VMware vCenter Configuration Manager Security Guide

vCenter Configuration Manager 5.5

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-000683-00

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

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

Contents

About This Book

The *VMware vCenter Configuration Manager Security Guide* describes how to harden vCenter Configuration Manager (VCM) for secure use.

Parts of this document describe assumptions made in the design and operation of VCM. For example, the guarantees regarding VCM logins assume that the domain controller for each user is trusted. Other parts of this document describe specific, nondefault hardening requirements that you must apply.

Intended Audience

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

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

Document Feedback

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

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.

1 Introduction to VCM Security

To understand VCM security requirements, familiarize yourself with the overall security environment, VCM components, VCM personnel roles, and trust zones.

VCM Security Environment

VCM operates in the context of a security environment, which involves system configuration, personnel and usage assumptions, organizational security policies, and best practices. Security requirements are met either by controls built into VCM that leverage the security environment or by controls built into the environment itself. When a security requirement is not met, the confidentiality, integrity, or availability of information assets that flow through the deficient system are at risk.

A healthy security environment assumes or provides certain guarantees:

- Trust in, and training for, your authorized VCM users
- Protection of VCM installation kits from tampering
- Protection of current VCM systems from access by unauthorized users
- Proper decommissioning of outgoing VCM systems

To establish proper security, you must prepare and apply security requirements across the following equipment:

- The server that acts as the VCM Collector
- The VCM SQL Server and database system
- The VCM Web server
- The VCM user interface Web browser
- Systems on which the VCM Agent runs
- The domain, its supporting infrastructure, and user accounts

VCM Components

VCM is a distributed application with several physical and conceptual components:

- Collector service that processes requests and receives results
- SQL Server database that stores results and application control information
- Internet Information Services (IIS) Web server that hosts the UI Web application and accepts work requests
- Browser-based user interface (UI) that renders in Internet Explorer (IE) on user desktops
- Agents that inspect managed machines and return results in response to requests

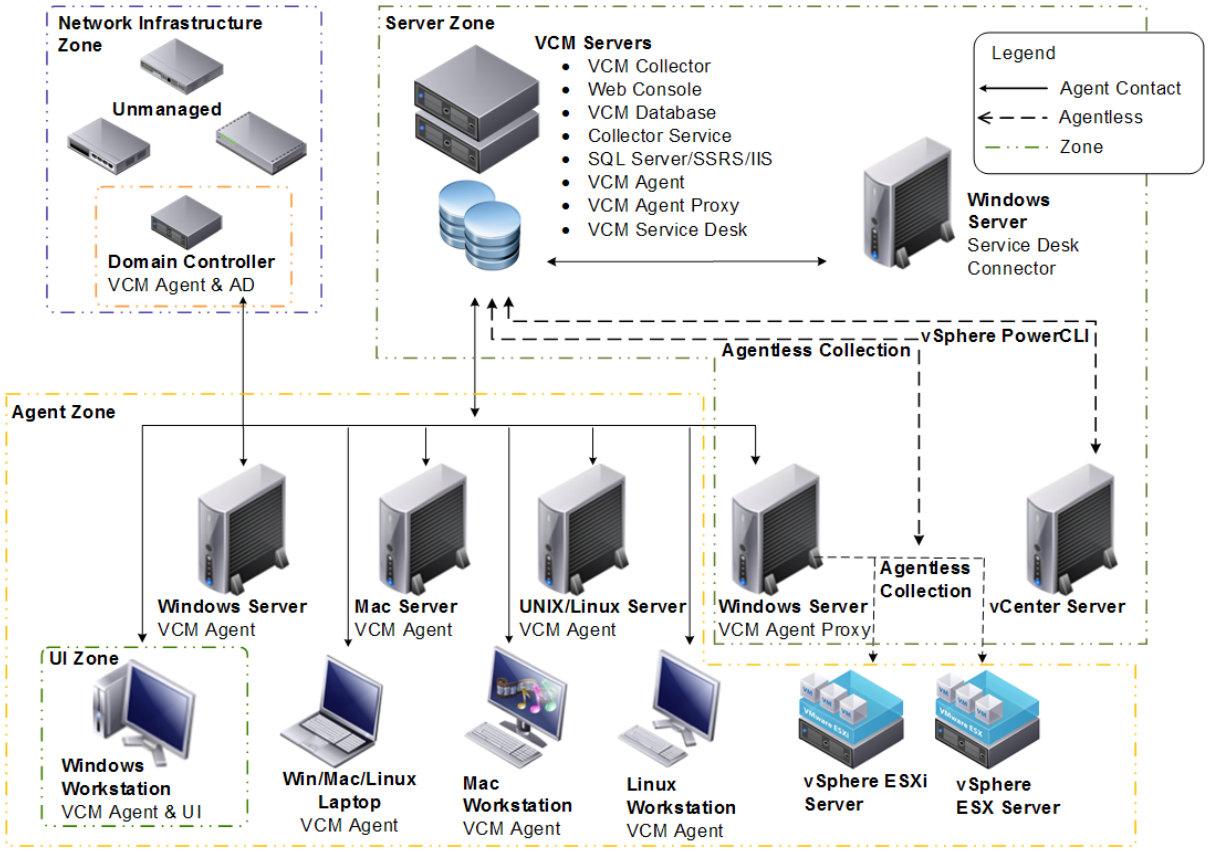
In some installations, optional components might also be present:

- An Agent proxy that works with ESX, ESXi, and vSphere servers
- An orchestration system that coordinates with service desk applications such as Remedy
- A VCM Remote service
- Operating system provisioning components
- Software provisioning components
- Alternative source file servers that store VCM installation kits and VCM Patching patches

With the exception of the UI, Agent, alternative sources, and OS Provisioning Server, all VCM components run on Microsoft Windows Server systems. The UI runs in Internet Explorer on Windows desktops. The Agent executes on either Windows or UNIX systems, including Linux, Solaris, HPUX, AIX, and Max OS X. An alternative source can be any file server that exports shares or FTP.

The following figure shows VCM components, with the exception of provisioning and alternative sources. Provisioning component areas appear in their respective chapters.

Figure 1–1. VCM Components and Zones



CAUTION Any system that participates in your VCM environment can contain sensitive data, or it can hold authentication keys that can grant access to sensitive data on other systems. Never reuse or dispose of VCM systems without proper decommissioning as described in "Decommissioning" on page 53.

As shown, a combination of VCM services can share one system. In a single-machine installation, the Collector, SQL Server, IIS Web server, and Web application are installed on one system. Optional split installation configurations support running the SQL Server and database on a separate system and the IIS Web server on a separate system.

How Personnel Use VCM

Different personnel use the features of VCM.

- Domain administrators create the accounts and manage the infrastructure in which VCM runs. The infrastructure includes domain controllers, routers, certificate servers, SMTP email servers, domain name services (DNS), and dynamic host configuration protocol (DHCP) servers.
- A VCM installer loads the VCM software and configures the Collector, SQL Server, IIS, and other services. The installer is also the first VCM administrator and is responsible for authorizing other administrators and regular VCM users from the inventory of accounts that the domain administrators

- VCM users and administrators log in to VCM and use its Web interface to administer managed machines using the Agents, run compliance tests, and generate reports. VCM administrators, users, or managed machine administrators can install, upgrade, and uninstall Agents.

Trust Zones

Conceptually, VCM components are organized into trust zones. The zones and boundaries are for ease in understanding VCM security and are not related to zones in Internet Explorer or your domain, nor are they cited anywhere in the VCM user interface.

- **Infrastructure**. Domain controllers, routers, SMTP servers, DNS servers, and other infrastructure items
- **User interface**. VCM user desktops
- **Server**. Collector service, SQL Server, IIS, Web application, Agent proxy, software provisioning repository, VCM Remote service, and Orchestrator
- **Agent**. Managed machines and alternative sources

  Multiple Agent zones are supported.
- **Operating system provisioning**. OS Provisioning Servers, provisionable targets, and the network infrastructure that connects them

Domain administrators manage the infrastructure, user interface zone, and server zone. A local zone administrator controls each Agent zone. This administrator is often the administrator of the managed machine or repository.

The zones help you understand the trust between VCM components at a more detailed level than by domain controller domains alone. A trust boundary separates each zone. Without special configuration or authentication, the machines and services in one zone distrust the machines and services in another zone. Special configuration can establish implicit trust, and authentication can establish trust between components that are not configured for implicit trust.

When an entire zone trusts another zone, every VCM component in the first zone implicitly trusts every component in the second zone. If two machines reside in the same zone, they do not necessarily trust each other, but rather they are not required to distrust each other by default. After you install VCM, the user interface and Agent zones trust the infrastructure and server zones.

The server zone trusts only the infrastructure zone, and does not trust the user interface zone except as a source of user interface commands from VCM users authenticated by the infrastructure. The server zone trusts the Agent zone as a source for Agent data, but not to provide data or implement change that would affect other Agents or the VCM configuration.

System Guidelines Across Zones

There are certain security requirements in this document that apply across more than one zone. The following table summarizes them in case you want to make these wider configuration changes in one pass through your security environment.

Table 1–1. Zones and Requirements

Requirement	Infrastructure Zone	Server Zone	UI Zone	Agent Zone
Cryptographic service providers are FIPS-140 validated.		X	X	
Only trusted software is installed in the zone.	X	X	X	

Requirement	Infrastructure Zone	Server Zone	UI Zone	Agent Zone
Access to machine configuration settings is restricted.	X	X	X	X
Routine backups, patches, and virus scanning are performed.	X	X	X	X

The provisioning zone is not listed in the table. For provisioning details, see "Software Provisioning Components" on page 45 or "Operating System Provisioning Components" on page 49 .

Domain Infrastructure 2

Securing the domain infrastructure for use with VCM involves configuring the domain controller, network infrastructure services, network infrastructure systems, certificates, accounts, and personnel.

Using VCM to Manage Infrastructure Zone Systems

After you install VCM, your first course of action should be to manage infrastructure zone systems in VCM and subject them to assessment. VCM comes with compliance rules for domain controller best practices, domain controller health, and other settings that are valuable in domain infrastructure zones. In addition, you can create your own templates and rules.

The rest of this chapter briefly explains the infrastructure zone security hardening steps to pursue, either manually or, if possible, through compliance rules.

Infrastructure Zone Machine Group

For the settings that you can apply using VCM, having the infrastructure systems in their own, dedicated machine group provides a way of managing the systems and synchronizing their settings.

For example, you prevent non-VCM administrators from having administrator access to infrastructure systems by placing all infrastructure systems in the dedicated machine group and configuring the group to be accessible only to VCM administrators.

Domain Controller

VCM relies on a domain controller in order to perform the following functions:

- Authenticate VCM users
- Discover machines to manage
- Enumerate domain group members
- Run VCM services under Network Authority accounts
- Authenticate administrators who control the systems on which VCM and its databases are installed

As the VCM installer and administrator, you identify the domain controller in VCM when you install, discover domain controllers, add new Network Authority accounts, or add VCM users.

CAUTION Do not authorize VCM accounts to principals authenticated by an untrusted domain controller, and do not join VCM servers to an untrustworthy domain.

Microsoft Domain Controller Hardening Guidelines

To secure the domain controller for use with VCM, start by following Microsoft domain controller hardening guidelines, available for various server versions on the Microsoft Web site.

The Microsoft guidelines are more comprehensive than the compliance templates and need to be followed even if you are managing the domain controller with VCM.

Domain Controller Diagnostic Tests

Part of correctly configuring a domain controller for use with VCM is to run the dcdiag utility. The dcgiag utility checks for general connectivity and responsiveness of a domain controller, which includes verifying that the domain controller has the following properties.

- Can be located in DNS
- Responds to ICMP pings
- Allows LDAP connectivity
- Allows binding to the Active Directory RPC interface

Network Infrastructure Services

VCM relies on network infrastructure services. For VCM to operate correctly and reliably, you must properly configure, secure, and make these services available and responsive. An active denial of service (DoS) or other attack on network infrastructure services can affect VCM performance.

- **DNS and WINS**. Translate domain names into IP addresses.
- **Email**. Used for VCM notifications and alerts.
- **Time servers**. Synchronize timekeeping across systems, which allows Kerberos authentication and certificate validation to work.
- **DHCP**. Even when not used directly on VCM servers, DHCP assigns IP addresses consistently in the rest of the security environment.

