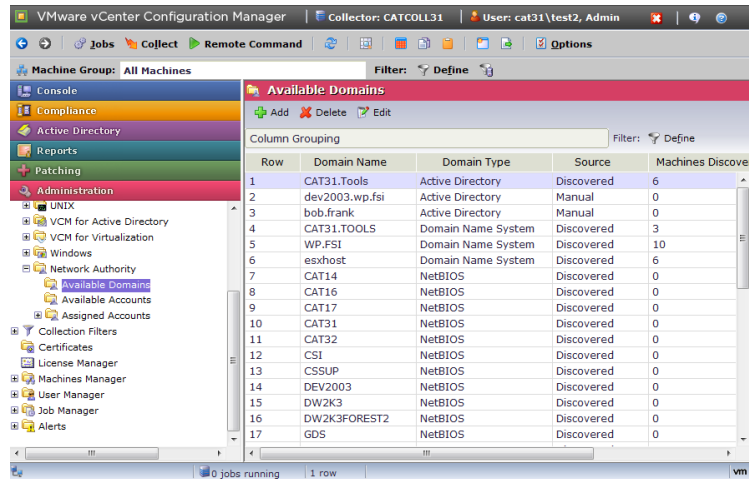
Follow the steps listed below to make VCM aware of your DCs and to perform an initial collection:

1. [Confirming the Presence of Domains](#)
2. [Adding and Assigning Network Authority Accounts](#)
3. [Discovering Domain Controllers](#)
4. [Verifying Domain Controller Machines in Available Machines](#)
5. [Licensing and Deploy the Agent](#)
6. [Performing a Machine Data Type Collection](#)

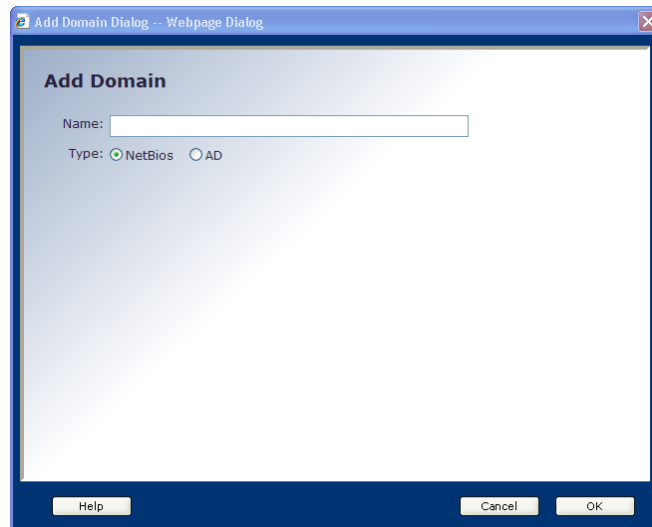
Confirming the Presence of Domains

Prior to setting up VCM for Active Directory, you must confirm that all fully-qualified DNS Domains that you want to manage have been discovered by VCM. Domains are discovered during the VCM installation process; however, you may need to manually add Domains that were unavailable during the installation process.

1. Click **Administration > Settings > Network Authority > Available Domains**.



2. Confirm that all Domains that you want to manage with VCM for Active Directory are displayed in the data grid with their fully-qualified DNS names and a **Domain Type** of Active Directory.
3. If an Active Directory Domain is not listed in the data grid, click **Add**. The **Add Domain** dialog box appears.



4. In the **Name** text box, type a fully-qualified DNS Domain name,
5. Select the **AD** type.
6. Click **OK**. Repeat the adding process to add additional Active Directory Domains.

Adding and Assigning Network Authority Accounts

Before you can perform any type of action (Discovery, Collection, and so forth), the Collector must gain access to each Domain to interact with the selected Domain Controllers (DCs) in the organization.

A VCM network authority account must have administrator rights and be added for each Domain to be managed in the organization. Once these accounts have been added, they must be assigned to Domains.

If you want to:

- Add a new Network Authority Account, refer to ["Checking the Network Authority" on page 70](#). Perform these steps for each Domain in which you will manage machines.
- Assign the Network Authority Account to each Domain, refer to ["Assigning Network Authority Accounts" on page 71](#). Perform these steps for each Domain that you plan to perform collections against.

IMPORTANT When assigning accounts, assign an available account to both the NetBIOS and Active Directory Domains.

Discovering Domain Controllers

VCM offers several options for the discovery of Domain Controllers in an organization. If you know which Domain Controllers are in your organization, then you can manually add them to the list of Available Machines. To manually add a machine, click **Administration > Machines Manager > Available (Windows) Machines**, and then click **Add Machines**.

If you have a large number of Domain Controllers to be manually added to VCM, and you only want Domain Controllers to appear in the Available Machines list, we recommend that you perform the following Browse List discovery using Domain Controller Type as a filter.

1. Click **Administration > Machines Manager > Discovery Rules**.
2. Click **Add**. The **Discovery Rules** page appears.
3. Type a **Name** and **Description** for this new discovery rule, then click **Next**. The **Discovery Method** page appears.

Discovery Method
Select the method to use when discovering machines.

Method

- By Active Directory:** Discover all machines with an account in selected AD domain.
- By Browse List:** Discover all machines that have the Computer Browser service turned on.
- By Domain Controller:** Discover all machines with an account in the selected Domain.
- By IP Address:** Discover all machines in one or more IP ranges.

Options

Also discover the presence and version of the VCM Agent when this rule is run. (Warning: If this option is selected, discoveries will take longer.)

Help Cancel < Back Next > Finish

4. Select **By Browse List**, then click **Next**. The **Discovery Filters** page appears.

Discovery Filters
Add any filters you want to apply to the set of machines during Discovery.

Discover all machines in the Browse List (warning: this could take a long time)

Only discover machines in the Browse List that match these criteria:

Where Domain Controller Type =

Add Reset

Help Cancel < Back Next > Finish

5. Select **Only discover machines in the Browse List that match these criteria**.
6. Specify the filter parameters. Select **Domain Controller Type <> "** (two single quotes).
7. Click **Next**. The **Important** page appears.
8. For the **Would you like to run this Discovery Rule now?** option, select **Yes**.
9. Click **Finish**.

IMPORTANT Click **Administration > Job Manager > History > Instant Collections > Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

Verifying Domain Controller Machines in Available Machines

Once your Domain Controller discovery is completed, verify that your Domain Controllers are available for licensing and Agent installation.

1. Click **Administration > Machines Manager > Available Machines > Available Windows Machines**.
2. Verify that the domain controller machines are available in the Domains that you added in your discovery rule.

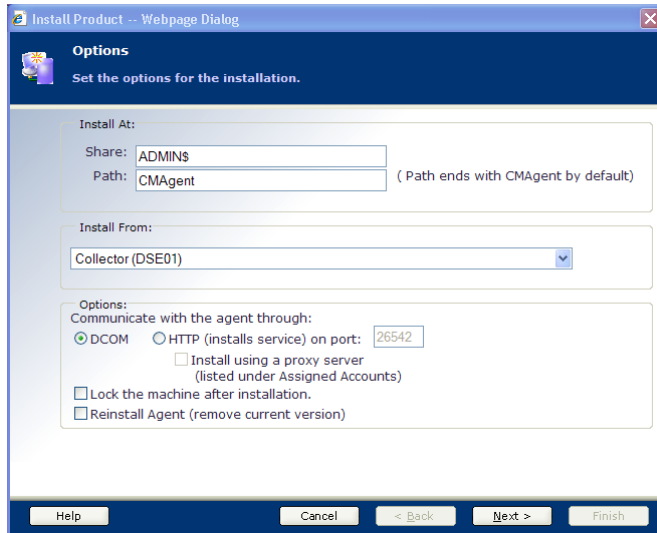
Licensing and Deploying the VCM Agent

All discovered Domain Controller machines appear in the **Available Windows Machines** list. You can group them by type (workstations or machines) and pick each Domain Controller individually or license and deploy the Agent to multiple Domain Controllers at the same time.

IMPORTANT If you are licensing and deploying the Agent on a Windows 2008 or Vista machine, you must first disable the User Account Control (UAC) on the target machine. See ["Disabling UAC for Agent Installation" on page 218](#) for more information.

NOTE Your license count determines how many machines (specifically Domain Controllers in VCM for Active Directory) that you can license. You should begin licensing Domain Controllers that have a Status Connection State of **OK**. If a connection state other than **OK** exists, you may need to work with Customer Support to assist you with troubleshooting the connection to that Domain Controller.

1. Click **Administration > Machines Manager > Available Machines > Available Windows Machines**.
2. In the data grid, select the Domain Controllers you are licensing. To select multiple Domain Controllers, use Shift-click or Ctrl-click.
3. Click **License**. The **Machines** page of the **Available Machines License** wizard appears.
4. By default, the machines selected in the data grid are displayed in the **Selected** list. To license additional Domain Controllers, double-click the machine name in the Available list to move it to the Selected list.
5. Select the **Install VCM agents for the selected machines** check box.
6. Click **Next**. The **Product License Details** page appears.
7. View your product license details, and then click **Next**. The **Important** page appears, reminding you that you are installing the Agent.
8. Click **Next**. The **Options** page appears.



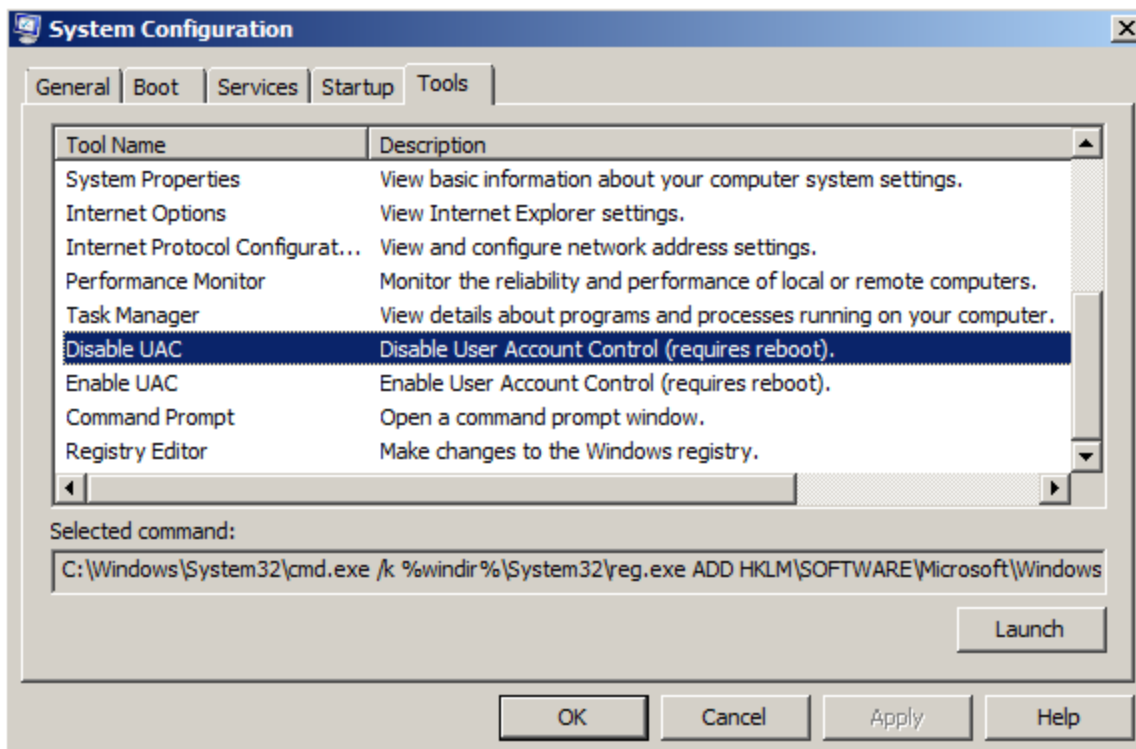
9. Verify the method used for communication. The default communication method is DCOM. For most VCM for Active Directory configurations, the default values in this screen should be used. Click **Next**. The **Schedule** page appears.
10. Select **Run Action now**, and then click **Next**.
11. Click **Finish**. The Selected Domain Controllers are moved from the **Available Machines** list to the **Licensed Machines** list, and an Install job is submitted to initiate the Agent installation on each Domain Controller.

Disabling UAC for Agent Installation

The following steps are required only if you are installing the Agent on a Windows 2008 or Vista machine. When installing the Agent on Windows 2008 or Vista, you must disable the User Account Control (UAC), install the Agent, and then re-enable the UAC.

Disabling UAC on one machine

1. On the target Windows 2008 machine, click **Start > Run**. The **Run** dialog box appears.
2. Type **msconfig** in the **Open** text box.
3. Click **OK**. The **System Configuration** dialog box appears.



4. Click the **Tools** tab.
5. In the **Tool Name** list, select **Disable UAC**.
6. Click **Launch**. A **Command** window displays the running action. When the command is completed, close the window.
7. Close the **System Configuration** dialog box.
8. Restart the machine to apply the changes.
9. Install the Agent as specified in [Licensing and Deploying the VCM Agent](#).
10. After installing the Agent on the target machine, re-enable UAC. To enable, perform the steps specified above and select **Enable UAC** in the **Tool Name** list.
11. Restart the machine to apply the changes.

Disabling UAC using Group Policy

Use the following procedure to disable the UAC on multiple machines. The instructions assume you have configured the Windows 2008 and Vista machines targeted for Agent install in a common Active Directory domain/OU.

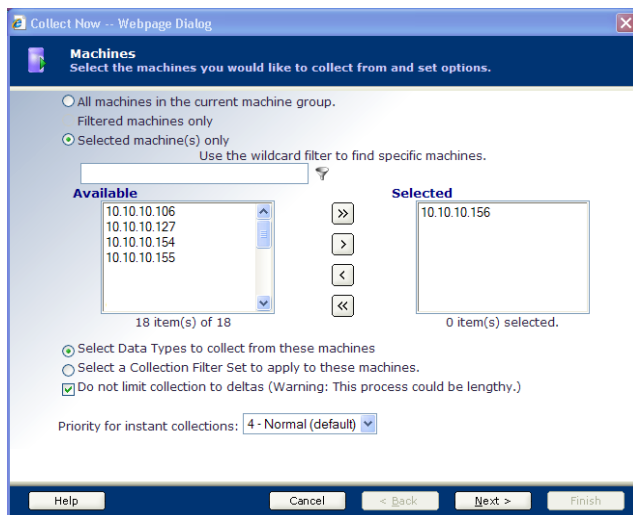
1. On a Domain Controller, click **Start > Run**. The **Run** dialog box appears.
2. Type **mmc** in the **Open** text box.
3. Click **OK**. The **Console** window appears.
4. Select **Console Root**, and then click **File > Add/Remove Snap-in**. The **Add or Remove Snap-ins** dialog box appears.
5. In the **Available snap-ins** list, double-click **Group Policy Management Editor**. The **Select Group Policy Object** dialog box appears.
6. Click **Browse**. The **Browse for a Group Policy Object** dialog box appears.

7. On the **Domains/OUs** tab, select the domain/OU to which the target machines belong, and then click **OK**.
8. On the **Select Group Policy Object** dialog box, click **Finish**.
9. On the **Add or Remove Snap-Ins** dialog box, click **OK**.
10. The domain/OU policy is added to the Console Root in the left pane.
11. Expand the added domain/OU and browse to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**.
12. In the right pane, locate the **User Access Control** policies. On each of the policies specified below, right-click and select **Properties**. Configure as follows:
 - **User Account Control: Behavior of the elevation prompt for administration in Admin Approval Mode:** Elevate without prompting.
 - **User Account Control: Detect application installations and prompt for elevation:** Disabled
 - **User Account Control: Run all administrators in Admin Approval Mode:** Disabled
13. Restart the machine to apply the changes.
14. Install the Agent as specified in [Licensing and Deploying the VCM Agent](#).
15. After installing the Agent on the target machines, re-enable UAC. To enable, perform the steps specified above and change the policies to Enabled.
16. Restart the machine to apply the changes.

Performing a Machine Data Type Collection

Now you must perform a collection based on the **Machines Data** type. Refer to [Performing an Initial Collection](#) for detailed procedures on how to perform a collection.

1. Configure the **Machines** page (Step 2) as follows:



- Add only your Domain Controllers to the **Selected** list.
 - Select the **Do not limit collection to deltas** check box. Selecting this option ensures that a full collection will occur during set up of VCM for Active Directory.
2. On the **Data Types** page (Step 3), select **Machines**.

IMPORTANT Click **Administration > Job Manager > History > Instant Collections > Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

Configuring VCM for Active Directory as an Additional Product

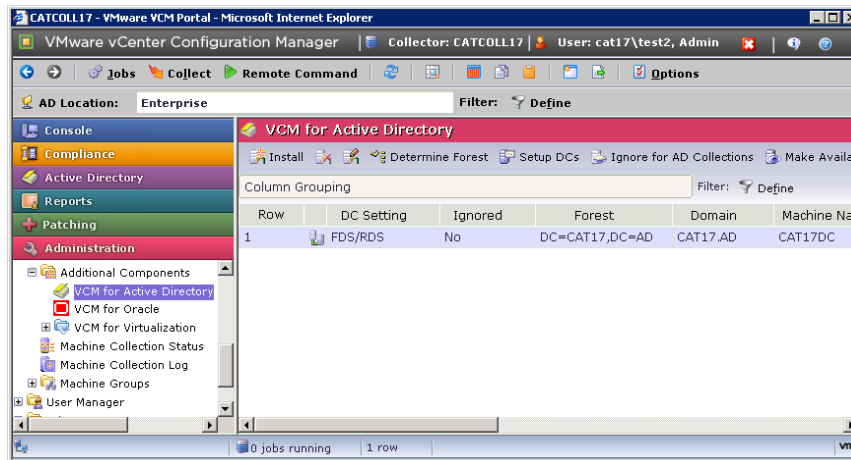
Now that VCM is aware of your Domain Controllers, follow the steps listed below to configure VCM for AD as an additional product.

1. [Deploy VCM for AD to the Domain Controllers](#)
2. [Run the Determine Forest Action](#)
3. [Run the Setup DCs Action](#)

Deploying VCM for AD to the Domain Controllers

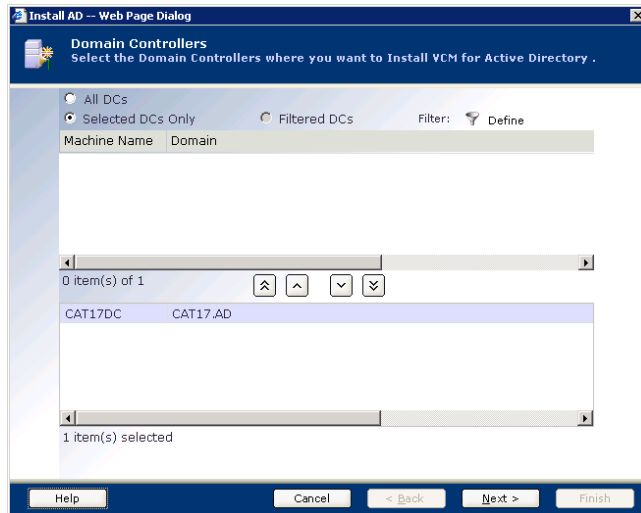
Use the following procedure to install VCM for Active Directory on each Domain Controller from which you want to collect data.

1. Click **Administration > Machines Manager > Additional Components > VCM for Active Directory**.



NOTE If the Domain Controllers that you want to collect from are not listed in **Additional Products > VCM for Active Directory** node, you may need to confirm or repeat the procedures described in the previous sections.

2. Click **Install** to deploy VCM for Active Directory to the Domain Controllers from which you want to collect Active Directory data.
3. Select the Domain Controllers on which you want to install VCM for Active Directory. We recommend that you install VCM for Active Directory on all Domain Controllers.



NOTE VCM for AD will operate with only a single domain controller configured with VCM for AD as both the FDS/RDS (Forest Data Source/Replication Data Source). However, to collect important non-replicated attributes such as Last Logon, it is essential that you configure as many domain controllers as possible with VCM for AD.

If you have machines that you plan to promote to Active Directory machines, but have not yet done so, you must install VCM for Active Directory manually. Go to **Program Files (x86)\VMware\VCM\AgentFiles** and run the `ADProductInstall.exe` installer.

4. Click **Next**.
5. Verify that **Run Action now** is selected, then click **Finish**.

IMPORTANT Click **Administration > Job Manager > History > Other Jobs > Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

Running 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. Therefore, your next step is to perform a Forest Determination for all of the licensed Domain Controllers in your list.

1. Click **Administration > Machines Manager > Additional Components > VCM for Active Directory**.
2. Click **Determine Forest**. The **Domain Controllers** page appears.
3. Move all Domain Controllers for which you want to determine the Forest to the lower pane. The Forest determination job will run only on those DCs where VCM for Active Directory is installed. We recommend determining the Forest for all Domain Controllers in the list.
4. Click **Next**. The **Important** page appears.
5. Click **Finish**.

6. Upon completing the Setup DCs action, a collection will be submitted to the selected DCs. Forest information will be displayed in the **Administration > Machines Manager > Additional Products > VCM for Active Directory** data grid. Each Setup DCs job initiates these jobs:
 - AD Schema Collection
 - AD Specifier Collection
 - AD Structure Collection

IMPORTANT Click **Administration > Job Manager > History > Instant Collections > Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

Running the Setup DCs Action

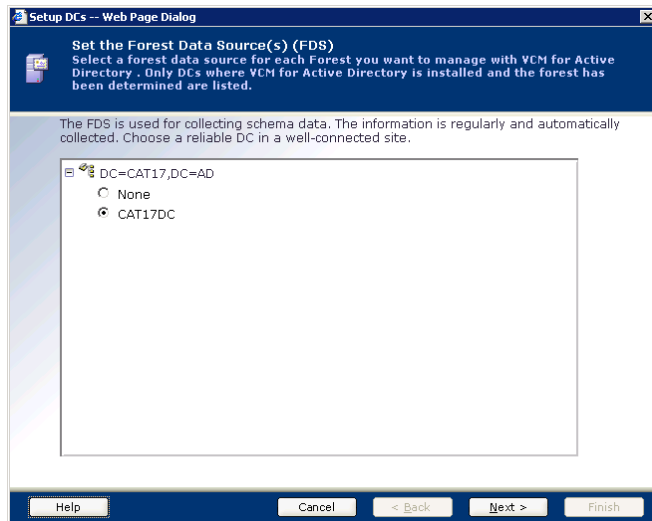
The final step that you must take prior to collecting AD objects from your Domain Controllers is to run the Setup DCs action. VCM for Active Directory collects the AD schema and your AD structure during the Setup DCs action. A Forest Data Source (FDS) and Replication Data Source (RDS) must be specified before Active Directory data is collected from a Forest.

VCM for Active Directory uses the FDS as a resource for all required Forest-level information. One Domain Controller for each Forest must be distinguished as the FDS in order for VCM for Active Directory to perform collections. The RDS serves as the Domain Controller from which all replicated data will be collected. VCM for Active Directory requires one RDS per Domain so that collections on replicated attributes are only performed on a single DC. All other Domain Controllers which have VCM for Active Directory installed will only be accessed during collections for non-replicated attributes.

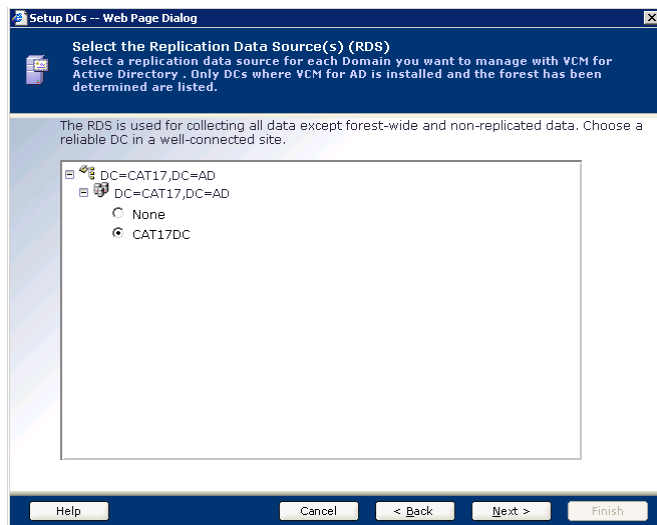
NOTE A single Domain Controller may be selected as both an FDS and RDS. We recommend selecting DCs with reliable connections and availability to serve in the FDS and RDS capacities for VCM for Active Directory collections.

If you change your RDS, any data previously collected from the RDS is not purged. The data is refreshed when you run a new collection and gather data from the new RDS.

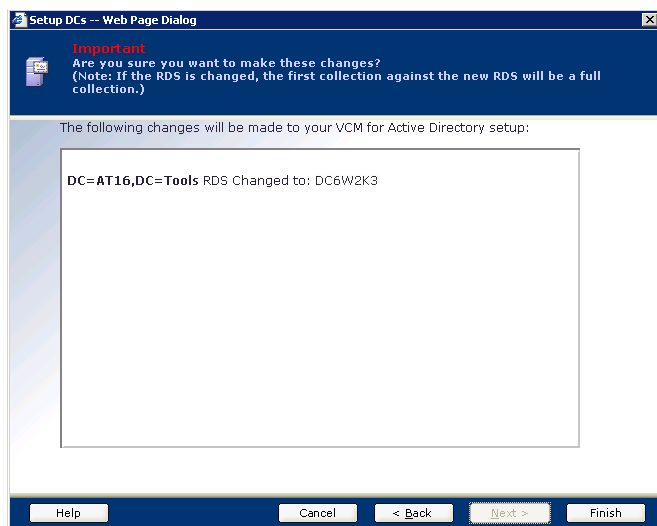
1. Click **Administration > Machines Manager > Additional Components > VCM for Active Directory**.
2. Click **Setup DCs**. The **Set the Forest Data Source(s) (FDS)** page appears.



3. Select a Forest Data Source (FDS) for each Forest to be managed in VCM for Active Directory, and then click **Next**. The **Select the Replication Data Source(s) (RDS)** page appears.



4. Select a Replication Data Source (RDS) for each Domain that you want to be managed by VCM for Active Directory. Click **Next**. The **Important** page appears.