Network Infrastructure Systems

VCM relies on secure infrastructure services; such as DNS, NTP, DHCP, routers, and services that issue certificates. The systems on which these services are hosted must be at least as secure as VCM. Protect network infrastructure systems with the following:

- Firewalls or vShield
- Anti-virus software
- Current security updates
- Controls or login authorizations that restrict access to trusted personnel only

Domain Accounts

VCM accounts must only be granted to users who are trusted, trained, and qualified as system and network administrators. A "VCM account" is a domain or local account that is granted authorization to use VCM.

Carefully Assigning Accounts

As an enterprise-wide configuration management and compliance tool, VCM can collect, correlate, and change system data on managed machines throughout the enterprise. VCM can configure security policies, collect and aggregate confidential information, install software and patches, and generally act as an administrator interface over an entire network.

VCM is intended for use only by responsible system and network administrators who protect their access from being subverted for unauthorized uses.

VCM administrators must follow these guidelines:

- Do not assign entire domain groups to VCM accounts.
- Set Windows login restrictions and password policies for user accounts that are VCM accounts to values consistent with administrator accounts.

VCM Application Services Account

Make the VCM Application Services account a domain user account. The VCM Application Services account must be a domain user because the account has full administrator authority for the CSI_Domain database.

Do not use the VCM Application Services account for VCM login or for any other purpose.

Personnel Considerations

For your VCM environment to be secure, the personnel who work with VCM must be trusted.

Confidentiality of Collected Data

The results of a VCM collection can contain infrastructure configuration settings, password and credential policies, encrypted password file entries, and any file uploaded from a managed machine.

VCM users must protect collected data as confidential information. Even if this data was not guarded as confidential on the managed machine itself, it might be confidential to the machine users. Without explicit knowledge about what data is sensitive, VCM users must treat and protect all collection results as confidential.

CAUTION Do not store collected data on public shares or in directories that are accessible to other users, including other VCM users, because they might not have collection rights on the machine from which the data originated.

Vulnerability of Exported Data

VCM supports several ways for personnel to export collected data:

- Email notifications and alerts
- Exported or printed grids
- Exported SRS summary views and reports
- Service desk work requests
- Uploaded and exported files
- Screen snapshots

VCM cannot control access to data after it is exported in these ways. When data must be exported, personnel must protect the exported files while stored or in transit to other sites.

VCM Installation Kits

3

Like the systems on which VCM runs, the software installation kits for VCM must be secured and protected from tampering.

Sources for Installation Kits

Secure operation of VCM requires that its product software kit not be tampered with and that it is intact as delivered by VMware. The best practice is to ensure that each kit is obtained directly from VMware, from another secure and trusted source, or that it is verified.

VMware ships VCM and add-on products on CD/DVD and in packages signed by the VMware Software Publisher Certificate. The kit can reach customer machines in the following ways:

- Physical CD/DVD
- Download from http://downloads.vmware.com
- ClickOnce download from the server zone
- Agent push install by the Collector service
- Patching Agent push by VCM Patching
- Thin client user interface by HTTP
- VCM Remote updates
- Patching deployed patches and updates
- VMware VCM software provisioning
- SMS
- Group Policy
- VCM Remote Command file attachments

You can verify EXE and MSI installers with the chktrust.exe certificate verification tool from the Microsoft Developer Network. Alternatively, you can verify using signtool.exe, also available from Microsoft.

Protecting Installation Kits

VCM installation kits that are stored on writable media must be protected from tampering before installation. Authenticode signatures on installation kits are verified before installation. For example:

```
C:\> signtool verify /a /v "CMAgent<version>.msi"
```

Unknown Software Publisher Warnings

Do not ignore unknown software publisher warnings during ClickOnce installations unless the publisher is VMware.

When you install ClickOnce software through the VCM user interface, Internet Explorer warns you when the software comes from an untrusted publisher. An untrusted publisher can be anyone, even a company that you recognize. The warning means only that the certificate is not in the trusted software publisher certificate store.

If you receive an unknown software publisher warning, open the certificate details view. VMware software is signed with the VMware Software Publisher Certificate. If the software publisher is VMware, you can install in spite of the warning.

Do Not Use VCM Remote to Install Other Software

Although VCM Remote can push new VCM Remote Agents to VCM Remote clients, do not use this mechanism to distribute software other than VCM Remote.

Server Zone Security

4

Address the following security environment guidelines for all systems in the server zone, including the VCM Collector, SQL Server host, and Web server. These three functions might reside all on one system, or they might be distributed across two or three. Be sure to apply the security settings in this chapter to all the systems that are used.

Server zone systems must be treated and managed with security measures that are consistent with those used for the infrastructure zone.

- For security instructions that are unique to the VCM Collector, see "VCM Collector Server" on page 25.
- For security instructions that are unique to the SQL Server host, see "SQL Server" on page 27.
- For security instructions that are unique to the Web server, see "Web Server" on page 31.

Using VCM to Manage Server Zone Systems

After you install VCM, your first course of action should be to manage server zone systems in VCM and subject them to assessment. VCM comes with compliance rules for some of the necessary security settings on the Collector, SQL database server, and Web server. In addition, you can create your own templates and rules.

The rest of this chapter briefly explains security hardening steps to pursue, manually or through compliance rules, for all server zone systems.

Machines in the VCM server zone need to be trusted more than those in the user interface, managed machine, or provisioning zones. In VCM, server zone systems must be controlled with the same measures used for infrastructure systems such as domain controllers.

Server Zone Administrator Role

VCM can manage its own servers, but it is unsafe to allow nonadministrator VCM users into server zone systems. When nonadministrator VCM users administer a VCM server, they have access to all the data and actions that are authorized to VCM. To help prevent this situation, create a role dedicated solely to server zone administration.

Having a role dedicated to server zone administration minimizes the risk of granting access to VCM servers to nonadministrator VCM users.

Server Zone Auditor Role

Create an auditor role, for example, VcmAuditor, in VCM that has read-only access to all VCM data but has no rights to create change actions or invoke inspections. Place at least one user account in that role.

Having an auditor role is an industry best practice.

General Security Guidelines for VCM Servers

In the server zone, VCM systems store and manipulate the collected data and change requests for every managed machine.

All server zone systems must have the following properties:

- Unavailable for login by general users
- Protected from the open Internet by firewalls
- Updated to the current operating system patch levels
- Routinely backed up
- Trusted by managed resource administrators

  Specifically, managed resource administrators implicitly delegate administrative rights over their resources when they allow the VCM Agent to be installed. Consequently, the managed resource administrators must have administrative trust in both the VCM users and in the VCM servers.

Protection Profiles

Operating systems for VCM servers must conform to the Controlled Access Protection Profile (CAPP) or General Purpose Operating System Protection Profile (GPOSPP), described on the Common Criteria Evaluation and Validation Scheme Web site.

The protection profiles ensure the following safeguards:

- Access to the system is protected by a certified authentication process.
- User data is protected from other users.
- Security functions of the operating system are protected from unauthorized changes.

Windows 2000, 2003, XP, and Vista, 2003 Server, and 2008 Server, 2008 Server R2, and Windows 7 conform to the CAPP. Windows 7 and Windows Server 2008 R2 conform to the GPOSPP.

Physical Security

An administrator must maintain possession and control of any VCM server zone system. The loss of possession or control of a VCM server zone system subjects the server to offline analysis, which can mean the loss of confidentiality or integrity of its data or the misuse of its software. Even the temporary loss of possession presents a risk, regardless of whether confidentiality appears to have been preserved.

If the VCM server zone systems run on virtual machines, the administrator must maintain possession and control of physical machines on which the virtual machines are hosted.

Use physical (possession, locks) or cryptographic (encrypted file system) means to maintain continuous control of VCM server zone systems.

Disabling Automatic Login

VCM systems in the server zone must require login access control.

Automatic login is a convenience that logs a specific Windows user into a machine after the machine finishes restarting. Because it bypasses the access control that the login prompt provides, always disable automatic Windows login on VCM systems in the server zone.

Dedicating a Server to VCM

VCM relies on the server operating system to protect the confidentiality, integrity, and availability of server zone data from other services or users that run on the VCM server zone systems.

When server zone systems are used for purposes other than VCM, the risk of granting unintended access to VCM data exists if those services or users have server administrator rights.

Foundation Checker

The VCM Foundation Checker determines whether a machine configuration is compatible with VCM.

Candidate systems must pass the Foundation Checker evaluation before you install VCM. Do not install VCM on systems that fail Foundation Checker.

Trusted Software

Even if server zone systems are dedicated to running VCM, you might need software packages beyond those from VMware or Microsoft.

Install only trusted software, preferably software that is accompanied and verified by a software publisher certificate. It is unsafe to run software of unaccountable origin on machines in the VCM server zone.

Routine Backup, Patching, and Virus Scanning

Routine maintenance functions like backups, patches, and virus scanning must be performed on VCM servers. You can perform these functions using VCM.

Authentication Certificates

VCM establishes the validity of HTTPS SSL certificates that IIS uses, and TLS certificates used during Collector-to-Agent communication. To verify the validity, VCM checks signatures up the trust chain, from the certificate in question up to a certificate installed in one of the trusted certificate stores.

VCM assumes and trusts that:

- A certificate in a trusted store is in fact trusted.
- Certificate authorities that issue certificates in a trusted store are trusted.
- Certificate services that manage certificates in a trusted certificate store, and the associated renewals and revocations, are trusted.

IMPORTANT VCM trusts any certificates in the trusted store, even when they were not issued with VCM.

To view the contents of the trusted certificate stored on Microsoft platforms, use the Certmgr.exe Certificate Manager Tool or the Microsoft Management Console (MMC) Certificates snap-in.

For more about authentication and certificates, see "Authentication" on page 57.

FIPS Cryptographic Service Providers

Most government and financial organizations require the use of FIPS cryptography. FIPS is also part of the VCM Common Criteria Security Target. All cryptographic service providers (CSPs) installed in the zone should be FIPS 140-validated.

The Microsoft CSPs that ship with Windows 2000, 2003, XP, Vista, Windows 7, and Server 2008 meet the FIPS 140–2 standard. Do not delete, replace, or supplement these packages with non-FIPS cryptography.

All systems in this zone are Microsoft Windows-based. To view the list of installed cryptography providers, run the following command:

```
C:\> certutil -csplist
```

Check your list against the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) Web site to verify that your modules are FIPS 140-validated.

VCM Collector Server 5

The following sections describe security and hardening guidelines that are unique to the VCM Collector function by itself. The Collector might be the same machine as the one that hosts the database or the Web server, or it might be a standalone system.

Using VCM to Manage the Collector Server

After you install VCM, use it to manage the Collector server itself, subject it to assessment, and maintain its integrity. Running the following VCM compliance template against the Collector detects and identifies some of the security setting and configuration issues that you must address, including non-VCM administrators who have access to systems and administrator functions.

VMware vCenter Configuration Manager Hardening - Host

NOTE If you have VCM installed and are preparing to set up another Collector, running the template can help you preharden the candidate system.

Having a Collector Machine Group in VCM

To better manage Collector systems, place them into a separate, dedicated Collector machine group in VCM, and make sure that the machine group is not authorized to any nonadministrator VCM user. Without a machine group, you might mix VCM Collector management with non-VCM servers, which can result in the misconfiguration of necessary security settings.

Managing the right group of Collectors allows them to be assessed routinely by the VCM security assessment compliance tests and monitored for configuration and change. These tests and changes can be managed and tracked through VCM.

If you do not organize all Collectors into a machine group, it is harder for VCM to assess, track, and control the security posture of the Collectors. Also, if a new Collector comes under VCM management, it might be incorrectly placed into a machine group that is managed by nonadministrator VCM users.

The remaining Collector hardening steps are the same as those that you apply for all server zone systems. See "Server Zone Security" on page 21.

SQL Server 6

The following sections describe security and hardening guidelines that are unique to the system where Microsoft SQL Server and your databases are installed. The database machine might be the same one as the VCM Collector, or it might be a separate machine if you are running a split VCM installation.

Using VCM to Manage the SQL Server

After you install VCM, use it to manage the SQL Server system, subject it to assessment, and maintain its integrity. Running the following VCM compliance template against SQL Server detects and identifies some of the security setting and configuration issues that you must address.

VMware vCenter Configuration Manager Hardening - SQL Server 2008

NOTE If you have VCM installed and are preparing to set up another SQL Server, running the template can help you preharden the candidate system.

The remaining SQL Server hardening steps in this chapter are in addition to those that you apply for all server zone systems. See "Server Zone Security" on page 21.

Having a SQL Server Machine Group in VCM

To better manage SQL Server systems, place them into a separate, dedicated SQL Server machine group in VCM, and make sure that the machine group is not authorized to any nonadministrator VCM user. Without a machine group, you might mix VCM SQL Server management with non-VCM servers, which can result in the misconfiguration of necessary security settings.

Managing the right group of SQL Server allows them to be assessed routinely by the VCM security assessment compliance tests and monitored for configuration and change, all of which can be managed and tracked through VCM.

Failure to follow this guideline means that the security posture of unmanaged VCM SQL Servers cannot be assessed, tracked, or controlled with VCM. Later, if a SQL Server comes under VCM management, there is also the risk that it might be incorrectly placed into a machine group that is managed by nonadministrator VCM users.

Microsoft SQL Server Best Practices and Hardening Tests

Microsoft provides guidelines and an auditing tool that ensure the secure installation and operation of SQL Server. The following tools are available from the Microsoft Web site.

- SQL Server 2005 Best Practices Analyzer Tool
- SQL Server 2008 R2 Best Practices Analyzer Tool

A secure installation of VCM pays particular attention to the Security Best Practices items regarding patching, physical security, service packs, and firewalls. See the following references, available from the Microsoft Web site.

- SQL Server 2005 Security Best Practices
- Security Considerations for a SQL Server Installation

Direct SQL Server Login

Even from within the server zone, regular VCM users must not connect directly to the VCM database using tools such as Query Analyzer. These types of direct login connections bypass the administrator safeguards afforded by the VCM user interface.

Enable the Microsoft host-based firewall and use a network firewall to help prevent direct SQL Server login.

Login Accounts for SQL Server

Configure SQL Server to accept existing Windows user account credentials for logging in. Do not set up separate SQL Server login accounts.

Restrict Access to Configuration Tools

SQL Server contains configuration tools such as the system stored procedure called sp_configure or SQL Server Surface Area Configuration Tool. Always restrict access to sp_configure or the SQL Server Surface Area Configuration Tool. The tools allow users to activate services and features that are usually disabled by default:

- xp_cmdshell
- SQL Server Web Assistant
- CLR Integration
- Ad hoc remote queries (the OPENROWSET and OPENDATASOURCE functions)
- OLE automation system procedures
- System procedures for Database Mail and SQL Mail
- Remote use of a dedicated administrator connection

NOTE Features managed with the Surface Area Configuration Tool in SQL Server 2005 are now managed with Facets in Policy Based Management starting in SQL Server 2008.

Delegation for Split Installations

VCM can operate in a split-server installation, where the SQL Server database runs on a different machine than that of the Collector and Web services. A split installation has the following SQL Server login possibilities.

- Use a private login to the SQL Server.
- Delegate VCM user credentials to the Web service for login to SQL Server.

For secure operation of VCM, configure for delegation. With private login, the VCM Web service maintains a copy of the VCM user's login credentials, which presents a security risk.

Do Not Connect from Outside the Server Zone

Prevent connections to the VCM SQL Server database from outside the server zone.

Even authorized VCM users must not connect directly to the database from remote locations. A firewall is one means of preventing these connections. The general guideline for preventing connections from outside the server zone is to block TCP port 1433 and UDP port 1434.

Web Server 7

This chapter describes security and hardening guidelines that are unique to the Web server system where Microsoft Internet Information Service (IIS) is installed and from which the VCM Web console is served. The Web server machine might be the same one as the VCM Collector, or it might be a separate system if you are running a split VCM installation.

Using VCM to Manage the Web Server

After you install VCM, use it to manage the Web server, subject it to assessment, and maintain its integrity. Running the following VCM compliance template against the Web server detects and identifies some of the security setting and configuration issues that you must address, including non-VCM administrators who have access to systems and administrator functions.

VMware vCenter Configuration Manager Hardening - Host

NOTE If you have VCM installed and are preparing to set up another Web server, running the template can help you preharden the candidate system.

The remaining Web server hardening steps in this chapter are in addition to those that you apply for all server zone systems. See "Server Zone Security" on page 21.

Having a Web Server Machine Group in VCM

To better manage Web server systems, place them into a separate, dedicated Web server machine group in VCM, and make sure that the machine group is not authorized to any nonadministrator VCM user. Without a machine group, you might mix VCM Web server management with non-VCM servers, which can result in the misconfiguration of necessary security settings.

Managing the right group of Web server allows them to be assessed routinely by the VCM security assessment compliance tests and monitored for configuration and change, all of which can be managed and tracked through VCM.

Failure to follow this guideline means that the security posture of unmanaged VCM Web servers cannot be assessed, tracked, or controlled with VCM. Later, if a Web server comes under VCM management, there is also the risk that it might be incorrectly placed into a machine group that is managed by nonadministrator VCM users.

Using Windows Integrated Authentication

By default, IIS uses Windows integrated authentication for the VCM Web site root. The interface to the VCM console is through a thin, browser-based interface to an IIS-served Web application located at the `/VCM` virtual directory.

Use Integrated Windows Authentication (IWA) with this directory by setting the IIS metabase property `NTAuthenticationProviders` to the string `'Negotiate,NTML'`, which is the default value. As a VCM administrator, set this value at the `/VCM` virtual directory to prevent subsequent modifications to the IIS metabase from unintentionally overriding the default value.

Instructions to set the metabase property are in a Microsoft knowledge base article about *how to configure IIS to support both the Kerberos protocol and the NTLM protocol for network authentication*.

Using HTTPS

HTTPS provides security against snooping and insures connection to a legitimate, not spoof, instance of VCM.

Do not use plain HTTP for the VCM user interface because sensitive collection results, configuration data, and configured passwords travel across the network. As a VCM administrator, set the VCM site root to require HTTPS by following the directions described in a Microsoft knowledge base article about *how to set up an HTTPS service in IIS*.

An HTTPS connection activates security precautions built into Internet Explorer when HTTPS is used in combination with Internet Explorer secure configuration recommendations from Microsoft.

Also set SQL Server Reporting Services (SSRS) reports to use HTTPS, as described in the *VCM Installation Guide*.

Web Server Certificates

When VCM uses SSL, TLS, or HTTPS, it authenticates the Web server and user interface client using certificates issued by certificate authorities (CAs). These CAs must be internal, customer CAs or members of the Microsoft Root Certificate Program as listed on the Microsoft Web site.

Mutual Authentication

Configure IIS to require client side certificates for mutual authentication from the VCM user interface system. Client side certificates enhance security for the following reasons:

- They approximate two-factor authentication.
- They provide better assurance that the VCM user interface is being run from a trusted machine and not, for example, from a kiosk.
- They are required by some organizational security policies. For example, U.S. DoD client PKI initiatives require client side certificates that are issued by DoD certification authorities.

VCM Agent Systems and Managed Machines

8

This chapter describes security and hardening guidelines for what is possibly the largest part of your security environment, the enterprise-wide body of managed machines that you monitor through VCM.

The VCM Agent is the software that is installed on each managed machine to collect configuration information and securely return it to the VCM Collector. For security purposes, each managed machine becomes its own trust zone, controlled by the domain and local machine administrator.

Trusting the VCM Agent on a Managed Machine

The VCM Agent is subject to the local security policies and security environment of its managed machine. Agents do not trust other Agents, but do trust machines in the server zone, such as the Collector.

Server zone machines trust the Agent to manage and return machine configuration data, but the Agent is not trusted as a source of data for making changes to any other machines or to your VCM configuration. The trust by the server zone in the Agent depends on the protection of the following assets:

- **Agent executable code**. Programs and libraries included in the VCM Agent installation kit. These kits and updates are signed by the VMware Software Publisher Certificate.
- **Machine configuration**. Local settings that activate the VCM Agent, grant it execution and data storage rights, and allow it to use infrastructure services like networking and DNS.
- **Collected machine data**. Settings the Agent acquires by inspecting the managed machine. Collected data is transmitted to the VCM Collector.
- **Agent/Collector credentials**. Certificates and private keys that the Agent and Collector use to authenticate each other.

Using VCM to Manage Machines

After you install VCM, always use VCM to manage the machines in your security environment, which includes installing and running the Agent on those machines. Do not allow unmanaged machines to run in the security environment and affect the operation and security of other machines.

Machine Groups

In the security environment, use the machine group feature of VCM to organize and control the configuration of systems. Machine groups make it easy to apply and synchronize security and hardening settings across multiple systems.

Restricting Access to Scripting

Grant access to script authoring, remote commands, content authoring, and import and export only to VCM administrators.

VCM role-based access controls protect the confidentiality and integrity of data from any user interface or API actions, but not from scripts written by users. Malicious VCM scripts, remote commands, compliance rules, or imported content can bypass the VCM role-based access controls.

By default, only VCM administrators should have access to these functions. The **VMware vCenter Configuration Manager Hardening - Host** compliance template can report on any nonadministrators who have access to them.

Users Who Are Not Local Administrators

Local machine administrators delegate administrator control of managed machines to VCM. In turn, VCM delegates administrator access to VCM users. The result is that VCM users can effectively be administrators outside of whether they are registered as a local machine administrator in Active Directory or in the local machine administrator group.

To account for and disclose the existence of these "effective" administrators, register the VCM users as local machine administrators on the machines that they manage. That way, an examination of the local machine administrator list correctly reveals all users who have administrator rights.

The **VMware vCenter Configuration Manager Hardening - Host** compliance template can report VCM users who are not local administrators of the machines that they manage.

VCM Agent

Address the following security guidelines regarding the VCM Agent that is installed on managed machines.

Agent Installation Directory

The Agent executable code, collection results, and credentials are stored in files in the Agent installation directory. Configure this directory and its contents so that an administrator account owns it, and have it deny read or modification access by nonadministrators.

The integrity of Agent files and the integrity and confidentiality of collected data are at risk if nonadministrators can access the Agent files and directories.

Agent Availability

The Agent operates in response to requests from the Collector service. VCM does not require the Agent to be available at all times, but it must be at least periodically available for the collection of timely data to occur.

The security environment must guarantee that the Agent is not permanently disabled or disconnected from network access or from connection requests by the Collector. The security environment must also maintain the network infrastructure required for Agent-Collector communication.

Continuous Possession and Control of the Agent

An administrator must maintain possession and control of any system where the Agent is installed. Even the temporary loss of possession of an Agent risks exposure of its private keys, regardless of whether confidentiality appears to have been preserved.

Use physical (possession, locks) or cryptographic (encrypted file system) means to maintain continuous control.

Unauthorized Agents

The managed machine administrator must not allow unauthorized Agents to run, even when the Agent is an authentic one.

An Agent can be installed using an authentic installation kit, but still not be authorized to return data. For example, it can be a nonadministrator's private Agent. Whenever possible, only one Agent should be installed per managed machine, and it should be the authorized Agent.

Restricting Access to Machine Configuration

The Agent depends on the integrity of settings in system configuration files, the Windows Registry, and the `UNIX/etc` directory. These settings activate the Agent and grant it access to infrastructure services like networking and domain name services (DNS), as well as access to the data sources and files from which the Agent collects data. These settings must be protected from unauthorized modification.

Local Administrator Account

Nonadministrator users of a managed machine must not be allowed to log in as the local machine administrator and bypass access controls. Apply one of the following safeguards:

- Disable the local administrator account.
- Set the local administrator account password to a strong, nondefault value.

BIOS Password

Enable and set the BIOS password of a managed machine to a strong, nondefault value.

nonadministrator users of a managed machine must not be allowed access to the BIOS and its ability to change the system time, enable or disable hardware, or start up into maintenance mode or alternative operating systems.