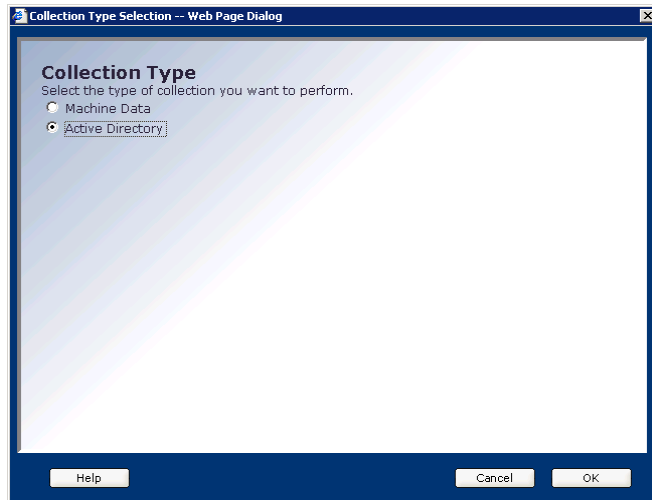
5. Click **Finish**.
6. When the Setup DCs action is completed, VCM for Active Directory performs a schema and a structure collection. The information obtained from the structure collection identifies the OU structure which supports the use of VCM for Active Directory.

IMPORTANT Click **Administration > Job Manager > History > Instant Collections > Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

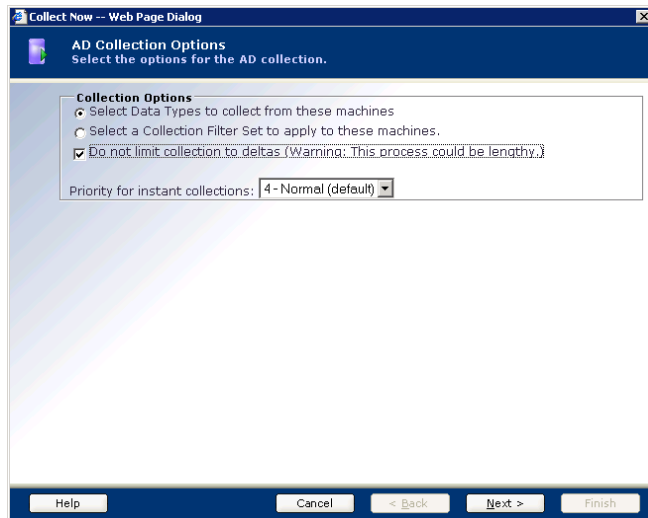
Performing an Active Directory Data Collection

You are now ready to perform your first collection of Active Directory objects using the same collection wizard used for Windows and UNIX/Linux collections. The first time you run an AD collection, the Agent will return all the objects and attributes from your Active Directory specified in the default filter set.

1. Click **Collect**, located on the Portal toolbar. The **Collection Type Selection** dialog box appears.



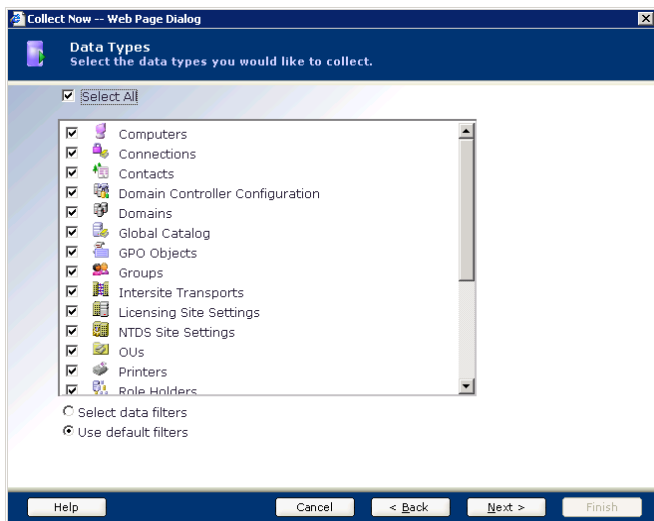
2. For the **Collection Type**, select **Active Directory**.
3. Click **OK**. The **Collect Now** wizard appears, displaying the **AD Collection Options** page.



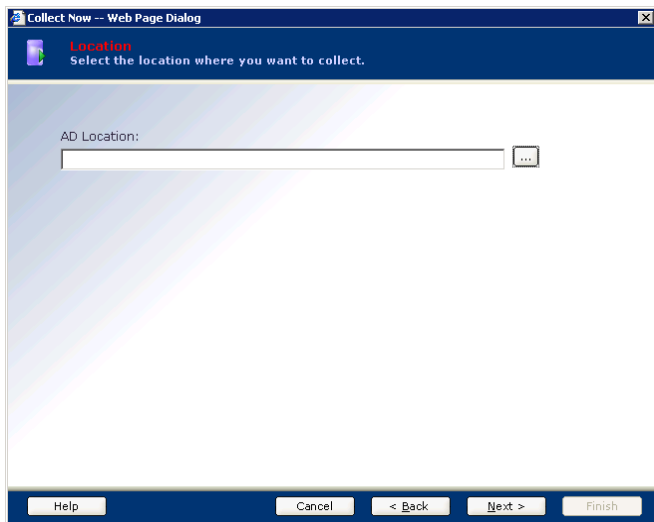
4. Click **Select Data Types to collect from these machines**.
5. To ensure that a full collection will occur during setup of VCM for Active Directory, click the **Do not limit collection to deltas** check box.

NOTE The delta collection feature makes subsequent collections run faster and more efficiently than the initial collection. For the initial collection, make sure that you click the check box so that the delta feature is disabled.

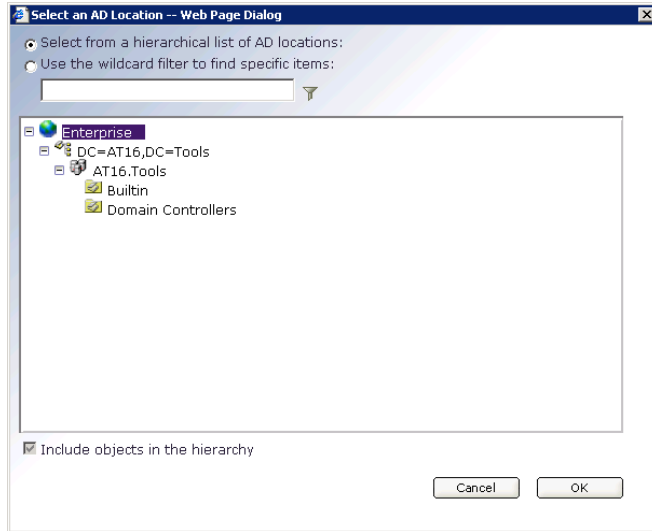
6. Click **Next**. The **Data Types** page appears.



7. Click **Select All**.
8. Select the **Use default filters** is selected option.
9. Click **Next**. The **Location** page appears.



10. To specify a location click the lookup ellipsis button (...). The **Select an AD Location** page appears.



11. Expand the **Enterprise** tree, and then select an AD Location.
12. Click **OK**, to close the page.
13. On the **Location** page, click **Next**.
14. Click **Finish**.

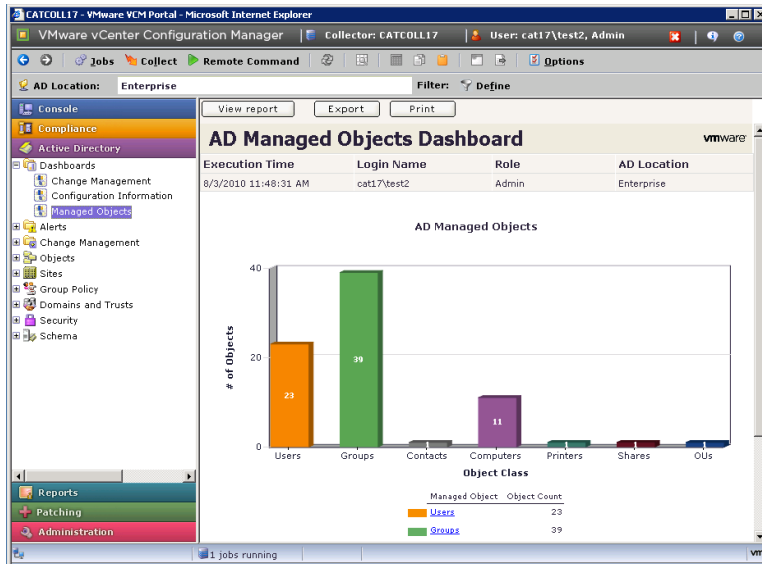
IMPORTANT Click **Administration > Job Manager > History > Instant Collections > Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

Exploring Active Directory Collection Results

Now that you have performed an initial Active Directory collection, you can explore that data in the Portal. VCM for AD presents enterprise-wide, summary information in graphical SSRS charts that you can view, export, or print. Each VCM for AD Dashboard is run only when the node is selected against the current data available in the CMDB. Therefore, Dashboard data is only current as of the time was collected. In addition, it may take time for the data to display based upon the volume or complexity of the data requested.

Active Directory Dashboards

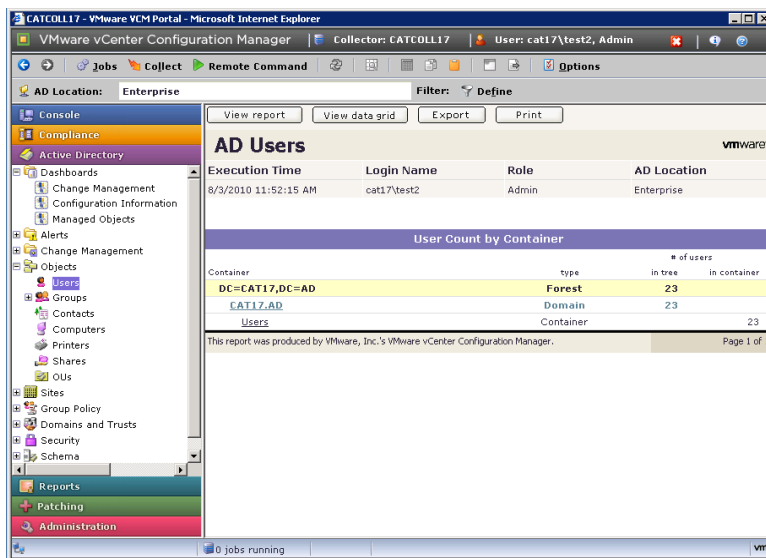
Begin by looking at the VCM for Active Directory dashboard under **Active Directory > Dashboards > Managed Objects**.



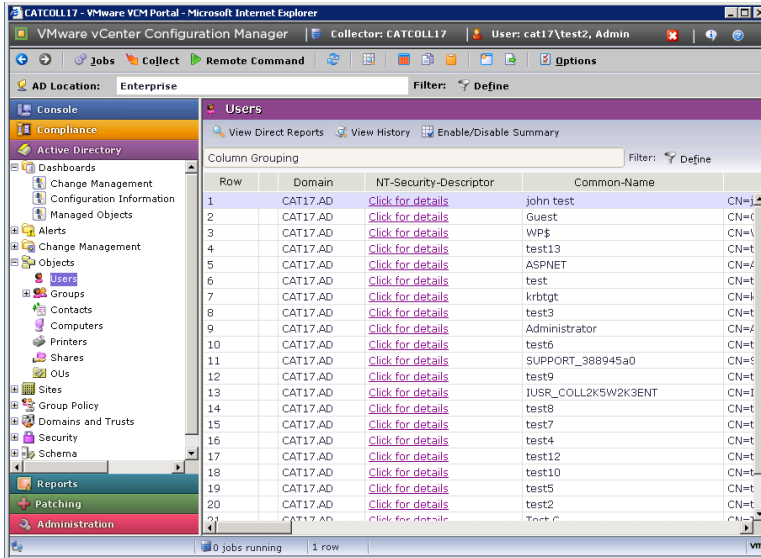
Note that several other Active Directory Dashboards are available. Take time to familiarize yourself with the remainder of the VCM for AD Dashboards.

Active Directory Summary Reports

Your AD Collection Results are also available to you in a more “raw” format as well. This level of reporting is more relevant for day to day operations, troubleshooting, and analysis and can be viewed in a Summary report or data grid format. To view a VCM for AD Summary report or data grid, click **Active Directory > Objects**. Select an object type.

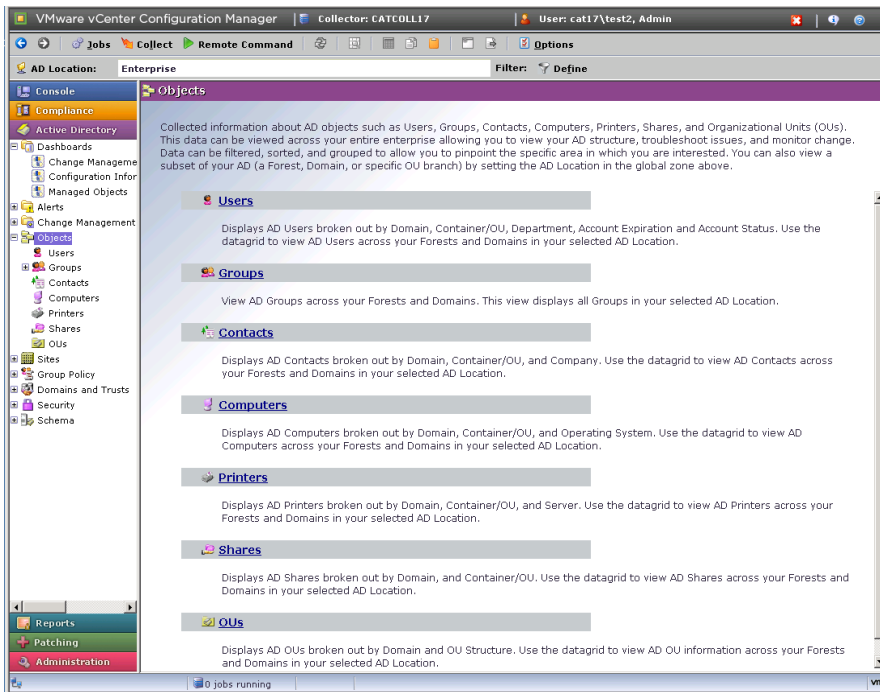


When you select the node, you will see a Summary Report, as displayed above, of the data you selected. Click **View Data Grid** to go directly to the data, or click an area of the Summary Report to filter the data before the data grid is displayed.



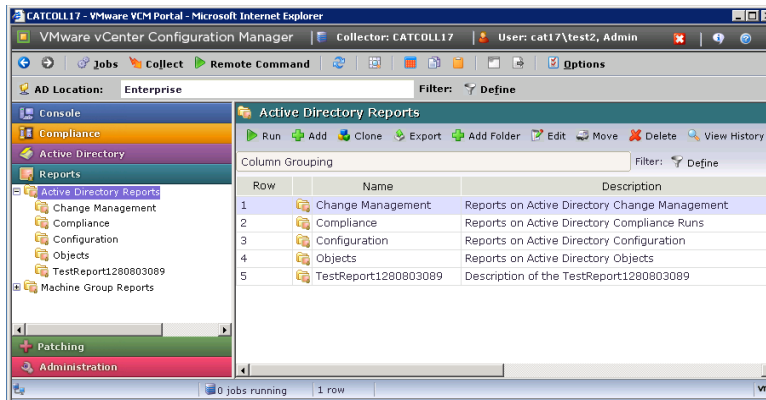
NOTE The default view is the Summary Report. At any time, however, you may switch the default view to go directly to the data grid by using the Enable/Disable Summary feature on the data grid view. See **Help** for more information on how to filter and sort your data and get full use of the data grid.

Several other categories (called “data classes”) of information regarding your AD Collection are available under the Active Directory Slider. This is where the remainder of your collected AD data is visible through the Portal.



Active Directory Reports

An alternative way to view your collected AD data is by running VCM Reports or creating your own custom reports using VCM's reporting wizard. To begin exploring VCM's Reporting functionality, click **Reports > Active Directory Reports**.



Like VCM for AD Dashboards, AD Reports are run real-time against the current data available in the CMDB, therefore they are only as current as of the time that the data was collected. In addition, it may require time for the report to generate based upon the volume or complexity of the data requested. Refer to the online Help for more information on how to schedule and disseminate reports.

Compliance for Active Directory

You may now begin to run Compliance against your collected data. To run a Compliance check, click the **Compliance** slider, and then follow the steps provided in the online Help to create rule groups, rules, filters, and templates.

Further Reading

Refer to [Customizing VCM](#) for information on how to customize for your environment. Each of these areas regarding customization also applies to VCM for Active Directory. You can also read "[Maintaining VCM After Installation](#)" on page 237 for important information regarding additional data retention settings and database maintenance steps which should be taken.

When using VCM for Active Directory, refer to the Help for specific task information. To access the Help, click the **Help** button, located on the Portal toolbar.

Accessing Additional Compliance Content

VMware provides several additional VCM Compliance Content Packages relative to the different components you have just activated. These packages are not available in the Portal until you download and import them. It is important to check to see if any of the VCM Compliance Content Packages are important to your organization, and then import them at this time.

Before you begin using this content, you must complete these steps:

1. [Locate the Content Directory.](#)
2. [Launch VMware Compliance Content Wizard \(CCW\) to Import Relevant Content.](#)
3. [Explore Imported Content Results in the Portal.](#)

Locating the Content Directory

To access the Content Packages that were supplied during your VCM content download, navigate to:
C:\Documents and Settings\All Users\Application
Data\Configuresoft\ECMImportExport\Content\.

Launching the Content Wizard to Import Relevant Content

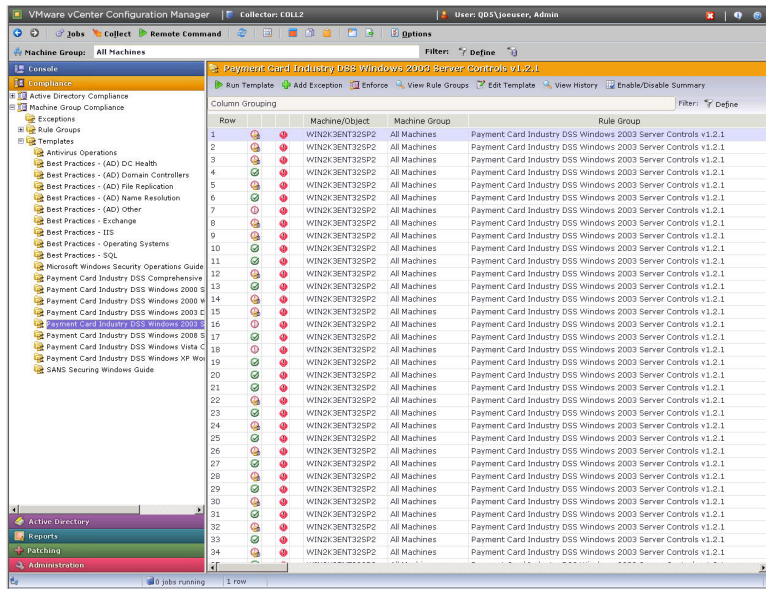
If you are loading content into VCM for the first time, refer to VCM Import/Export and VMware Content Wizard for information on how to launch VMware Content Wizard. After you have performed this initial load, you can maintain your content with VMware VCM Import/Export.

NOTE If you have Internet connectivity from your Collector, you may use the VMware Content Wizard to browse to the latest content and download it directly from VMware. VMware Content Packages are updated frequently and new Content Packages are released on a regular basis. Regardless of your connectivity, VMware recommends that you check back regularly for content updates.

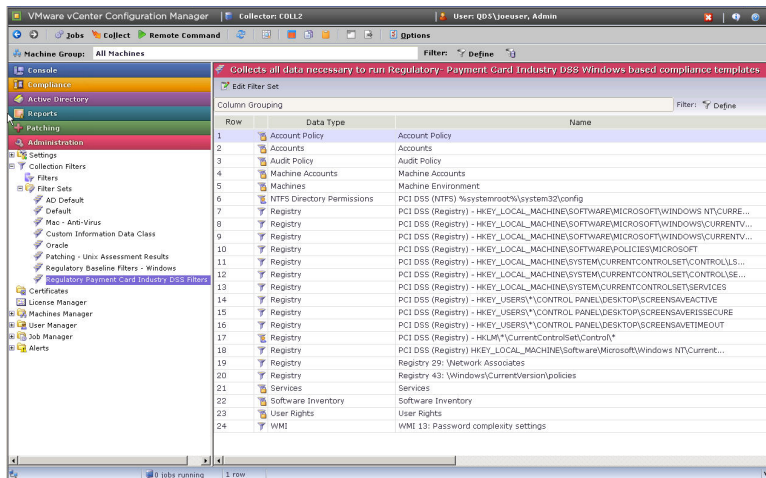
Exploring Imported Content Results in the Portal

Depending upon the particular VCM Content Package(s) you have imported, the results of your import will appear in the Portal in the following locations with their rules and rule groups expanded under the corresponding Compliance nodes.

- **Compliance > Machine Group Compliance > Templates**
- **Compliance > Active Directory Compliance > Templates**



If the particular Content Package(s) you have imported contains filter sets, they will appear under **Administration > Collection Filters > Filter Sets**.



Particular VCM Content Package(s) may contain SSRS Reports, SSRS Node Summaries, and SSRS Dashboards, which will show up in their respective locations in the Portal.

After this content has been imported into the Portal, further collections using custom filters may be required to use it. These filters are included in the Content Package. See the online Help for information on how to use a custom filter set. After the appropriate data has been collected relevant to the Content Package, see the online Help to learn more about running Compliance Templates.

Installing and Getting Started with VCM Tools

17

Several VCM components and tools were automatically installed on the Collector machine by the VCM Installation Manager during installation, as explained in the chapter [Using VCM Installation Manager](#). However, if you want to install only the VCM tools on a non-Collector machine, follow the procedure in the first section in this chapter, [Installing the Tools Only](#).

The subsequent sections in this chapter explain how to get started using the VCM tools, including:

- [Foundation Checker](#)
- [Import/Export Tool and Content Wizard Tool](#)
- Package Studio
For information about using Package Studio, see the online Help in Package Studio.
- [Deployment Utility for UNIX/Linux and ESX/vSphere](#)

Installing the VCM Tools Only

If you want to install only the VCM tools on any Windows machine other than the Collector, follow the procedure in this section. If you will be installing VCM on this machine later, you will first need to uninstall these tools and then install VCM.

1. Insert the installation CD into a drive on the non-Collector machine on which you want to install the tools. The **Installation Manager** appears.
2. Click **Run Installation Manager**.
3. Complete the initial pages, clicking **Next** to move to each subsequent page, until the **Select Installation Type** screen appears.
4. Clear the **VMware vCenter Configuration Manager** check box.
5. To install all of the tools, leave **Tools** checked, which will leave all of the individual tools checked as well. To install a subset of the tools instead, clear the Tools check box, and then clear the check box for each tool that you do not want to install. Only the tools you want to install are selected.
6. Click **Next**.
7. Complete the remaining screens, clicking **Next** to move to each subsequent screen, until the **Installation Complete** page appears.
8. Click **Finish**. You return to the initial Installation page of the Installation Manager. Click **Exit** to close the Installation Manager.

The VCM tool or tools are now installed on this machine. Proceed to the following sections in this chapter to get started using the tools.

NOTE The VCM Tools installation has prerequisites much like a VCM installation. Each tool in the Advanced Installation has its own installation requirements. For example, Import/Export (I/E) and Content Wizard can be installed only on a machine that is running VCM. Because of these requirements, you should specifically select the tools that you want to install, and note the installation requirements that VCM Installation Manager confirms using Foundation Checker.

Foundation Checker

Installation Manager uses VCM Foundation Checker to check a machine's viability for a successful VCM deployment. Foundation Checker runs a series of system checks that look for various conditions, settings, and requirements. After the system checks are complete, a results file lists which system checks passed, failed, or generated warnings.

When system checks fail, the results file includes remediation steps describing how to fix the conditions that caused the system checks to fail (a failed condition is indicated with an Error status). After you fix the conditions, you can run Foundation Checker again to ensure that all of the remediation steps were successful. If you encounter issues with your configuration, contact VMware Customer Support. A Team member may ask you to run Foundation Checker and confirm the configuration results.

Installation Manager also installs a command line version of Foundation Checker on your Collector machine during installation. For more information, see the *VCM Foundation Checker User's Guide* in `C:\Program Files (x86)\VMware\VCM\Documentation`.

After you have launched Foundation Checker, follow the steps in the wizard.

IMPORTANT If you choose to install and run the Foundation Checker before installation, it is important to uninstall the Foundation Checker before running the Installation Manager.

VCM Import/Export and Content Wizard (CW)

Use Import/Export (I/E) and the Content Wizard (CW) to move or update VCM Business Objects between databases. These tools do not import or export any collected data. However, they support the migration of any VCM Management Extension for Asset data that has been added to VCM manually. Specifically, the Import/Export Tool supports these scenarios:

- Backup (export) and restore (import) Business Objects to the same machine.
- Backup (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).
- Using CW, 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 using the Command Line Interface to automate and schedule the backup of VCM content and configuration parameters.

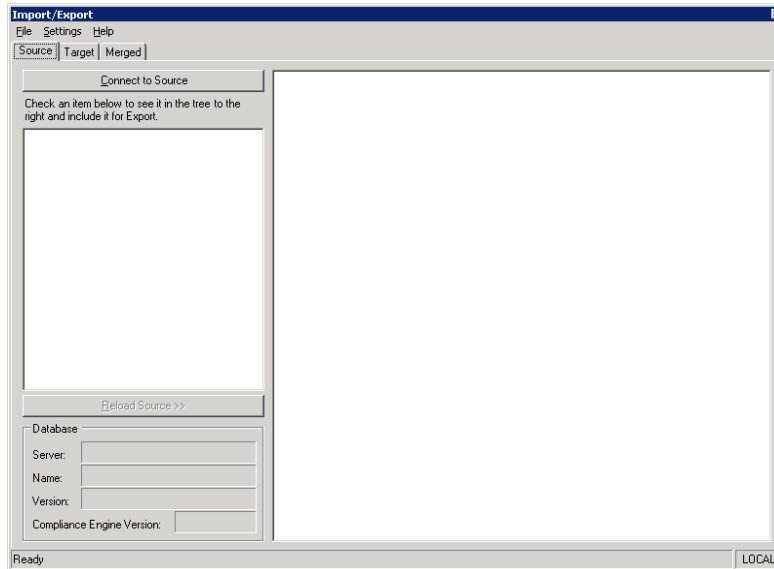
The Command Line Interface (CLI) is a powerful extension of the Import/Export graphic user interface (GUI). In addition to supporting the scenarios noted above, the CLI allows content to be overwritten (as opposed to "rename only") and provides for automation through scripting suitable for customizations.

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

Import/Export and CW were automatically installed on your Collector machine during your VCM installation. Import/Export and CW can only be run on a Collector machine. Refer to the following sections to get started with each tool.