Disabling Alternative Startup

In the BIOS, configure the managed machine to start up only from the managed operating system. Do not present the user with multiple startup operating system options.

nonadministrator users of a managed machine must not be allowed to bypass file system access controls by starting up into an alternative operating system.

Maintenance Mode

In the BIOS, set the maintenance mode (single-user mode) password of a managed machine to a strong, nondefault value.

nonadministrator users of a managed machine must not be allowed to bypass file system access controls by entering maintenance mode.

Trusted Certificate Store

The Agent validates up to two certificates while authenticating and authorizing a Collector: a root certificate and an Enterprise certificate. During VCM installation, the customer can create a single, self-signed certificate to serve as both root and Enterprise certificate, or point to a root certificate from an external public key infrastructure. In either case, the root certificate is stored in the managed machine's trusted certificate store.

CAUTION Certificates, whether used by VCM or not, must not be placed in the trusted certificate store unless they originate from a trustworthy certificate authority.

Customer generated Enterprise certificates are assumed to be trustworthy. To verify the trustworthiness of other certificates, look for the issuer's membership in the Microsoft Root Certificate Authority Program, available from the Microsoft Web site. The site also describes admission criteria for the program.

Protecting Private Keys

Protect the Agent private keys from tampering, unauthorized replacement, or disclosure. Disclosure of or tampering with a private key threatens confidentiality.

Protecting Authorized Collector Certificates

Any system that possesses the private key corresponding to an authorized Collector certificate can communicate with Agents and send software packages and patches. To guard against this security risk, protect the inventory of authorized Collector certificates from tampering.

Securing Machine Backups that Contain Keys

The Agent private key authenticates the Agent to VCM servers. You must secure any backup copies and snapshots of machines that contain the Agent private key.

An unsecured Agent private key can be used to return false data to VCM servers that have not revoked that Agent enrollment.

NOTE If the Agent is to be decommissioned permanently, its private key must be destroyed everywhere, including on any backups or virtual machine snapshots. See "Decommissioning" on page 53.

Enterprise Certificate

The Agent only sends collection results to authorized Collectors. To be authorized, the Collector certificate must be signed by the Enterprise certificate authority and stored in the authorized Collector certificate list on the Agent.

The initial Enterprise certificate is shipped with the Agent installation, but that certificate can be replaced.

Trustworthiness of Data

The security of each managed machine determines the degree to which data that originates from that machine can be trusted.

Managed machines might have less stringent security requirements, depending on where they are. Data collected from a less secure machine that is connected to the Internet is not as reliable as data collected from an infrastructure system that is isolated within a company network.

Individual Collection Results

Trust individual collection results to be only as valid as their source.

Data collected by VCM is returned by the Agent that runs on the managed machine. Although the Agent should be protected from tampering by nonadministrator users, it is ultimately subject to modification and tampering by the machine administrator or a malware infection.

For this reason, do not trust the collected data more than the integrity of the data source. Base your decisions on aggregate values rather than on individual collection results. For example, consider the number of machines that have a vulnerability rather than the compliance state of a specific machine.

VCM User Interface System

9

The VCM Web Console runs in Internet Explorer and connects to the VCM Web application served by IIS.

Because VCM users also browse the Internet using Internet Explorer, VCM requires security measures to protect users of the VCM browser interface from spoofing and cross-site scripting attacks.

Using VCM to Manage the UI System

After you install VCM, your first course of action should be to manage user interface systems in VCM and subject them to assessment. Run the following VCM compliance template against your user interface zone systems to detect and identify some of the security setting and configuration issues that you need to address, including VCM logins from unmanaged machines.

VCM Client Best Practices

NOTE If you have VCM installed and are preparing to set up a UI system, running the template can help you preharden the candidate system.

The rest of this chapter briefly explains the user interface zone security hardening steps to pursue, either manually or, if possible, through compliance rules.

User Interface Systems Machine Group

Placing all VCM user interface systems into a dedicated user interface machine group allows the VCM administrator to separate the management of those systems and test the separation using compliance rules. In addition, having the group allows the VCM administrator to prevent non-VCM administrators from controlling user interface machines in the group. Except for VCM administrators, VCM users must not manage the user interface systems of other VCM users.

Access Control

The security environment for machines in the user interface zone is less strict than in the server zone. User interface machines are not required to be protected by firewalls or isolated from the Internet. In spite of the less strict conditions, you must still implement the following measures for these machines:

- Run operating systems that meet the Controlled Access Protection Profile (CAPP) or General Purpose Operating System Protection Profile (GPOSPP), described on the Common Criteria Evaluation and Validation Scheme Web site.
- Patch them to the current security level.
- Run anti-virus software.

Disabling Automatic Login

Systems that run the VCM user interface must require mandatory login.

Automatic login is a convenience that logs a specific Windows user into a machine after the machine finishes restarting. Because it bypasses the access control that the login prompt provides, always disable automatic Windows login on the VCM user interface system.

Disabling Simultaneous Login

The VCM user interface machines must not allow users to simultaneously log in to VCM by running multiple browser sessions on either the same system or from different systems.

Simultaneous login sessions defeat the traceability of actions back to a specific VCM user and reduce accountability.

Using Windows Credentials

To reduce susceptibility to spoofing attacks, do not allow VCM users to use a direct login to VCM. Instead, have the Internet Explorer browser forward the VCM user interface system Windows login credentials, or Run As or kinit credentials, to the VCM Web application. See "Customizing Internet Security Options" on page 42.

Service Account Credentials

Do not log in to VCM with service account credentials. Logging in to VCM with a service account can lead to unexpected or inconsistent behavior. Services using the same account as a logged in user can modify the logged in user's current role, machine group, or log the user out of the system at inappropriate times.

Recognizing Direct Login Prompts

Because you log in to VCM by transmitting your Windows account credentials, treat direct VCM login prompts in the browser with skepticism and caution.

When a user logs in to Windows using a domain account known to VCM, and connects to VCM, the system authorizes the user by their Windows credentials rather than requiring them to explicitly log in to VCM. Using the Windows login system resists spoofing and cross-site scripting attacks that exploit the Internet Explorer browser.

VCM can support a separate, browser-based login when Windows credentials are either unavailable or from a domain controller not trusted by VCM. However, the better practice is still to log in, or Run As, using a domain account, configure Internet Explorer to transmit those credentials, and treat direct VCM login prompts in the browser with skepticism and caution.

Public Access Points

Do not run the VCM user interface from public systems or from public Internet access points like kiosks or Internet cafés.

Network traffic between the VCM user interface and VCM Web server is encrypted and mutually authenticated. In spite of the safeguards, running VCM across the open Internet suggests that the VCM user interface system is also being used for general Internet browsing and purposes other than configuration management.

In particular, do not run the VCM user interface from public access points like kiosks or Internet cafés. These locations expose the VCM user interface to threats and malicious attacks that circumvent secure networking traffic by infecting the VCM user interface system itself.

Run the VCM user interface only on systems that are directly connected to your company network.

Cross-site Scripting

Cross-site scripting (XSS) allows an infected Web site to attack a Web application by injecting commands into the Web application. The opportunity occurs when you temporarily browse to the infected site while you are still logged in to the Web application. The malicious site typically adds hidden scripting and styles that silently invoke actions in the application login session.

As a VCM user, minimize the risk of cross-site scripting attacks by taking these precautions:

- Add the VCM Web server to the Internet Explorer trusted zone.
- Never place untrusted machines in the trusted zone.
- Do not allow links into the trusted zone.
- Evaluate "enter trusted zone" and "exit trusted zone" messages from Internet Explorer.
- Do not open external links that claim to be pointing to the VCM user interface.
- Set Internet Explorer to transmit Windows login credentials.
- Avoid direct VCM logins in favor of using the Windows login credentials.
- Treat non-Windows login prompts with skepticism.
- Do not use VCM while browsing the Internet in other browser windows or tabs.

Internet Explorer Trusted Zone

By using the Internet Explorer trusted zone, you can identify reputable sites that you visit regularly, including the VCM user interface.

Adding the VCM Web Server

Add the VCM Web server to the Internet Explorer trusted zone. When you place the Web server in the trusted zone, Internet Explorer can delegate the VCM user's Windows credentials to the Web service for use with SQL Server when running in a split installation configuration. This setup is a requirement for proper SQL Server preparation in split installations.

When you place the Web server in the trusted zone, users also can disable navigation into the trusted zone from less privileged Internet Explorer zones, which reduces the exposure to cross-site scripting attacks and makes some attacks more detectable.

To add the VCM Web server to the Internet Explorer trusted zone, see the instructions in the *VCM Installation Guide*.

Removing Untrusted Systems

Do not allow untrustworthy systems to remain in the Internet Explorer trusted zone with the VCM Web server. This step isolates the VCM Web site from untrusted sites and helps reduce the risk of cross-site scripting attacks.

Customizing Internet Security Options

In Internet Explorer, apply the following settings:

- Enable **Automatic login with current username and password**
- Disable **Navigate subframes across different domains**
- Disable **Web sites in less privileged web content zone can navigate into this zone**
- Disable **Display mixed content**

When you allow automatic logins, Internet Explorer can transfer credentials to machines in the trusted zone, specifically the VCM Web server, without user interaction. When this ability is combined with the IIS setting to use integrated windows authentication, the result makes the login process resistant to spoofing and cross-site scripting attacks. With this configuration, login prompting does not take place within the context of the browser, but rather within the Windows login system, which is more resistant to cross-site scripting attacks.

Trusted Software

Even if a user interface system is dedicated to running VCM, third party software packages are often needed.

When that happens, install only trusted software, preferably software that is accompanied and verified by a trustworthy software publisher certificate. It is unsafe to run software of unaccountable origin on machines in the VCM user interface zone.

Verifying Certificates

When you connect to VCM from the user interface system, Internet Explorer prompts you to verify that the certificates that VCM uses for authentication are correct.

Click to view certificate signing details before deciding to trust the software. If the signature is known to you and valid, you can add the certificate to your trusted store so that you do not need to repeat the verification every time that you connect.

HTTPS Certificate

The SSL certificate used for HTTPS with the VCM Web server might be issued by a trusted root certificate authority or be self-issued.

When a certificate comes from a trusted authority, you do not receive any warning messages. When Internet Explorer detects an untrusted certificate, review the signature details.

- If you recognize the signature, you can add the certificate to the trusted store.
- If the signature is suspicious, cancel and avoid opening the Web page.

NOTE Initially, Internet Explorer asks you to review the details of self-signed certificates. It treats self-signed certificates as suspicious until you add them to the trusted store.

Trusted SSL certificates are those that are issued by members of the Microsoft Root Certificate Program, listed on the Microsoft Web site.

VMware Software Publisher Certificate

Some components of the VCM user interface that are downloaded to the browser as ClickOnce deployments are signed by the VMware Software Publisher Certificate. When you activate these components in the interface, Internet Explorer prompts you about trusting the software publisher certificate and adding it to the trusted store.

Before adding it to the trusted store, verify that the certificate is authentic and authorized by clicking the **Details** tab of the dialog box and verifying the information with VMware.

FIPS Cryptographic Service Providers

Most government and financial organizations require the use of FIPS cryptography. FIPS is also part of the VCM Common Criteria Security Target. All cryptographic service providers (CSPs) installed in the zone should be FIPS 140-validated.

The Microsoft CSPs that ship with Windows 2000, 2003, XP, Vista, Windows 7, and Server 2008 meet the FIPS 140–2 standard. Do not delete, replace, or supplement these packages with non-FIPS cryptography.

All systems in this zone are Microsoft Windows-based. To view the list of installed cryptography providers, run the following command:

```
C:\> certutil -csplist
```

Check your list against the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) Web site to verify that your modules are FIPS 140-validated.

Running Anti-virus and Anti-rootkit Tools

Systems on which you run the VCM user interface receive credentials and issue actions that affect managed machines and the VCM configuration itself. As such, a virus or rootkit infection of a user interface system is a serious threat to the confidentiality of the credentials used by VCM and of the integrity of user interface actions.