VCM Import/Export

1. To start Import/Export on your Collector machine, click **Start > All Programs > VMware vCenter Configuration Manager > Tools > Import Export Tool**.



2. To use Import/Export, you must identify a source for the data to be imported or exported. Click **Connect to Source** (or **Connect to Target**, if you are exporting). The **Connect to Data Store** dialog box appears.
3. If you are importing, you can either select a **Server** in the drop-down list or type a server name in the text box, or import VMware content supplied by Installation Manager. To import content, click the ellipses button (...) to the right of the **File** text box, and then browse to the appropriate Content Package, commonly located at `C:\Documents and Settings\All Users\Application Data\CM\Content\`.

NOTE To add a new database, enter the database name into the selection field.

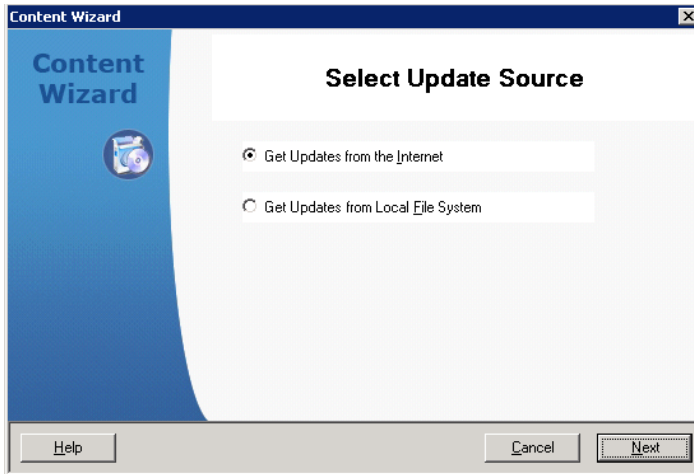
4. Identify a **Target** (destination) for the data to be exported on the **Target** tab. The target identifies the database to be imported into or compared with, or an xml file to be imported into or compared against.
5. If importing to a database, compare the selections made on the **Source** tab with the **Target** database. Specifically, you can compare the names of items and elements selected on the **Source** tab with the corresponding names of items and elements in the target database. Any duplicate items and elements must be resolved before you can continue with the import operation.

For detailed procedures on any of these steps, click **Help > Contents**, then select the appropriate topic from the left Table of Contents pane.

NOTE VMware recommends that you refer to Import/Export Help to gain a thorough understanding of the logging of Content that is not imported by Import/Export even though it is requested by the user.

Content Wizard

Unlike Import/Export, Content Wizard may be used when no user intervention is required or when you want to connect directly to the VMware Web site for the latest Content Package updates. To start the CW from your Collector Machine, click **Start > All Programs > VMware vCenter Configuration Manager > Tools > Content Wizard**.



Before you can use Content Wizard, you must specify whether you want to **Get Updates from the Internet** (which requires Internet connectivity and access beyond your local network) or **Get Updates from Local File System** if you would like to select a Content Package supplied by VCM Installation Manager. If you choose local file system, CW automatically looks in the previously mentioned Content folder. You cannot browse to an alternate location.

As you proceed through the wizard, you can select which content packages you want to import. Be advised that some Content Packages are very large. Therefore, in order to maximize performance and reduce the possibility of encountering a network issue impacting the download and/or import process, we recommend that you subdivide your imports to no more than two to three packages at a time.

Follow the wizard to completion. Since the Import/Export Merge process is transparent to the user when using CW, you must refer to the error log for any issues regarding the download or import process.

Maintaining VCM After Installation

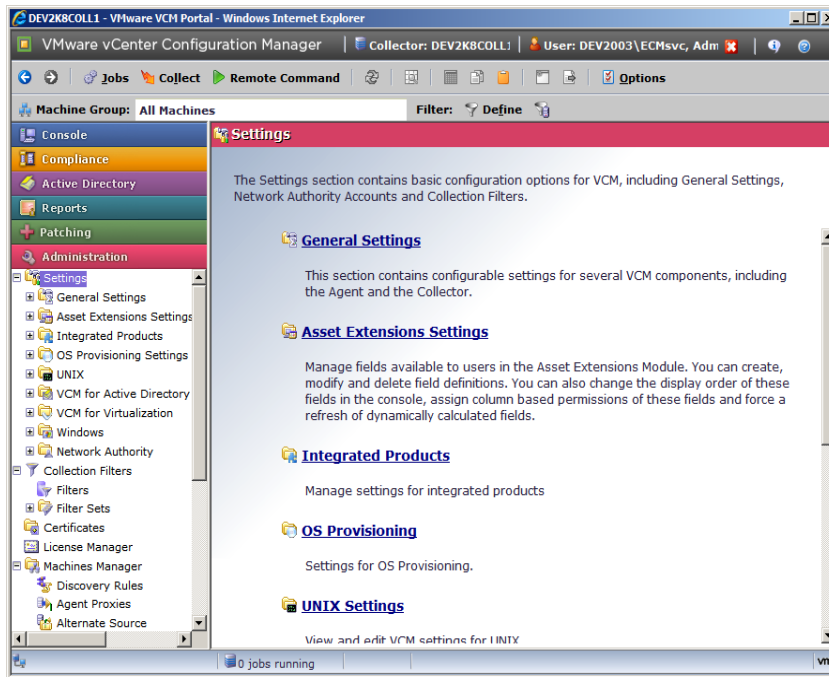
After you have performed the initial setup and familiarized yourself with VCM and its components and tools, VMware recommends that you step through the specific configuration settings for each licensed component and customize them. Additionally, you should perform routine maintenance on your VCM configuration management database (CMDB) just as you would any other SQL database in your enterprise.

Follow the guidance below to keep VCM running smoothly and performing efficiently.

1. [Customize VCM and component-specific settings.](#)
2. [Configure Database file growth.](#)
3. [Configure Database recovery settings.](#)
4. [Create a Maintenance Plan for SQL Server 2008 R2.](#)
5. [Incorporate the VCM CMDB into your backup and disaster recovery plans.](#)

Customize VCM and Component-specific Settings

VCM and its components have configuration settings that should be customized to your environment. VMware strongly suggests reviewing **Administration > Settings** to familiarize yourself with the configuration parameters that you should customize for your environment. You should also specify settings such as data retention and thread priorities for communication with the agent for certain collection types.



In addition to several general global settings, these components have specific settings that should be considered if you licensed the component.

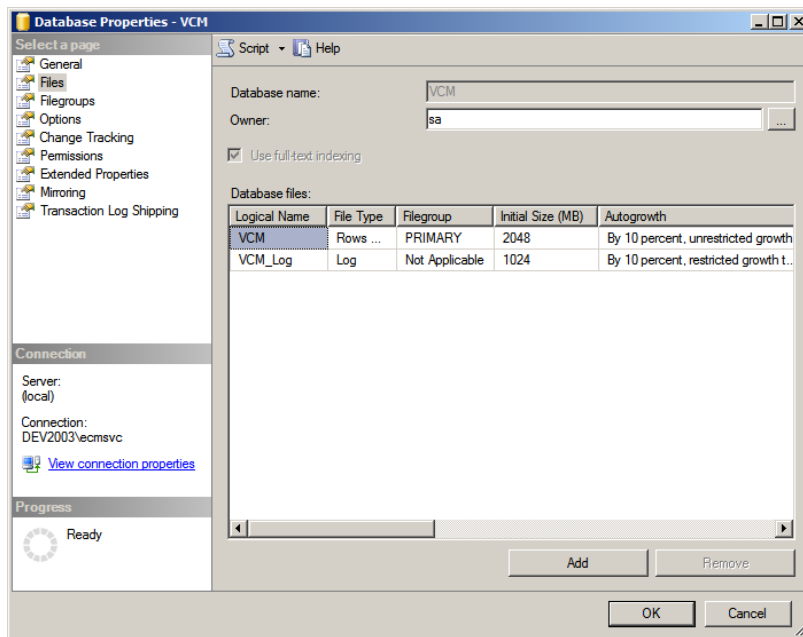
- Asset Extensions (VCMMXA)
- VCM for Active Directory
- VCM for Virtualization
- UNIX
- Windows

For more information on settings specific to these products, see the Help associated with each product. To access the Help for any particular component, navigate to a node within that component and click **Help**.

Configure Database File Growth

After VCM is installed, the installer creates a single 2GB data file and a 1GB log file. As data is added to VCM through normal operations, these files will grow as required. File growth settings are set to the default for Microsoft SQL Server 2008 R2. The default values may result in file fragmentation or sub-optimal performance in some environments. This procedure describes how to set the AutoGrowth property in each database. It is important to set the **AutoGrowth** value properly in each of the databases.

1. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Expand the SQL instance.
3. Expand **Databases**.
4. Right-click **VCM** and select **Properties**.



5. In the left pane, select **Files**.
6. In the **Autogrowth** column, click the ellipsis button.
7. Select **Enable Autogrowth**.
8. In the **File Growth** area, select **In Percent** and type or select **10**. A value of 10% indicates that every time the transaction log file grows it will grow by 10% of its current size. The value is critical in larger environments where the log file can grow large even when using the Simple recovery model. Reserve as much space as possible for your transaction log file so that it does not ever have to grow. This configuration will result in the best performance.
9. In the **Maximum File Size** area, select **Unrestricted File Growth** and click **OK**.
10. Repeat the same procedure for **VCM_Log**.
11. Return to the database list and repeat the above procedures for all VCM-related databases.

Configure Database Recovery Settings

SQL Server supports these recovery models, which you can set differently for each database:

- **Simple.** In Simple recovery, the only information kept in the transaction log is data that is necessary to recover the database to a known good state when the server restarts. It is a misconception that this setting does not cause the transaction log file to grow. In this mode, SQL Server is in what is known as “Auto Truncate” mode, which means that the log file is periodically “rolled over” as data is moved from the log file to the data file. In this mode, transaction log backups are not allowed, and “point in time” recovery is not available. Due to the nature of VCM, use the Simple recovery model for all VMware databases, and use the nightly FULL or INCREMENTAL backups.
- **Bulk Logged.** In Bulk Logged recovery, the transaction log retains all “normal” transaction information and effectively discards transactions that result from a bulk operation. VCM makes extensive use of the IROWSETFASTLOAD interface, which is bulk logged.
- **Full.** In Full recovery, the transaction log retains all information until it is effectively purged through the use of a SQL Server LOG backup operation, which is used when the Database Administrator wants to perform point-in-time recovery. It is also used to allow incremental backups of the database. Factors in VCM weaken the point-in-time recovery model, so do not use point-in-time recovery.

If you decide to implement Full Recovery, you must set up scheduled daily backups of the transaction log. The log files will continue to grow and accumulate changes until they are backed up, so a Full Recovery database without scheduled backups can quickly fill its disk and stop the system.

NOTE VCM database settings are set to Simple by default. If you change the VCM database recovery setting to Full, you must manage your own log backups.

To configure the database recovery settings, follow these steps:

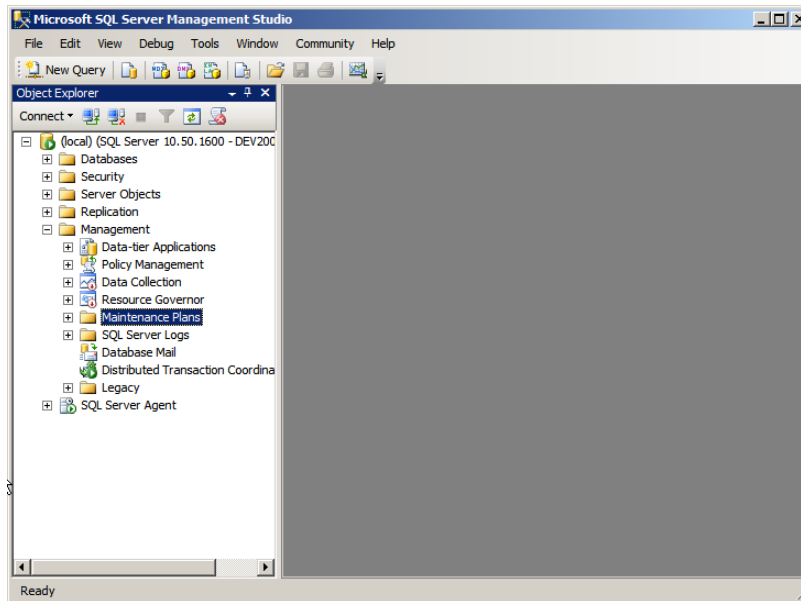
1. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Expand the **SQL instance**.
3. Expand **Databases**.
4. Right-click **VCM** and select **Properties**.
5. Click **Options**.
6. In the **Recovery model** drop-down, select either **Simple**, **Bulk-logged**, or **Full** and click **OK**.

Create a Maintenance Plan for SQL Server 2008 R2

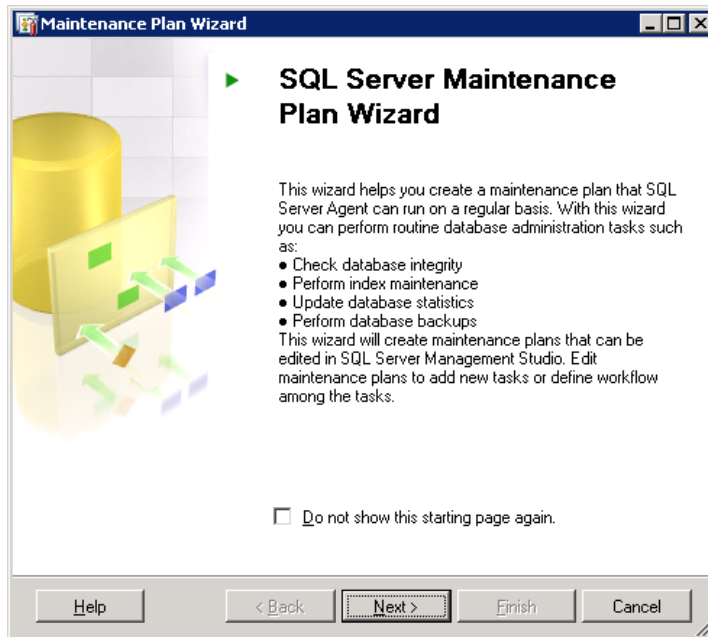
Because VCM relies heavily on its SQL databases for its operation, set up routine maintenance for SQL Server 2008 R2. Set up the automated maintenance functions on SQL Server 2008 R2 servers that host the VCM database to ensure that VCM runs at peak performance and requires little operator intervention during its lifecycle.

Follow these steps to create a maintenance plan for SQL Server 2008 R2.

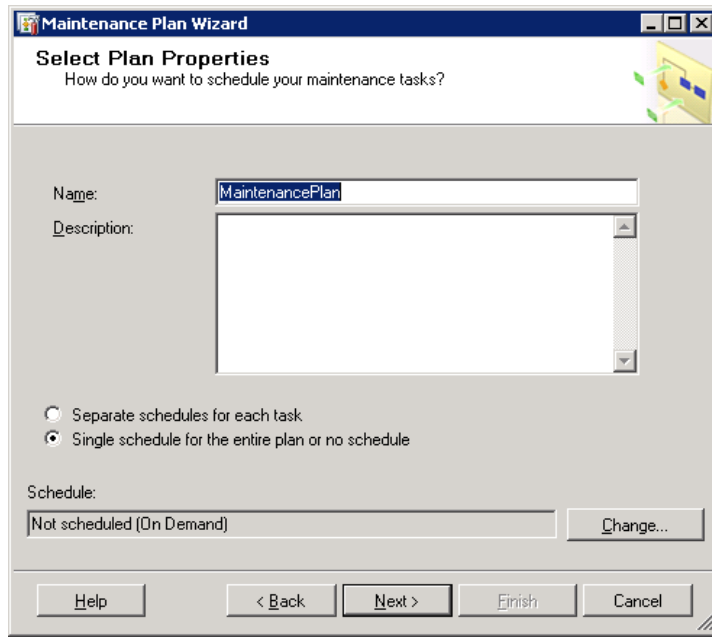
1. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.



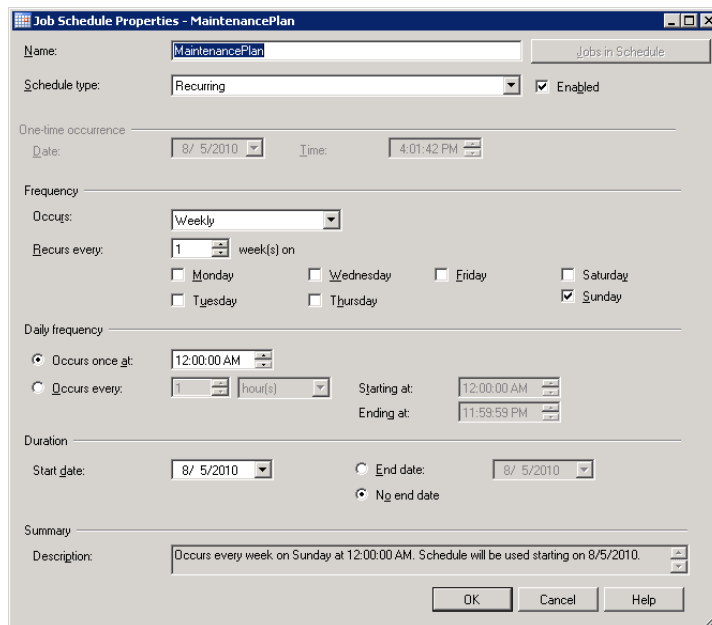
2. Open the **Management** folder, right-click **Maintenance Plans** and select **Maintenance Plan Wizard**.



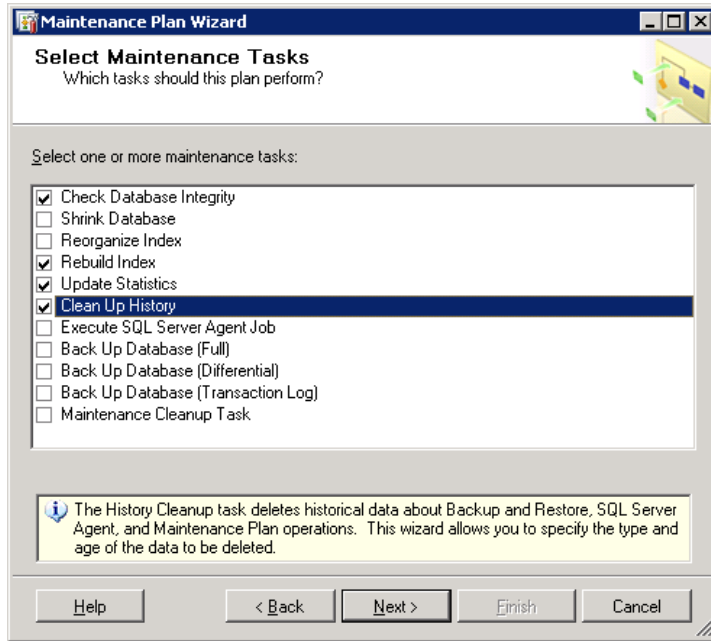
3. Click **Next**. The Select Plan Properties page appears.



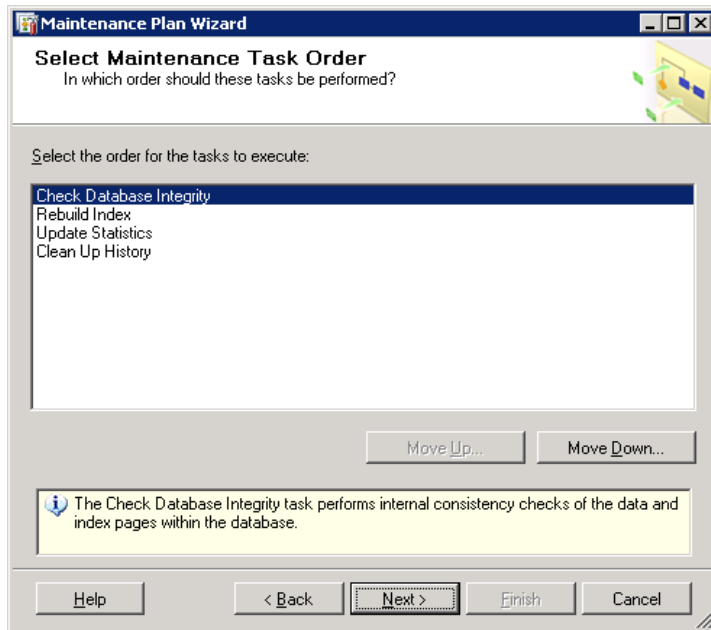
4. Enter a maintenance plan name, select **Single schedule for the entire plan or no schedule**, and click **Change**.



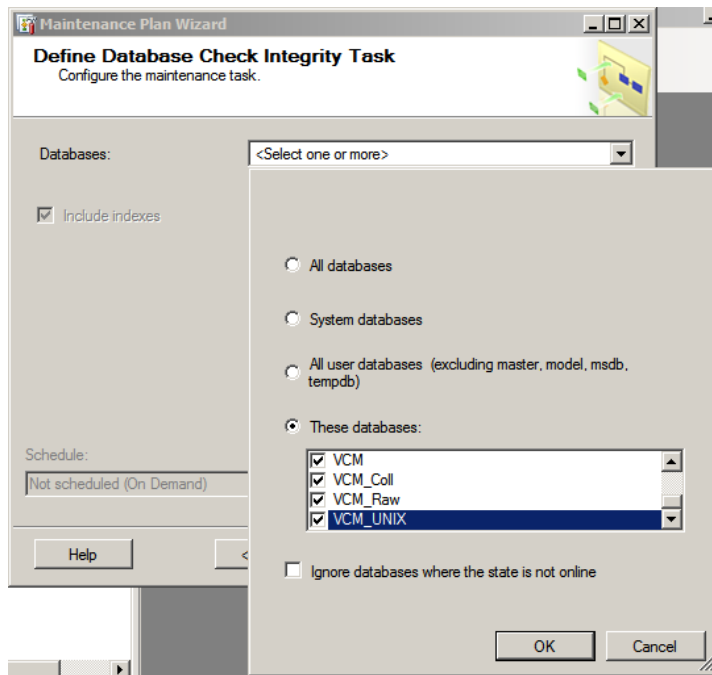
5. In the Job Schedule Properties - Maintenance Plan dialog box, set the scheduling properties for the job, as shown in this example. Schedule the run time when the system is idle or has low usage.
6. Click **OK** to return to the Select Plan Properties page and click **Next**.



7. On the Select Maintenance Tasks page, select the maintenance tasks to be performed, including **Check Database Integrity**, **Rebuild Index**, **Update Statistics**, and **Clean Up History**, and then click **Next**.

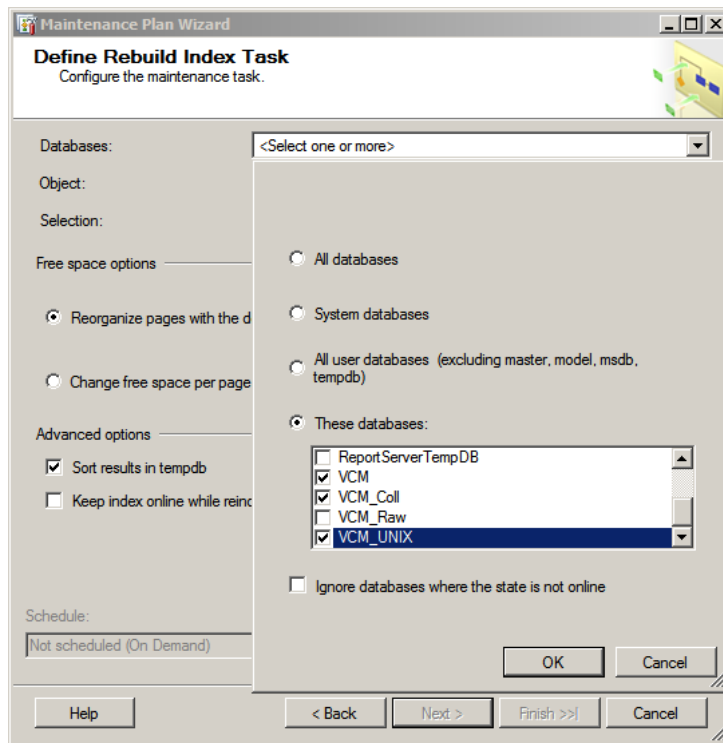


8. On the Select Maintenance Task Order page, specify the order for the maintenance tasks to be performed and click **Next**.



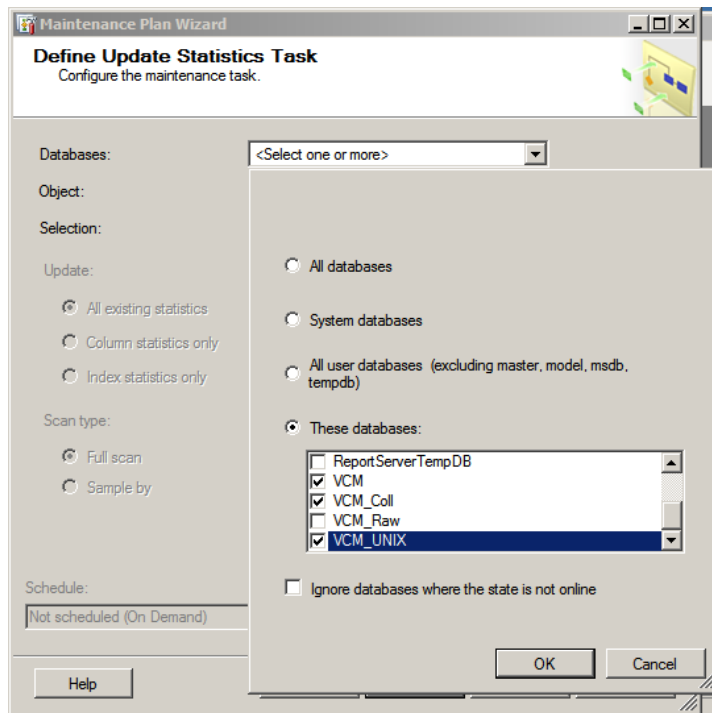
9. On the Define Database Check Integrity Task page, click the Databases drop down menu and select the CSI_Domain, VCM, VCM_Coll, VCM_Raw, and VCM_UNIX databases and click **OK**. When the databases are selected, **Specific databases** appears in the Databases field. Check the option **Include indexes** and click **Next**.

NOTE It is important to select the VCM_Raw database because it contains transient data that is consumed by the other databases.