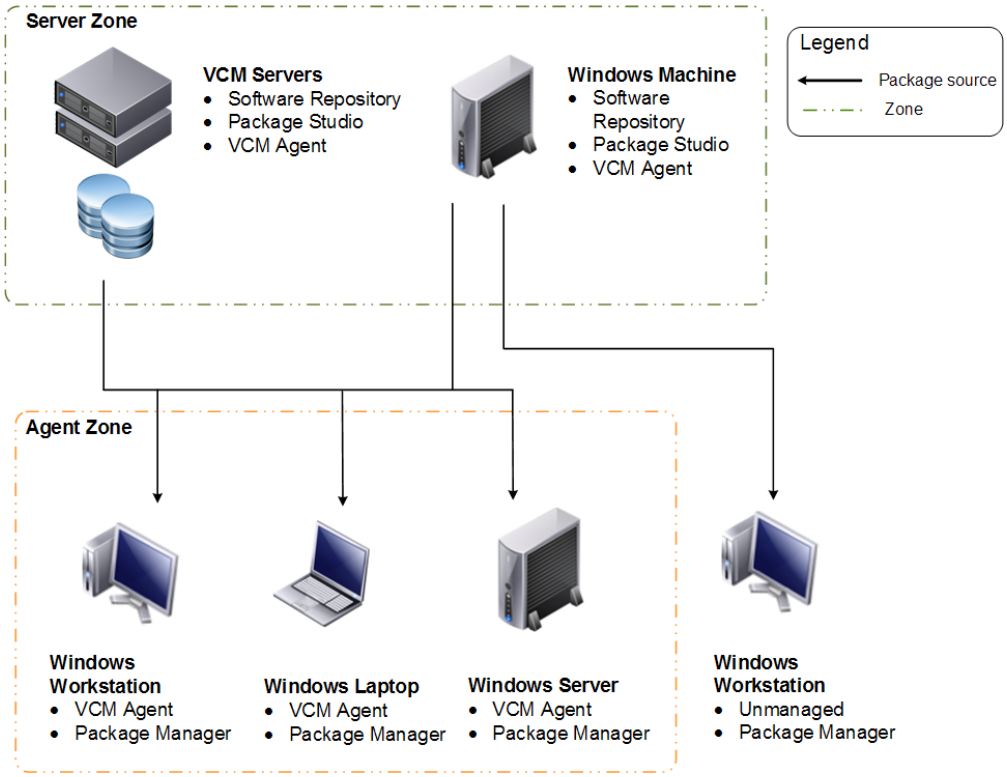
You must run virus and rootkit detection software. In addition, run the Microsoft malicious software detection tool on a routine basis. You can download the malicious software detection tool from the Microsoft Web site.

Software Provisioning Components 10

A software package is composed of the files and scripts necessary to install and remove programs. VCM software provisioning supports software that is installed using technologies such as MSI and EXE packages. The VCM software provisioning components are Package Studio, Package Manager, and software package repositories.

The software repository is a shared location on a Windows software provisioning server to which packages are published by Package Studio, as well as the location from which Package Manager downloads packages for installation. These components can operate independent of other VCM components. Although it is a good practice to do so, repositories and target machines do not need to be managed by VCM Agents.

Figure 10–1. Software provisioning components with respect to VCM trust zones



Separating and Securing the Software Provisioning Zone

Make the software provisioning zone network a private network. Use a separate, dedicated network interface to connect the software provisioning server with its provisioning zone network. For more information about private network interfaces, see the *VCM Installation Guide*. Restrict access to the software provisioning zone to personnel who are trusted to install software and act as network administrators.

Software provisioning operations take place across the network that connects the software provisioning server with provisionable target systems. The software provisioning zone, including its servers, network, and network infrastructure must be protected from unauthorized access and tampering, and must be kept available and responsive.

Failure to isolate the software provisioning zone exposes you to attacks that intercept `unattended.xml` files that contain credentials.

Software Publishers and Software Signing

Secure operation of software provisioning requires that you follow these practices:

- All packages are signed.
- Signatures are always validated.
- Certification authorities are trusted.

VMware packages are signed by the VMware Software Publisher Certificate verifiable by Verisign.

Third-party packages, or any repackaging of VMware software, must be signed by the certificates of other reputable publishers and be verifiable by Package Manager at installation time. Repositories must not contain unsigned packages placed there by means other than Package Studio.

When you use Package Manager, all packages must be signed with a private key before they are installed or uninstalled. To accommodate customers who do not use software signing or when circumstances require that you ignore a signature, VCM supports a "skip signature validation when installing a signed package" override as described in the *VCM Installation Guide*.

Protection of Repositories

Packages in a repository are available for Package Manager to download. Repositories must be protected from tampering or unauthorized deletion of important content. Repositories must reside on access-controlled systems that are protected with the measures described in "Server Zone Security" on page 21.

Connecting to Repositories

Use Package Manager to add or remove packages in software repositories.

Package Manager can connect to multiple repositories, but only configure trusted repositories as sources. In addition, the URI specified as the package source must reference a secure file share, or use an HTTPS scheme with a repository that uses a trusted SSL server certificate.

Software Provisioning Credentials

Normally, VCM does not store customer credentials on a managed machine. During software provisioning though, the Network Authority credentials are temporarily stored and used to authorize package installation, uninstallation, user access control (UAC), access to network repositories, restart, or resume activities. The credentials are protected from disclosure to unprivileged users but are accessible to a determined local machine administrator who uses custom software.

Because an untrustworthy local administrator can gain access to the Network Authority credentials during a software provisioning operation, you can mitigate the risk by using the following techniques:

- Do not initiate software provisioning installation or uninstallation operations on an untrustworthy machine.
- Assign the minimal necessary permissions and login rights to the Network Authority account used for software provisioning.
- Create an individual Network Authority account with a set of local administrator credentials for operations on an untrustworthy managed machine.

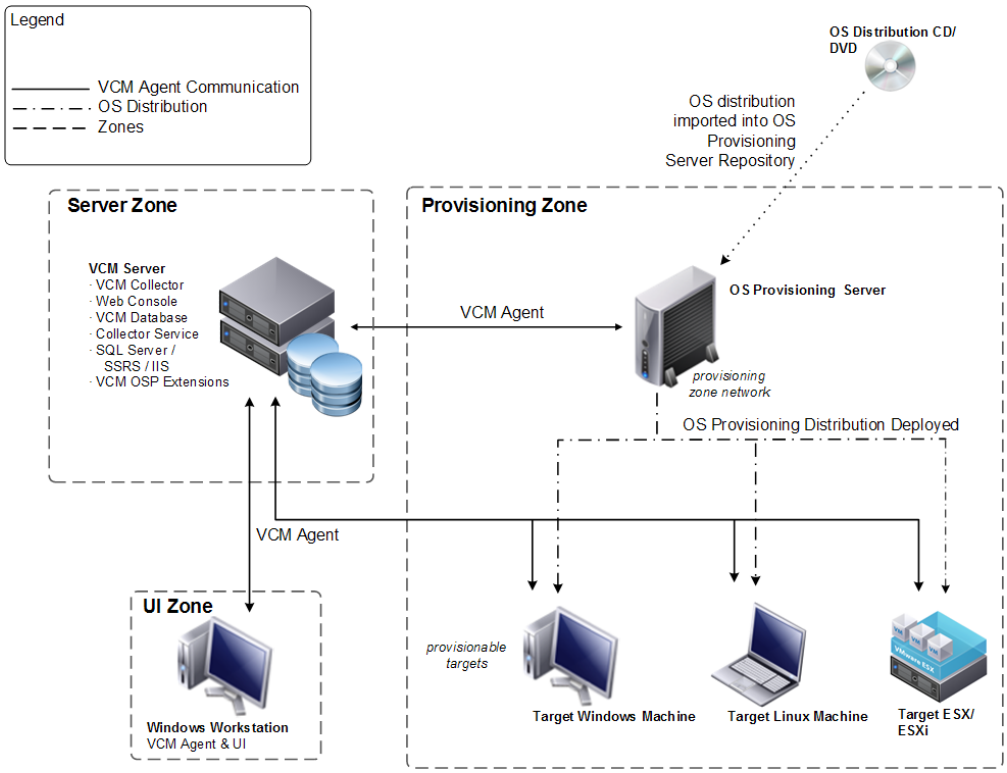
Operating System Provisioning Components

11

VCM operating system provisioning deploys operating system images to targets that are started over the network. The target machine uses a PXE startup process to contact a DHCP server that identifies the OS Provisioning Server as the source of a bootable image, referred to as a distribution. The target machine then requests the bootable distribution across Trivial File Transfer Protocol (TFTP) and boots the distribution, which in turn installs an operating system that is also retrieved from the OS Provisioning Server.

The OS Provisioning Server components consist of operating system provisioning extensions to VCM and an OS Provisioning Server.

Figure 11–1. Operating System Provisioning Components



Separating and Securing the OS Provisioning Zone

Make the operating system provisioning zone network a private network. Use a separate, dedicated network interface to connect the OS Provisioning Server with its provisioning zone network. For more information about private network interfaces, see the *VCM Administration Guide*. Restrict access to the operating system provisioning zone to personnel who are trusted to install operating systems and act as network administrators.

Operating system provisioning operations take place across the network that connects the OS Provisioning Server and the provisionable targets. The provisioning zone, including its servers, network, and network infrastructure must be protected from unauthorized access and tampering, and must be kept available and responsive.

Failure to isolate the operating system provisioning zone exposes you to attacks that intercept `unattended.xml` files that contain credentials.

Dedicating a Server to Operating System Provisioning

VCM relies on the OS Provisioning Server to protect the confidentiality, integrity, and availability of provisioning zone data and OS images. When the OS Provisioning Server is used for purposes other than provisioning, you risk granting unintended access to provisioning distributions. The OS Provisioning Server must be dedicated only to provisioning operations and must not allow logins except by the machine administrator and the VCM administrator who installs the OS Provisioning Server as described in the *VCM Installation Guide*.

Closing Unnecessary Ports

"VCM Ports" on page 84 lists the network ports that the OS Provisioning Server uses. Use the iptables host firewall, which you can manage through VCM, to keep other ports closed.

Protection of Baseline OS Images

The OS Provisioning Server deploys operating system images built from original distribution images from Microsoft, Red Hat, SUSE, VMware, and others. These images must be obtained from trusted sources, transferred over secure channels, and protected from tampering.

OS Provisioning Credentials

VCM protects and encrypts credentials stored on server zone machines. However, during operating system provisioning operations, credentials within bootable distributions are transmitted in clear text across TFTP. This process is an intrinsic limitation of the PXE startup protocol and makes credentials subject to attacks that can sacrifice the confidentiality, integrity, and authenticity of the credentials or other sensitive pieces of provisioned operating systems.

To mitigate this risk, use one or more of the following techniques:

- Use operating system provisioning only across a secure network. After a machine is provisioned, it can then be transferred to a less secure network and used like any other managed machine.
- Do not join machines to domains during operating system provisioning activities.
- Change secret passwords to temporary passwords before transmission by the OS Provisioning Server, and change them back immediately after provisioning operations are finished.
- Change any secret passwords transmitted during operating system provisioning immediately after the process is finished. Change the passwords everywhere they were used, even on machines not involved with provisioning operations.

12 Decommissioning

Systems where VCM was installed contain private keys, sensitive credentials, and collection results. Properly decommission such machines before disposing of them or using them for another purpose.

Erasing versus Deleting

For VCM decommissioning, full erasure involves more than deleting files.

After you transfer any sensitive data to retain, follow best practices to completely remove confidential data. Always run a secure erasing or disk scrubbing utility such as Windows secure delete (SDelete).

Confidential Data to Remove

VCM systems contain confidential data or credentials from managed machines. Depending on the role of the system, any of the following items might be present:

- Collected data
- File uploads
- Private keys for Enterprise, Collector, Agent, or IIS HTTPS certificates
- Managed machine login credentials
- Proxy machine credentials
- Alternative source credentials used for VCM Patching
- Secure communication session caches
- Network Authority account passwords
- Collector and Agent install kits
- VCM license files

Proper decommissioning requires the full erasure of these values from the respective machines. See "Erasing versus Deleting" on page 53.

Distinct Collector and Agent Keys

VCM associates a unique machine identity with the private keys used by Transport Layer Security (TLS). Do not copy these keys.