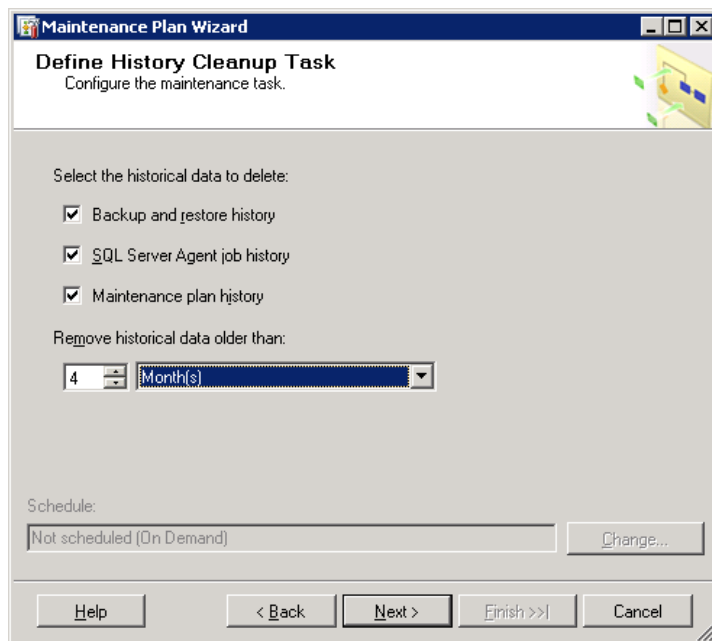


10. On the Define Rebuild Index Task page, specify how the Maintenance Plan should rebuild the Index. Click the Databases drop down menu, select the CSI_Domain, VCM, VCM_Coll, and VCM_UNIX databases, and click **OK**. When the databases are selected, **Specific databases** appears in the Databases field. In the **Advanced options** area, select **Sort results in tempdb** and click **Next**.

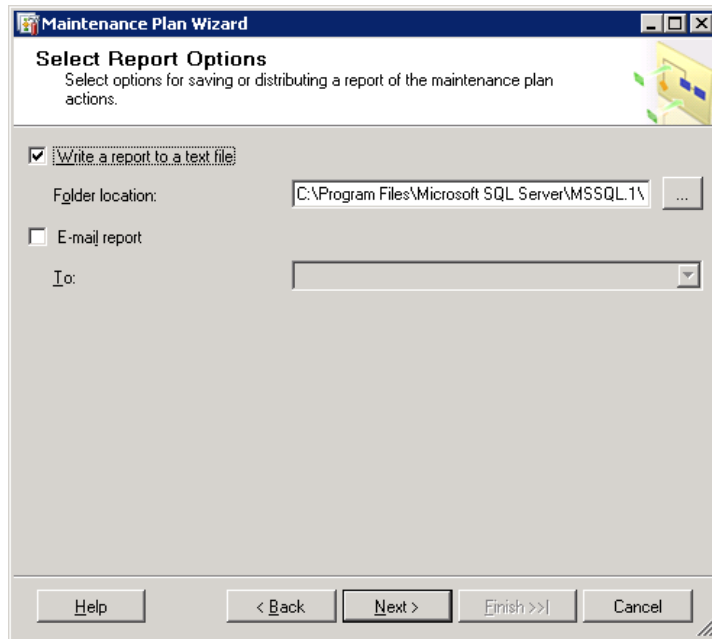
NOTE It is not necessary to rebuild the Index for the VCM_Raw database.



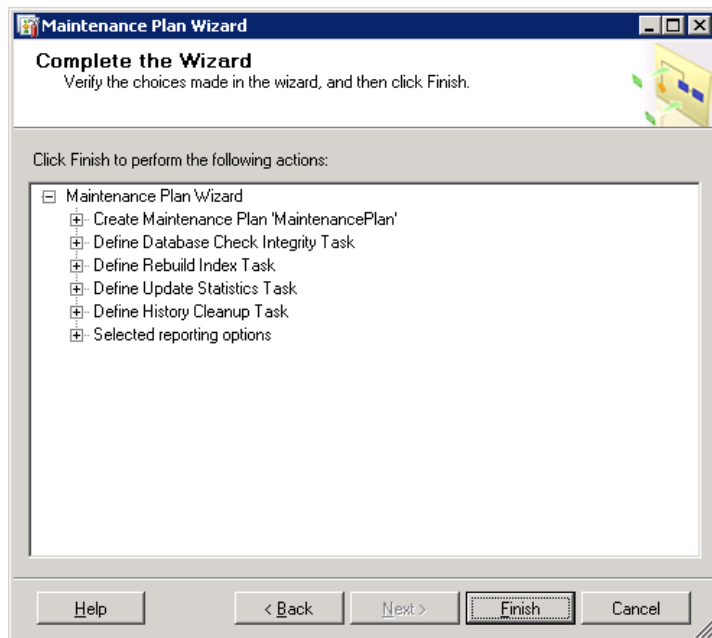
- On the Define Update Statistics Task page, specify how the Maintenance Plan should update the database statistics. Click the Databases drop down menu. Select the CSI_Domain, VCM, VCM_Coll, and VCM_UNIX databases, and then click **OK**. When the databases are selected, **Specific databases** appears in the Databases field. Click **Next**.



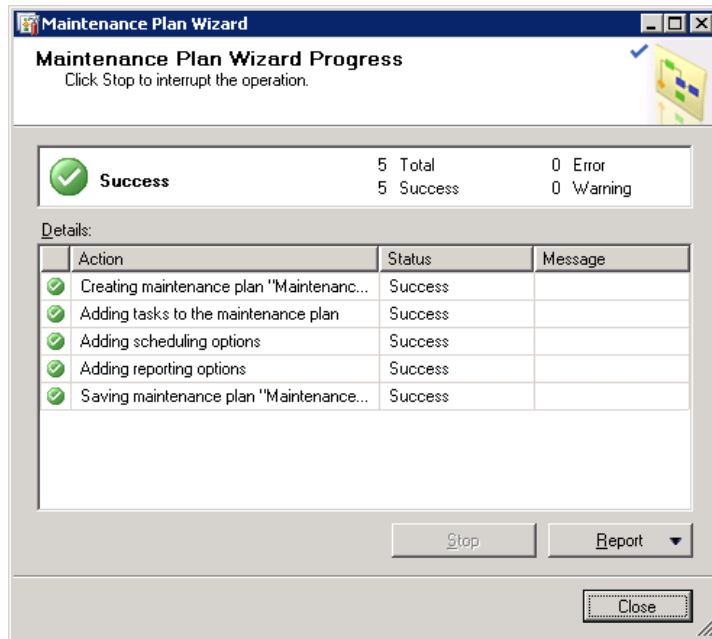
- On the Define History Cleanup Task page, select the historical data to be removed from the SQL Server 2008 R2 machine and set the **Remove historical data older than** option to **4 months** and click **Next**.



13. On the Select Report Options page, select **Write a report to a text file**, specify the folder location to save a record of the maintenance plan actions for future reference, and click **Next**.



14. On the Complete the Wizard page, verify the selections in the Maintenance Plan Wizard and expand the tree selections to view the settings, and click **Finish**.



15. When the Maintenance Plan Wizard completes, verify that the actions were successful.
16. To view, save, copy, or send the report, click **Report** and select an option.

You have now established a routine maintenance plan to assure that SQL Server 2008 R2 continues to operate efficiently.

Incorporate the VCM CMDB into your Backup and Disaster Recovery Plans

Consider your VCM CMDB as any other SQL database in your environment, and incorporate the CMDB into your corporate strategy for Backup and Disaster Recovery.

Troubleshooting Problems with VCM

This chapter provides important information that will help you troubleshoot issues that may occur during the VCM software installation, upgrade, or use. This chapter describes how to resolve the following issues:

- [Missing Patch Assessment Results](#)
- [Reports and Node Summaries Problems](#)
- [Protected Storage Errors](#)
- [Resetting the Require Secure Channel \(SSL\)](#)
- [Report Parameter Error](#)

In addition to the following information, the *VCM Troubleshooting Guide* is available on the VMware Web site at http://www.vmware.com/support/pubs/vcm_pubs.html.

Evaluating Missing UNIX Patch Assessment Results

Before you can install patches, VCM Patching for UNIX patch assessments must complete successfully by displaying the assessment results. If a UNIX patch assessment does not return any results, the problem may be due to one of the following reasons.

- The assessment template may contain patch bulletins that do not match the selected machine type.
- The selected patch may not match the machine architecture; you must select 32-bit patches for 32-bit machines, and 64-bit patches for 64-bit machines.
- If you have defined a custom filter for Patch Assessment, it may not be including any of the bulletins that apply to the selected machine type. Certain filter attributes may not apply to bulletins across all platforms. For example, Severity is not used by some platforms. If you have defined a filter based on Severity, you would not include in your assessment any bulletins that do not have Severity set.
- The bulletins may not be in the required location on the Agent machine, which could occur for several reasons. Review the following list, and then check your UNIX Agent machine to confirm whether the bulletins exist in the correct location. Consider updating your UNIX Agents to 5.4.
 - The Agent version and UNIX platform support for Patch Assessment may not match.
 - Agent versions prior to 5.0 do not support UNIX Patch Assessment.
 - Support for Patch Assessment was added for some UNIX platforms in 5.0, but the patch assessment required manual distribution of bulletin information to the UNIX Agent machine to perform the assessment.

- Support for additional UNIX platforms was added in 5.1, along with the automated distribution of bulletin information to Agent machines.
- The process of distributing the bulletin information to UNIX Agent machines has failed.
- The bulletin information was removed from the UNIX Agent machine.
- Bulletin information may not be loaded on your Collector. If the Check for Updates action is indicating that no updates are available, then try the **Force** option on **Check for Updates**.
- An upgrade of the Collector to 5.4 failed to reprocess the bulletin information in order to extract the necessary information required for filtering. This step should have occurred automatically during the upgrade. Executing **Check for Updates** with the **Force** option might correct this problem.
- On older agents such as VCM 5.1 and earlier, a **Machines - General** collection has not been done. Support for custom filters for UNIX Patch Assessment has been added to VCM, and can be used when assessing older agents. However, when assessing older agents such as 5.1 and earlier, you must have collected the **Machines - General** data class in order for the assessment to succeed. With the 5.1.x or later Agent, a **Machines - General** collection is not required.

Resolving Reports and Node Summaries Problems

After installing or upgrading VCM, problems with Visual Studio 2005 and the .NET Framework may occur and the following messages might appear:

- Server Unavailable
- The web application you are attempting to access on this web server is currently unavailable.
- Client found response content type of "text/html", but expected "text/xml".
- No results returned for specified parameters. This error may occur even if the reports run and part of the report appears.

To Resolve the Problem

If any of these messages occurs, follow the steps below.

1. Access the Microsoft Web site.
2. Search for the Knowledge Base article: KB913384. This article describes a hotfix for the following problem: A .NET Framework 2.0 application that runs under a user account context when no user profile is associated with the user account context may crash, or you may receive an access violation error message.
3. Download the hotfix that is applicable to your machine.
4. After you apply this hotfix, you must restart the machine.

Resolving Protected Storage Errors

When attempting to generate key pairs on the Agent Proxy machine, a protected storage error may occur. For example:

```
CsiCommProxyUtil:wmain(): Failed to get protected storage for VCMv. HRESULT 0x8009000b =
Key not valid for use in specified state.
```

If you encounter this type of error, use this workaround to resolve the problem.

1. Open a command prompt.
2. Navigate to the `C:\Program Files (x86)\VMware\VCMAgentData\protected` directory, and delete these files: `ECMv.csi.pds` and `ECMv.csi.pds.lock`.
3. Execute the following command: `GenerateAgentProxyKeys.cmd`.
4. Verify that the following files were generated:


```
<machine>_securecomm_public_key.txt
<machine>_ssh_public_key.txt
```
5. From the command prompt, execute the following command: `DatabaseUploadKey.cmd`
`<machine>_securecomm_public_key.txt` (where `<machine>` is the name of the Agent Proxy machine).

For more information about generating key pairs on the Agent Proxy Machine, see the Getting Started with VCM chapter.

Resetting the Required Secure Channel (SSL)

When using SSL on the VCM collector, the following settings must be configured for VCM to work properly with SSL:

- Web.config file in the WebConsole directory
- Require secure channel (SSL) setting in IIS – for the VCM virtual directory
- IIS HTTP string http or https Database setting in VCM

When upgrading the Collector, the Require secure channel (SSL) check box in the VCM virtual directory properties may become unchecked. This problem can occur on a VCM Collector that is using SSL, when all of the settings listed above have been configured.

After upgrading VCM, log in and verify whether https is still required. If not, confirm that the settings to the Web.config configuration file, the VCM virtual directory, and the IIS settings are correct by using these procedures.

Updating the VCM Virtual Directory

To update the VCM virtual directory, follow these steps:

1. Access Internet Information Services by opening a command prompt, and then typing `compmgmt.msc`.
2. Expand the **Services and Applications** node and expand **Internet Information Services > Web Sites > Default Web Site**.
3. Right-click the VCM virtual directory, and select **Properties**.
4. In the VCM Properties dialog box, click the **Directory Security** tab, and in the **Secure Communications** panel, click **Edit**.
5. In the Secure Communications dialog box, check the **Require secure channel (SSL)** check box, and click **OK** twice to save the virtual directory properties.

Updating the IIS Settings in VCM

To modify the IIS settings in VCM, follow these steps:

1. Log into VCM and select **Administration > Settings > General Settings > Database**.
2. In the Database settings, click to highlight the setting labeled **IIS HTTP string http or https**.
3. Click **Edit Setting** and change the IIS HTTP string setting to **https**.

After performing these steps, you can operate VCM through a secure channel.

Resolving a Report Parameter Error

After upgrading VCM, if you encounter a problem with a report, your report may not have been uploaded correctly. This error can occur when reports have been overwritten, rather than removed in Report Manager. If the parameter values for the report have changed, the changes may not have been acknowledged by Report Manager when the report was uploaded and overwritten.

Before uploading the report again, you must first remove the existing version. To remove the existing report, follow the steps below. This procedure will create a new report instance in Report Manager.

1. Open Report Manager on the VCM Collector by entering `http://collectorname/Reports`.
2. Open the folder where the affected report resides. The VCM Reports labeled ECM Reports, folders are as follows:
 - **ECMAD:** Active Directory
 - **ECMu:** UNIX
 - **RSCA:** RSCA
 - **Service Desk:** Service Desk and Change Reconciliation
 - **SMS:** SMS
 - **Standard:** Windows reports and Change Management and Compliance
 - **SUM:** VCM Patching
 - **Virtualization:** Virtualization
3. Click the **Show Details** button on the right hand of the screen.
4. Click the check box next to the affected report.
5. Click the **Delete** option. You will be prompted to be sure that you want to delete this item. Click **OK**.
6. Click **Upload File**.
7. On the **Upload File** screen, next to the **File to Upload** text box select **Browse**.
8. Select the report from the reports directory.
9. Click **OK**.

The report now includes all of the new parameter modifications.

Index

%			
%Systemroot% environment variable	79		
A			
About Patching	161		
about this book	11		
access by user	61		
accessing			
compliance content	231		
account			
application services	16		
collector services	16		
network authority	15		
Oracle collection user	125		
active directory			
(AD)	213		
agent	217		
collection results	227		
configuration	221		
data collection	225		
domain controllers	213		
getting started	213		
network authority account	215		
reference information	230		
run determine forest action	222		
run setup DCs action	223		
AD (active directory)	213		
adding			
assets hardware configuration	205		
assets software configuration	207		
Mac OS X	111		
Oracle Instances	124		
repository sources	194		
UNIX machines hosting Oracle	124		
UNIX/Linux machines	97		
administration			
rights	15		
ADProductInstall.exe for Windows	79		
agent			
active directory	217		
ADProductInstall.exe for Windows AD	79		
binaries per OS	100, 113		
CMAgentInstall.exe for Windows	79		
installation	18, 77		
installation, manually	78		
installation, Oracle	124		
installing			
Mac OS X	113		
platforms supported	55, 99		
proxy			
platform not supported	57		
upgrading	57		
upgrading manually	58		
uninstall, Mac OS X	118		
uninstall, UNIX/Linux	105		
uninstalling	80		
UNIX upgrade	55-56		
upgrading	53		
upgrading for UNIX	54		
agent communication			
changing after OS provisioning	182		
agents			
certificates	18		
AgentUpgradeLocal.sh for UNIX	55		
application services			
account	16		
assets			
configuration items	201		
getting started	201		
hardware configuration items	205		
software configuration items	207		
auditing	131		
authentication			
server	17		
automatic upgrade			
Remote client	54		
B			
backup/disaster recovery plan	248		
binary mode, use for ftp	100, 113		
broadband	149		
C			
certificates			
agents	18		
collector	17		
enterprise	17		
Enterprise Certificate	79		
PKI	79		
secure communication	16		
change detection			
WCI	90		
check			
for UNIX/Linux updates	169		
for Windows updates	165		
CMAgentInstall.exe			
for Windows	79		
uninstalling agent	80		
collect			
package managers	193		
repositories	193		

collection results			
AD	227		
Oracle	129		
Remote	159		
UNIX/Linux	107		
virtualization	143		
collection scripts			
custom for WCI	93		
collection user account			
creating, Config User Action	125		
creating, remote command	126		
Oracle	125		
collections			
active directory	225		
AD	220		
exploring, Windows	84		
Mac OS X	119		
Oracle	129		
patching	166		
Remote	159		
results, Mac OS X	121		
troubleshooting vCenter Server	138		
UNIX/Linux	106		
vCenter Server data	135, 137		
virtualization	142		
WCI	89		
Windows machines	83		
collector			
aware of Remote client	158		
certificates	17		
importing content	231		
install before agents	99, 113		
lock request	79		
collector services			
account	16		
compliance			
checking Windows	87		
checking, UNIX/Linux	107		
content, accessing	231		
imported content	231		
Mac OS X	121		
rule			
remediation			
software provisioning	197		
software provisioning	196		
components			
getting started	61		
configurations			
AD	221		
assets	201		
database file growth	239		
installation	14		
modifying hardware, assets	202		
modifying software, assets	204		
configuring			
popup blocker	62		
vSphere Client Plug-in	144		
content for compliance	231		
importing to collector	231		
location	231		
wizard	234		
copying			
files to ESX/vSphere servers	141		
creating			
Oracle collection user account	125-126		
csi.config file	101, 104, 114, 117		
CSI_AGENT_RUN_OPTION	104, 117		
custom filter sets			
for Remote	158		
customization			
component settings	237		
for your environment	130		
D			
database			
backup/disaster recovery plan	248		
recovery settings	240		
deploying			
AD agent	217		
AD to domain controllers	221		
patches, UNIX/Linux	173		
patches, Windows machines	168		
determine forest action			
running for AD	222		
developing			
custom collection scripts	93		
dialup	149		
disabling			
UAC on Windows machines	77, 81		
disaster recovery plan	248		
discovering			
domain controllers, AD	215		
Oracle Instances	124		
Windows machines	69, 72		
domain controllers			
active directory	213		
deploying AD	221		
domains			
active directory	213		
AD, confirming presence	214		
verifying	69		
E			
enabling			
popup blocker	62		
enterprise			
certificates	17		
environment variable, %Systemroot%	79		
ESX and ESXi			
configure after provisioning	181		
ESXi	134		
exploring			
AD collection results	227		
assessment results, UNIX	171		
assessment results, Windows	167		

collection results			
Oracle	129	agent on Red Hat, SUSE	99
UNIX/Linux	107	agent on UNIX/Linux machines	99
virtualization	143	agent on Windows machines	77
Windows	84	agent, manually	78
imported content	231	agent, UNIX	100, 113
Remote collection results	159	check prerequisites	15
		configurations	14
F		foundation checker	234
filter sets		maintenance after	237
imported content	231	navigating	21
in Remote settings	158	preparing	13
Remote	158	prerequisites	15
forest		Remote client	151
run determine forest action	222	command line	153
forests		remote command	154
active directory	213	tools	15, 233
foundation checker	233	understanding configurations	14
installation	234	using installation manager	14
ftp, use binary mode	100, 113	InstallICMAgent	103, 116
		installing	
G		Package Manager for Windows	190
getting started	69	Package Studio	188
active directory	213	packages	195
assets	201	repositories	187
auditing	131	integration	
components, tools	61	Service Desk	209
deploy patches, UNIX/Linux	173	invalid certificate in vSphere Client	
deploy patches, Windows	168	troubleshooting	146
explore assessment results, UNIX	171	J	
explore assessment results, Windows	167	job manager	233
launch assessment	166	job status reporting	
launching	62	WCI	90
logging on	62	jobs history	
patching collection	166	provisioning	196
Remote	149	L	
tools	233	LAN	149
virtualization	133	launch an assessment	166
vSphere Client Plug-in	145	launching	
WCI	88	content wizard	231
WCI PowerShell scripts	91	license	
Getting Started		Windows machines	69
Using Patching	165	licensing	
H		AD agent	217
HTTP agent, port number	79	Mac OS X	112
		UNIX/Linux machines	98
I		Windows machines	75
IIS settings		local package	
updating	251	UNIX agent upgrade	55
import/export wizard	234	location for compliance content	231
importing content		lock request, submit from collector	79
content wizard	231	M	
information bar in portal	64	Mac OS X	
install		adding	111
Windows machines	69	agent	
installation		installing	113
agent	18	agent, uninstall	118
agent on Mac OS X machines	113		

collection	119	permissions	
collection results	121	Oracle	128
licensing	112	planning maintenance	240
maintenance		platforms	
after installation	237	agent proxy support	57
backup/disaster recovery plan	248	UNIX agent support	55, 99
configure database file growth	239	popup blocker	
create plan	240	configure or enable	62
customize settings	237	port number for HTTP agent install	79
database recovery settings	240	port number for UNIX agent install	105, 118
migrating	45	portal	
modifying		familiarizing	63
assets hardware configurations	202	information bar	64
assets software configurations	204	sliders	65
		toolbar	64
N		PowerShell	
network authority account	15	executing for WCI	92
AD	215	for Windows Custom Info	88
checking	70	scripts, troubleshooting	96
node summaries		signing scripts for WCI	92
resolving problems	250	WCI getting started	91
		prerequisites	
O		check for installation	15
operating systems		for upgrading	46, 48
agent binaries	100, 113	vCenter Server collections	135
Oracle		Product Overview	161
10g installations	128	protected storage	
Add/Edit Instance	124	resolving problems	250
adding instances	124	provision machines	
agent installation	124	operating systems	180
collection results	129	provisioning	
collection user account	125, 128	compliance	
collections	129	remediation	197
Config User Action	125	compliance rule	196
discovering instances	124	install agent	18
permissions	128	jobs History	196
reference information	129	provisioning, operating system	177
remote command	126	agent communication	182
Oracle Database		collect distributions	179
Removing access	127	components	177
overview		configure ESX and ESXi	181
vSphere Client Plug-in	143	discovery	179
		provision machines	180
P		re-provision machines	182
Package Manager for Windows		workflow	178
installing	190	Public Key Infrastructure (PKI)	79
package managers		purge	
collect	193	for WCI	90
Package Studio		R	
installing	188	re-provisioning machines	
packages		operating systems	182
importing content	231	recovery plan	248
installing	195	Red Hat	
patching		install UNIX agent	99
check for updates, UNIX/Linux	169	Red Hat workstations	
check for updates, Windows	165	upgrading	54, 98
collection	166	reference information	
UNIX assessment results troubleshooting	249	AD	230

assets	208	remote	158
Oracle	129	setup DCs action	
Service Desk	211	running for AD	223
registering		signing	
vSphere Client Plug-in	59, 143, 145	PowerShell scripts	92
remediation		sliders	
compliance rule		in portal	65
software provisioning	197	sources	
Remote		repository sources	
collection results	159	adding	194
collections	159	SQL*Plus	
filter sets	158	Oracle	128
getting started	149	SSL	
settings	158	resetting required secure channel	251
filter sets	158	SUSE	
virtual directory	16	install UNIX agent	99
Remote client		T	
automatic upgrade	54	templates	
collector aware	158	for compliance	231
installing	151	ToCMBase64String	93
command line	153	toolbar	
remote command	154	in portal	64
remote package		tools	
UNIX agent upgrade	56	foundation checker	233
repairing		getting started	61, 233
uninstall, troubleshooting	22	import/export, content	233
reports		installation	15, 233
parameter error, resolving	252	job manager	233
resolving problems	250	troubleshooting	249
WCI	91	PowerShell scripts	96
repositories		vCenter Server data collections	138
collect	193	U	
installing	187	UAC	
repository sources		disabling on Windows machines	77, 81
adding	194	uninstall	
resetting		agent	80
required secure channel (SSL)	251	agent, Mac OS X	118
resolving reports parameter error	252	agent, UNIX/Linux	105
results		troubleshooting	22
collection, Mac OS X	121	UNIX agent	
imported content	231	platform support	55, 99
virtualization	143	port number	105, 118
rights		upgrading	54
administration	15	local package	55
running		remote package	56
determine forest action for AD	222	UNIX/Linux	
setup DCs action for AD	223	agent uninstall	105
S		AgentUpgradeLocal.sh	55
scripts		assessments results, troubleshooting	249
PowerShell	91	check for updates	169
secure communication	16	collections	106
server		machines, adding	97
authentication	17	machines, licensing	98
Service Desk integration	209	updates	
settings		check for content wizard	236
customizing for components	237	check for UNIX/Linux	169
database recovery	240		

check for Windows	165	discover, license, install	69
updating		discovering	72
IIS settings	251	install agent	77
virtual directory	251	licensing	75
upgrading	45	uninstalling agent	80
agent	53	wizards	
agent proxy	57	content	234
agent proxy manually	58	import/export	234
automatic	54	workstations	
failed, troubleshooting	22	upgrading Red Hat	54, 98
Red Hat workstations	54, 98		
UNIX agent	54		
local package	55		
remote package	56		
virtualization	56		
vSphere Client Plug-in	59, 145		
user access	61		
V			
vCenter Server	135		
data collections	135, 137		
VCM Summary and VCM Actions tabs are not displayed in vSphere Client			
troubleshooting	147		
verifying			
domain controllers, AD	217		
domains	69		
virtual directory			
Remote	16		
updating	251		
virtualization			
collecting	142		
results	143		
collections	142		
getting started	133		
upgrading	56		
vSphere Client Plug-in			
configuring	144		
getting started	145		
overview	143		
registering	143		
upgrading	59, 145		
W			
WCI			
change detection	90		
collection	89		
custom collection scripts	93		
executing PowerShell scripts	92		
getting started	88		
job status reporting	90		
purge	90		
running reports	91		
Windows			
check for updates	165		
Windows Custom Information (WCI)	88		
Windows machines			
collecting	83		
disabling UAC	77, 81		