Besides being difficult to copy securely, copying a private key presents the risk of sharing it with more than one machine, a configuration that is unsupported. Always generate a distinct key for each Collector during the installation process. Because TLS mutual authentication is used by default, the process of installing the Agent also creates a distinct key for each Agent.

Enterprise Certificate Key and Web Server Keys

If the Enterprise certificate server is the same machine as the VCM Collector being decommissioned, the private key must be manually transferred by exporting it using the Microsoft Management Console (MMC) Certificates snap-in. Use **Copy To File**, select the PFX file format, enable strong protection, and select to delete the private key if the export is successful.

The resulting PFX file can safely be transported to the replacement machine over a network because the file is passphrase protected.

Perform the same process to obtain a copy of the Web server keys before decommissioning the VCM Web server.

Removal of Agent Keys at Uninstallation

When you uninstall an Agent, erase its private key unless it is to be used with an updated Agent on the same managed machine. For Windows Agents, the MMC Certificates snap-in can erase both a certificate and its private key.

Network Authority Accounts

After Collectors or Agents are decommissioned, any special Network Authority accounts that were created specifically for them are not required. The need for the accounts is described in the *VCM Administration Guide*.

Disable or remove these Network Authority accounts by using the VCM Administration panel and the account management tools for your domain.

Erasing Server Disks

Server zone system disks contain collected data and login credentials from managed machines. Do not discard these disks or use them for other purposes unless they are fully erased. See "Erasing versus Deleting" on page 53.

NOTE Using these disks with a replacement Collector is a safe alternative to discarding them, and it preserves the previous collection results.

Erasing Virtual Machines

If a virtual machine participated in your VCM environment, and you do not plan to use the virtual machine for another purpose, fully erase the files that make up the virtual machine. See "Erasing versus Deleting" on page 53.

Virtual machines sometimes have a source machine behind them. For example, they can be cloned from a parent virtual machine, be based on a template, be a conversion from a physical machine, and so on. If the source machine was an original that participated in your VCM environment, you might have additional files or disks to decommission in order to fully destroy confidential data or keys. Furthermore, there may be other clones or copies to locate, siblings and cousins to the virtual machine that you started with.

Always trace the origin of your virtual machines backward and forward so that you find all systems that contain confidential data or keys.

13 Authentication

This chapter describes the VCM authentication and certificate structure. To understand these concepts, you must have some familiarity with secure authentication and certificates.

Transport Layer Security

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide endpoint authentication and secure communication over any transport. TLS is normally associated with TCP/IP communication but can be applied to any transport layer, including HTTP. TLS allows for server authentication and mutual authentication security.

Server Authentication

Server authentication only authenticates the server to the client. With server authentication, the client verifies that the server with which it is communicating is the server that it claims to be. When browsing, your browser is the client, and a Web site such as Amazon is the server. Millions of clients need to be sure that the site to which they are sending financial information is really Amazon.

To accomplish this using TLS, Amazon provides a certificate issued by a trusted authority such as Verisign. When your browser has a copy of the Verisign certificate in its trusted store, it can know when a server really is the one at Amazon. In the other direction, the server usually authenticates a client by verifying credentials such as a user name and password.

If you want to use server authentication without mutual authentication, VCM can support that configuration. Under server authentication, VCM Agents authenticate the identity of a VCM Collector by recognizing and verifying its certificate. However, counterfeit Agents are possible with server authentication. Server authentication alone is called *Collector Authentication* in VCM.

Mutual Authentication

Mutual authentication employs certificates in both directions; from the server to the client, and from the client to the server. Mutual authentication is more secure because the client certificate requires the private key that only exists on a legitimate client.

Starting with version 5.5, VCM uses mutual authentication out of the box. A Collector certificate is employed for server authentication, and Agent certificates are employed in the other direction so that the Collector authenticates the Agent.

Keys and Certificates

Communication between VCM systems relies on keys and certificates for authentication.

Using Single or Paired Keys

Encryption usually uses one of the following approaches:

- Single key (symmetric) algorithms rely on a single key that both encrypts and decrypts the information. A single key must always be kept secret.
- Paired keys (asymmetric) are slower but use one key to encrypt and the other to decrypt. Either key can encrypt, then the other decrypts.

  One key is considered to be the public key, which you can distribute freely, and the other is the private key that you keep secret. For convenience, users refer to this configuration as "public key" cryptography. One common practice is to use a public key to securely negotiate a session key, a symmetric key that is valid only for the duration of a single connection to the server.

Certificates

In public key authentication, you must know that the key you hold is not a fake and that it came from the entity that you think it did. Certificates are a mechanism for performing this verification.

A certificate is a package containing the public key, information identifying the owner or source of the key, and one or more signatures that verify that the whole package is authentic. To sign a certificate, the issuer adds the information about itself to the certificate, hashes the result, and then encrypts the hash using its private key to create a signature.

When you have a public key, you can verify that it came from the issuer identified in a certificate because the information in the public key is able to decrypt the signature, obtain the hash, and recalculate a matching hash value.

It is assumed that you trust certificate issuers, directly or by virtue of trust chains. See "Trust Chains" on page 58.

Public Key Infrastructure

Public key infrastructure (PKI) describes a management system that aids in the administration and distribution of public keys and certificates throughout an enterprise. TLS is supported in a security environment where certificates are managed by a PKI that guarantees the identity of servers and clients.

However, certificates can also be created, managed, and used by TLS without the support of a full PKI. Having multiple Collectors is the main reason for creating certificates in this way. See "Certificates for Additional Collectors" on page 64.

Trust Chains

NOTE *Signing* and *issuing* are synonymous.

An issuer's certificate can be signed by a previous issuer. This practice is called a trust chain. The chain flows backward until you arrive at a certificate that was issued and signed by itself, or you arrive at a certificate called a trust root. All certificates that are members of the chain can be trusted when the chain begins with such a trusted certificate. Typically, this trust relationship works because you or someone else has already installed the trust root in your local trusted certificate store.

Certificate Expiration and Revocation

Because keys can be compromised and circumstances can change, keys and certificates are not designed for indefinite use. Certificates are created for a finite period of validity, before and after which they must not be used or trusted. If a certificate expires without being renewed or replaced, it cannot be used to establish a TLS session.

You can revoke certificates to indicate the withdrawal of trust, even before they expire. The issuing authority might make a certificate revocation list available for additional validation of certificates that it has issued. Do not trust a certificate in the revocation list.

To view VCM certificates in the VCM user interface, click **Administration**, and select **Certificates**. The data grid displays your certificates and related information, including expiration dates.

For information on how to renew or replace your certificates, see "Changing Certificates" on page 64.

NOTE VCM supports certificate expiration but not revocation lists. To effectively revoke certificates, remove them from certificate stores.

Certificate Standards

Certificates are defined by the X.509 RFC standard, which specifies standard fields and capabilities. Certificate creators can add additional fields, either critical or noncritical. The fields are a contract between the creator and consumer. Because of custom fields that are implementation-specific, an application might encounter a certificate with fields that it does not understand. The application is obligated to fail validation on a certificate with critical fields that it does not understand. Noncritical fields are not subject to this rule.

One common noncritical extension is Enhanced Key Usage. This field specifies the valid uses for the certificate. Uses might include server authentication, client authentication, code signing, or certificate signing.

Certificate Storage

In Microsoft systems, certificates are physically kept in files, the Windows Registry, memory, Active Directory, or other locations. Taken together, a collection of physical stores that share common properties is known as a logical store. For purposes of this guide, any discussion of certificate stores is assumed to mean logical stores unless stated otherwise. For a description of the logical system of stores provided by Microsoft, see the Microsoft TechNet Web site.

On UNIX systems, Collector certificates for server authentication, and Agent certificates and Agent private keys for mutual authentication, are stored in a proprietary protected store. Although the store is not encrypted, it is protected from simple viewing. Use the CSI_ManageCertificateStore utility and the associated help provided with your VCM UNIX Agent installation package to view or manage the UNIX Agent certificate store. For more information, see the *VCM Administration Guide*.

How VCM Uses Certificates

Authentication between Collector and Agent is more automatic and secure by default as of VCM Version 5.5. You no longer need to manually configure the VCM security environment for mutual authentication to work. That is, you no longer need to manually create and issue certificates for use on Agents, which was the case in previous releases.

NOTE If you have an existing PKI in your enterprise, VCM can be configured to use it. Contact VMware Technical Support for assistance in having Collectors and Agents use an existing PKI.

The following certificates enable Collector-Agent communication in VCM:

- An Enterprise certificate
- One or more Collectors, each with a certificate
- An Agent certificate for each managed machine, for mutual authentication

VCM Agents and Collectors trust each other when their respective certificates are issued by the same Enterprise certificate.

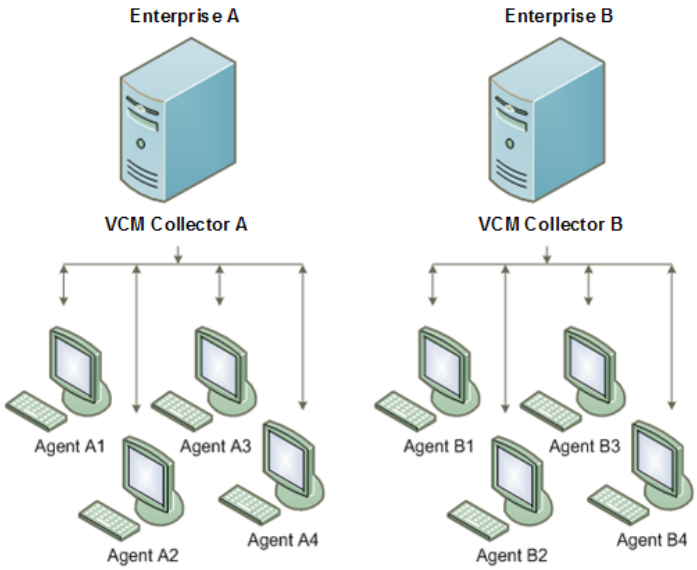
To view information regarding your Enterprise and Collector certificates, click **Administration**, and select **Certificates**.

Enterprise Certificate

The Enterprise certificate enables VCM to operate in a multiple Collector environment. Agents have the Enterprise certificate in their trusted certificate stores, and can use it implicitly to validate any certificate that the Enterprise certificate issues. All Collector certificates are expected to be issued by the Enterprise certificate.

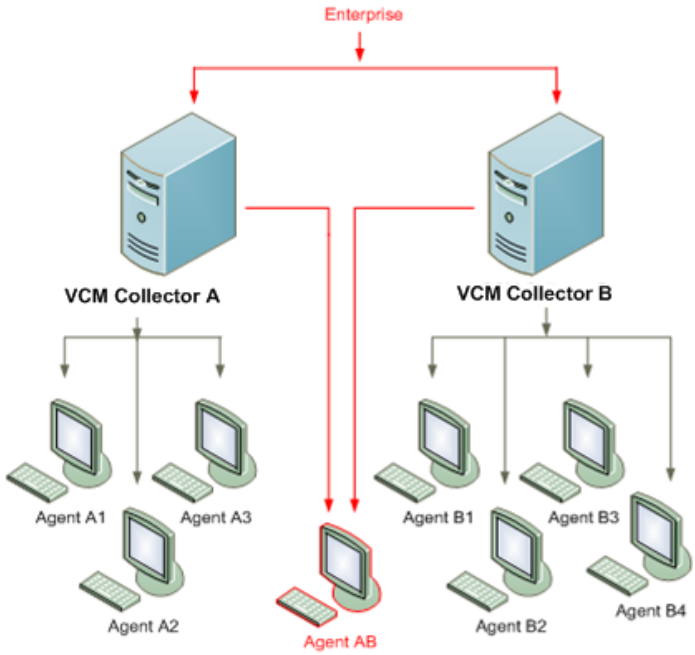
Without an overall Enterprise certificate, Agents can only report to their own Collector as shown in the following figure. In effect, each Collector becomes an isolated Enterprise.

Figure 13–1. Dedicated Collector-Agent Relationship



In cases where a single Agent must report to two Collectors, a common Enterprise certificate must exist, and the Enterprise certificate must issue all Collector certificates. When both Collector certificates are issued by the same trusted authority, the Agent that is shared between the two can trust both Collectors as shown in the following figure.

Figure 13–2. Shared Collector-Agent Relationship



To properly support the trust chain, mutual authentication, and multiple Collector environments, Enterprise certificates in VCM must have the following properties:

- Must be able to sign certificate requests.
- Can be self-signed. If the certificate is self-signed, it is assumed that you trust it. The trust is implemented by placing the certificate in the Trusted Root store (Windows) or in the VCM store (UNIX).
- Can be signed by another certificate in an existing PKI and placed in the trusted store.
- Must be stored in the local machine Trusted Root Certification Authorities store on the Windows Collector and Agents (Windows only).
- On UNIX platforms, the Agent has a vendor-implemented certificate store. The Enterprise certificate must be added to this store. The certificate is added during initial installation, but you must add subsequent certificates manually using the CSI_ManageCertificateStore utility included with your VCM UNIX Agent.
- Can be authorized as explained in "Authorized Certificates in the Trust Chain" on page 62.

Collector Certificate

The Collector certificate must secure an initial TLS communication channel with the Agent. The Agent must establish that the Collector certificate can be trusted. Because the Enterprise certificate is installed in the managed machine (Agent) trusted store, the Collector is trusted whenever the Collector certificate was issued by the same, trusted Enterprise certificate.

Collector certificates in VCM must adhere to the following requirements:

- Must be kept in the local machine personal certificate store on the Collector.
- Must be valid for server authentication (OID: 1.3.6.1.5.5.7.3.1).

Authorized Certificates in the Trust Chain

Agents maintain a store of trusted certificates used for authenticating Collectors. When a Collector sends its certificate to the Agent during the TLS handshake, the Agent verifies the trust chain from the Collector certificate back to a trust root, such as the Enterprise certificate.

VCM 5.5 extends the trust process to require that at least one of the certificates in the chain be marked as authorized to communicate with the Agent. If there are no authorized certificates in the trust chain, the TLS handshake fails even if the chain is otherwise valid.

This feature prevents multiple Collectors that share the same issuing root certificate from automatically being able to communicate with each other's Agents. By requiring an authorized certificate somewhere in the chain, an administrator can configure which Collectors have access to which Agents. If you want all Collectors to have access to each other's Agents, authorize the shared root certificate.

By default, the Enterprise certificate is authorized during the standard Agent installation from the Collector. If you choose to add certificates to the Agent certificate store manually, make sure that at least one of the certificates in the chain is authorized.

- **UNIX**. At least one of the certificates added to the Agent certificate store using CSI_ ManageCertificateStore must be inserted using the **-z** option to mark the certificate as authorized. See "CSI_ManageCertificateStore Options" on page 76.
- **Windows**. Create Agent Registry entries in `HKEY_LOCAL_MACHINE\SOFTWARE\Configuresoft\CSI\5.0\Listener\Authorized` for manually imported certificates. See "Mark a Certificate as Authorized on Windows" on page 69.

Agent Certificates

Agent certificates are used in mutual authentication. A copy of the Agent's certificate is stored in the Collector database and is viewable in the Certificates data grid in VCM. The Agent's private key must not exist anywhere but on the Agent machine. The following sections provide additional detail about the Agent certificate process.

Mutual Authentication by Default

In prior releases, VCM supported server authentication by default. Starting in VCM Version 5.5, new Collector-Agent communication employs mutual authentication by default.

If you have existing Agents that were set up manually for mutual authentication, and that take advantage of existing Enterprise certificates and trust chains, you do not need to change their configuration to use them with a 5.5 Collector. Furthermore, older Agents that authenticated over server authentication can continue to do so with a 5.5 Collector. New version 5.5 Agents, however, configure themselves to mutually authenticate with 5.5 Collectors.

Version 5.5 Agents on DCOM communication still use server authentication, but they follow the new process for generating their own certificate and private key pair. The certificate and private key pair allow for the following practices:

- Data to be encrypted as explained in "Encryption Between Collector and Agent" on page 63.
- The protocol to be switched to HTTP for mutual authentication.

You can view the managed machine communication security level and protocol by selecting **Administration**, and clicking **Machines Manager > Licensed Machines > Licensed *Windows or UNIX* Machines**.

First Contact

When a Collector first contacts an Agent, the Agent determines whether the Agent already has a certificate and private key pair. If the Agent does not have a certificate and private key pair, it generates a self-signed certificate and private key. The Agent stores these in its own certificate storage area, the Microsoft store on Windows or the VCM certificate store on UNIX.

Next, the Agent certificate is sent to the Collector as part of the TLS handshake. If the Collector has already stored a certificate for that Agent, the Collector compares the stored certificate with the incoming one and rejects the TLS connection if they do not match. If the Collector has no certificate for the Agent, the Collector stores the incoming Agent certificate, allows the TLS connection to succeed, but does not trust the Agent certificate until you tell the Collector to do so as explained in "Encryption Between Collector and Agent" on page 63.

Changes to Agent Certificates

When the Collector stores an Agent certificate, the Agent machine is associated with the Agent certificate at the Collector. If the Agent attempts to use a different certificate to establish TLS communication with the Collector, authentication fails.

The preceding scenario can happen, for example, if you uninstall and reinstall an Agent without preserving the existing certificate and private key pair, which causes the Agent to generate a new certificate and private key pair when contacted by the Collector. See "First Contact" on page 63.

If an Agent needs to use a new Agent certificate and re-establish mutual authentication with a Collector, reset the stored certificate and security level at the Collector. Select **Administration**, and click **Certificates**. Select the action to re-establish mutual authentication.

Encryption Between Collector and Agent

The Agent certificate and private key pair serve an additional function unrelated to the TLS handshake with the Collector. The certificate and private key pair decrypt any encrypted, sensitive data that the Collector sends to the Agent.

Although the creation and trust of the Agent certificate and private key pair is automatic when a Collector first contacts an Agent, the encryption feature requires that you separately tell the Collector to trust the Agent certificate. To mark an Agent certificate as trusted for data encryption, on the Collector, select **Administration**, and click **Certificates**. Select one or more certificates, and select the action to **Change Trust Status**.

Installing Certificates for the VCM Collector

You can generate certificates during VCM installation or create them and store them in the local certificate store in advance. Either way, the VCM Installation Manager registers the certificates in VCM and configures the Agents to trust these certificates.

Installing Certificates on the First Collector

VCMInstallation Manager lets you generate certificates during installation or browse to your certificate store to select existing certificates. If you plan to use your own certificates, place the existing certificates on the Collector before starting the installation, and in the following stores.

NOTE The certificates do not need to be separately available on the SQL Server system in a split configuration.

- **Collector certificate**. Local machine personal system store
- **Enterprise certificate**. Local machine trusted root system store

  The private key of the Enterprise certificate does not need to be stored on the Collector.

To create your own certificates in advance of VCM installation, see "Collector Certificate" on page 61 for requirements, or see "Creating Certificates Using Makecert" on page 70 to create certificates without full PKI support.

If circumstances change after VCM installation, you can replace the certificates that you generated or selected during install. See "Changing Certificates" on page 64.

Certificates for Additional Collectors

To ensure seamless operation across Agents and Collectors, all Collector certificates in the VCM environment must be issued by the same Enterprise certificate. The option to generate certificates during installation fails to create the right Collector-Enterprise relationship if you use it beyond the first time, on the first Collector.

Rather than choosing to generate certificates a second time, sign certificates with the first generated VCM certificate, making that your Enterprise certificate, and manually add the signed certificates to subsequent Collectors before you install VCM. Each Collector needs its own Collector certificate, and access to the Enterprise certificate that issued it.

If all Agents are to be contacted by only a single Collector, then a single trust hierarchy and overall Enterprise certificate is not necessary. If you plan to have shared Collectors communicate with an Agent though, you cannot generate certificates during each Collector installation throughout your security environment.

Changing Certificates

Certificates always have an expiration date, after which they are not valid. The validity period for a certificate is a matter of policy and ranges from minutes to decades. In the case of expiring certificates, you can either renew or replace certificates.

Renewing Certificates

When you renew a certificate, you extend the validity period for the certificate and use the same key pair, issuer, and identifying information. Whatever mechanism was used to create the VCM certificates can be used to renew them.

You can renew a certificate by updating the expiration date. When you update the expiration date, a new certificate is issued with the same public key and identifying information as the old certificate. Because the only change is the validity period, it is safe to accept the new certificate at the same level of trust as the old one. Both certificates are valid for the same purposes, and both are usable during their validity periods.

When the Collector initiates communication with the Agent, it reveals the certification path from the Collector certificate back to its trusted root, typically the Enterprise certificate, to the Agent. For each certificate in the path, the Agent checks to see if it has a matching certificate in the local machine personal or root stores. If it finds a match in either location and the "new" certificates have different dates, the Agent installs the new certificates, and the current trust level is preserved.

No certificate is added to the trusted store unless an equivalent certificate is already present. The old certificates are not removed.

This renewal process only works for Collector certificates stored in the Agent certificate store. In mutual authentication in the other direction, Agent certificates do not have an automated renewal capability at the Collector certificate store.

Replacing Certificates

The only way to ensure the authenticity of a new root or trusted certificate is to receive it from a secure and trusted source. During installation, VCM Installation Manager handles Enterprise and Collector certificate installation and management.

Later, at VCM Agent installation, the Agent is configured to properly trust the Enterprise and Collector certificates. If the Enterprise and Collector certificates were updated with new expiration times, the updates are added to the Agents' certificate stores as described in "Renewing Certificates" on page 64.

The following circumstances require that you replace Enterprise and Collector certificates:

- Compromised private keys
- Security policies that govern the lifetime of keys
- Company or department changes that result in merging VCM environments
- Product evaluations that previously used VCM-generated certificates that are moved into production without reinstallation

Replace the Enterprise and Collector Certificates

After VCM installation, you can replace the certificates generated or selected during installation. To replace both the Enterprise and Collector certificates, follow these steps.

1. Create or obtain a new Enterprise certificate.

   To create an Enterprise certificate using the Makecert certificate creation tool, see "Create the Enterprise Certificate and First Collector Certificate" on page 71.

2. Create or obtain a new Collector certificate that is signed by the new Enterprise certificate.

   To create a Collector certificate using Makecert certificate creation tool, see "Create the Enterprise Certificate and First Collector Certificate" on page 71.

3. Import the new Enterprise certificate to the local computer trusted root store on the VCM Collector.

   See "Import a Certificate on Windows" on page 69.

4. Import the Collector certificate and the private key to the personal store on the VCM Collector.

   See "Import a Certificate on Windows" on page 69.

5. Update the Collector certificate thumbprint in the VCM Collector database.

   See "Update the Collector Certificate Thumbprint in the VCM Database" on page 74

6. Restart the Collector service.

7. Import the Enterprise certificate to the trusted root store on managed machines.

   See "Import a Certificate on Windows" on page 69.

   To place the new Enterprise certificate onto a Windows managed machine, you can install the VCM Agent with the Enable HTTP option selected, or change the protocol to DCOM and back to HTTP if the Collector can communicate with Agents using DCOM.

   For UNIX Agents, copy the certificates to the VCM Agent certificate store.

Replace Only the Collector Certificate

After VCM installation, you can replace the certificates generated or selected during installation. To replace only the Collector certificate, follow these steps.

1. Create or obtain a new Collector certificate (and associated private key) that is signed by the Enterprise certificate.

   To create a Collector certificate using the Makecert certificate creation tool, see "Creating Certificates Using Makecert" on page 70.

2. Import the Collector certificate and the private key to the personal store on the VCM Collector.
3. Update the Collector certificate thumbprint in the VCM Collector database.

   See "Update the Collector Certificate Thumbprint in the VCM Database" on page 74

4. Restart the Collector service.

Delivering Initial Certificates to Agents

VCM Agents use the Enterprise certificate to validate Collector certificates, so the Agent must store a copy of the Enterprise certificate as a trusted certificate. In most cases, VCM delivers and installs the Enterprise certificate as needed to the Agent. When installing or updating the Agent over HTTP from the Collector, the Enterprise certificate that is installed on the Agent comes from the CollectorData folder on the Collector.

- In a new Agent installation, all module files are installed. The Enterprise certificate is installed if and when the EcmComSocketListenerService module is installed. If the Enable HTTP option is not chosen for the installation, then the module and certificate are not installed.
- All upgrades of HTTP-enabled Agents from non-TLS Agents to TLS Agents receive a new version of the EcmComSocketListenerService and the Enterprise certificate. This also applies to upgrades that you perform with the "License and Install Agent on Discovered Machines" option when discovering machines in VCM.

Installing the Agent

You can use several methods to install the Agent.

- Install from disk media on Windows
- Run CMAgtInstall.exe over a network share on Windows
- Use Linux, UNIX, or Mac OS X packages
- Use a provisioning system

Installing on Windows with Disk Media

The VCM installation DVD does not contain certificates for Agents. Instead, the Agent installer requests the location of your VCM certificate, so you must have it preloaded on the managed machine before installing. To do so, copy the certificate file with the .pem extension from the CollectorData folder of the Collector.

Installing on Windows with CMAgtInstall.exe

The CMAgtInstall.exe installer executable file does not contain certificates for Agents. Instead, `CMAgtInstall.exe` requests the location of your VCM certificate, so you must have it preloaded on the managed machine before installing. To do so, copy the certificate file with the .pem extension from the CollectorData folder of the Collector.

NOTE The same guidelines apply if you are installing from an MSI installer.

Installing on Linux, UNIX, or Mac OS Packages

Each Linux, UNIX, or Mac OS X installation package is targeted for one or more supported platforms. If certificates were specified when the Collector was installed, they are embedded in the Agent installation package.

To manage the VCM UNIX Agent certificate store, use the CSI_ ManageCertificateStore utility and related help provided with your UNIX Agent installation package. For more information about Linux, UNIX, or Mac OS X Agent installation or packages and platforms, see the *VCM Administration Guide*.

Installing Using Provisioning

You can install the VCM Agent using a provisioning system or software push.

Installing the Agent with Provisioning on Windows

The manual installation program is available in EXE and MSI formats. Both versions allow you to specify the Enterprise certificate file with a command-line switch. The certificate installation step can also be omitted with 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 can push the Enterprise certificate to Agents by some other means and configure the provisioning system to omit certificate installation.

Installing the Agent with Provisioning on Linux, UNIX, or Mac OS X

Each Linux, UNIX, or Mac OS X installation package is targeted for one or more supported platforms. To install the Linux, UNIX, or Mac OS X Agent using a provisioning system, extract the installation package as appropriate, and deploy the extracted file with the provisioning system. The Enterprise certificate is embedded in the installation package. For more information about Linux, UNIX, or Mac OS X Agent installation, see the *VCM Administration Guide*.

Changing the Communication Protocol

For Windows Agents, you can change the communication protocol from DCOM to HTTP, or the reverse.

- Changing the protocol to HTTP installs the EcmComSocketListenerService module. The current Enterprise certificate is delivered with the EcmComSocketListenerService module.
- Changing the protocol to DCOM uninstalls the EcmComSocketListenerService module from the Agent. Because DCOM does not use certificates, the Agent stops using them. Changes to the Enterprise certificate are not propagated to the Agent until you set the protocol back to HTTP, at which point the current Enterprise certificate is delivered or redelivered.

Storing and Transporting Certificates

A certificate contains the public half of a key pair, identifying information, and an authenticating signature. Although none of this information is confidential, you must ensure and maintain the authenticity of certificates that you distribute so that untrustworthy certificates are never used inadvertently.

You can store a certificate in a format that includes the private key. In that case, the data is sensitive, and you must safeguard, store, and transport it securely.

NOTE To import or export a certificate to UNIX, use the CSI_ ManageCertificateStore utility provided with your VCM UNIX Agent installation package.

Access the Windows Certificate Store

To work with certificates on a Windows machine, open the Microsoft Management Console (MMC) and Certificates snap-in.

Procedure

1. At the command prompt, type **mmc**.
2. Select **File > Add/Remove Snap-in**.
3. Select **Certificates** and click **Add**.
4. Select **Computer account** and click **Next**.
5. Select **Local computer** and click **Finish**.
6. Click **OK**.

Export a Certificate on Windows

One way to export a certificate is through the Microsoft Management Console (MMC).

Prerequisite

Open the certificate store. See "Access the Windows Certificate Store" on page 68.

Procedure

1. In the certificates stores, navigate to the certificate to export.
2. Right click the certificate, and select **All Tasks > Export**.
3. In the Certificate Export wizard, click **Next**.
4. If the private key for the certificate is available and exportable, the Export Private Key wizard page appears, and you can opt to export the private key.
5. On the Export File Format wizard page, if you are exporting the private key, select the PFX format.

   Otherwise, select the Base-64 encoded X.509 format.
6. If you are exporting the private key, enter a password to protect the private key. The password is required when importing the file.
7. Click **Next**.
8. Browse to the folder where you are storing the exported certificate file.

If you are exporting the private key, store the file to a secure folder.

9. Type a name for the certificate file and click **Save**.
10. Click **Next**.
11. Review your settings and click **Finish**.

Import a Certificate on Windows

A computer might have file associations that allow you to click the certificate file to import it to the store for the current user. If you use this method, move the imported certificate from the user store to the corresponding local computer store, which is where VCM looks for certificates.

NOTE MMC supports dragging certificates, but the feature does not always work correctly.

If your computer does not allow you to click the certificate file to import it, import a certificate through the Microsoft Management Console (MMC).

Prerequisite

Open the certificate store. See "Access the Windows Certificate Store" on page 68.

Procedure

1. Select the store into which to import the certificate.
2. Select **Action > All Tasks > Import**.
3. In the Certificate Import wizard, click **Next**.
4. Browse to and select the certificate file, and click **Open**.

   The PFX or CER file format is acceptable. The PEM format is typically a synonym for CER and is commonly used on UNIX.
5. Click **Next**.
6. If the file contains a private key, enter the password.

   You have the option to make the private key exportable whenever you export the certificate from this system.

   IMPORTANT Do not enable strong protection.
7. Click **Next**.
8. Verify or browse to the store into which to import the certificate.

   Alternatively, select the option to let Windows choose the store.
9. Review your settings and click **Finish**.

Mark a Certificate as Authorized on Windows

To manually authorize a certificate on a Windows Agent machine, do the following:

CAUTION This procedure involves carefully editing values and adding them to the Windows Registry.

Prerequisites

- Open the certificate store. See "Access the Windows Certificate Store" on page 68.
- Import the certificate into the Agent machine. See "Import a Certificate on Windows" on page 69.

Procedure

1. Open a text editor. You need a blank page on which to temporarily paste some long values.
2. Browse to the store and certificate, right-click, and select **Open**.
3. Select the **Details** tab.
4. In the list of fields, select **Subject**.
5. In the lower pane, highlight and copy the entire common name value to a line in your text editor.

   The common name is shown as CN={*common-name-value*}.
6. In the list of fields, select **Thumbprint**.
7. In the lower pane, highlight and copy the entire thumbprint to another line in your text editor.

   The thumbprint is a series of 32-bit hexadecimal values separated by spaces.
8. In your text editor, carefully remove the spaces from the thumbprint so that it becomes one long alphanumeric value.
9. Start the Registry editor (regedit).
10. Navigate to

    `HKEY_LOCAL_MACHINE\SOFTWARE\Configuresoft\CSI\5.0\Listener\Authorized`
11. Add a new String Value (REG_SZ).
12. By pasting the common name from the text editor, rename the new String Value to perfectly match the common name from the certificate.
13. By pasting the thumbprint from the text editor, modify the string value data so that it perfectly matches the spaceless thumbprint.
14. Close the Registry editor.

Creating Certificates Using Makecert

VCM is designed to run in TLS mode with two levels of certificates. An Enterprise certificate is the ultimate trusted authority. The Enterprise certificate signs all Collector certificates. All Agents have access to the Enterprise certificate as a trusted authority. As a result, any Collector certificate can sign an Agent certificate, and any Agent can mutually authenticate with multiple Collectors.

Some steps can be simplified if the Enterprise and Collector systems are the same machine or if the Enterprise or Collector machines are certificate servers. In the following example, the Enterprise machine is the same as the (first) Collector machine.

Obtain the SDK download from Microsoft, which includes the Makecert certificate creation tool, the cert2spc software publisher certificate test tool, the pvkimprt PVK digital certificate files importer, and related utilities. For more information, visit the Microsoft Developer Network and search for the downloads by platform.

- **Pre-Vista**. Windows Server 2003 SP1 Platform SDK full download
- **Vista**. Windows SDK for Windows Server 2008 and .NET Framework version 3.5

Create the Enterprise Certificate and First Collector Certificate

In this process, the Enterprise and first Collector systems are the same machine. See "Makecert Options" on page 72 for details about the command-line switches used here.

1. Type the following command to create the CM Enterprise certificate:

```
makecert -pe -n "<enterprise-cert-name>" -ss Root -sr LocalMachine -r -sky
exchange -sk "<enterprise-key-name>" -b mm/dd/yyyy -e mm/dd/yyyy -len 1024
-h 2 -cy authority -eku 1.3.6.1.5.5.7.3.1 <filename[.cer | .pem]>
```

Example

```
makecert -pe -n "CN = CM Enterprise Certificate AAAAAA" -ss Root -sr
LocalMachine -r -sky exchange -sk "CM Enterprise Certificate AAAAAA" -len
1024 -h 2 -cy authority -eku 1.3.6.1.5.5.7.3.1
```

NOTE VCM programmatically embeds a long GUID, represented by AAAAAA or BBBBBB, in the Common Name to ensure that the name is unique. You do not need a long GUID in the manual process though. Any unique identifier is sufficient.

---

2. Type the following command to create the first Collector certificate, signed by the Enterprise certificate.

```
makecert -pe -n "<collector-cert-name>" -ss My -sr LocalMachine -sky
exchange -sk <collector-cert-name> -b mm/dd/yyyy -e mm/dd/yyyy -len 1024 -
in <Enterprise_cert_common_name> -is Root -ir LocalMachine -cy authority
<collector-cert-name.[cer|pem]>
```

When the Enterprise machine is separate, and the Enterprise certificate is not stored with its private key on the Collector, follow the steps for creating an additional Collector, but use them to create the first Collector. See "Create Certificates for Additional Collectors" on page 71.

Create Certificates for Additional Collectors

If you need additional Collectors, or if the first Collector is a different machine from the Enterprise system, create additional Collector certificates signed by the Enterprise certificate. This process is supported even if the original certificates were generated by the VCM Installation Manager.

Follow these steps on the Enterprise machine, because you must access the private key for the Enterprise certificate. You are creating an installable file that includes the new Collector private key, without storing that key on the Enterprise machine. See "Makecert Options" on page 72 for details about the command-line switches used here.

1. Type the following command:

```
makecert -pe -n "<collector-cert-name>" -sky exchange -sv "<collector-
cert-key-file>" -b mm/dd/yyyy -e mm/dd/yyyy -len 1024 -in "<Enterprise_
cert_common_name>" -is Root -ir LocalMachine -cy authority -eku
1.3.6.1.5.5.7.3.1 " <collector-cert-name.[pem|cer]>"
```

Example

```
makecert -pe -n "CN=CM Collector Certificate BBBBBB" -sky exchange -sv "CM
Collector BBBBBB.pvk" -b 04/07/2008 -e 04/07/2018 -len 1024 -in "CM
Enterprise Certificate AAAAAA" -is Root -ir LocalMachine -cy authority -
eku 1.3.6.1.5.5.7.3.1 "CM Collector BBBBBB.pem"
```

2. Type the following command to convert the x509 certificate file to a file-based certificate store in the named SPC file.

   ```
   cert2spc <collector-cert-name>.cer <collector-cert-name>.spc
   ```

   Example

   ```
   cert2spc "Collector Certificate BBBBBB.cer" "Collector Certificate
   BBBBBB.spc"
   ```

3. Type the following command to export the file-based certificate store, that contains the certificate, and the private key in the key file to a PFX file.

   ```
   pvkimprt -pfx <collector-cert-name>.spc <collector-cert-key-file>
   ```

   This launches the Certificate Export Wizard. Select Yes, and export the private key. Keep the PFX format. Clear all of the check boxes. Optionally, choose a password for secure transport of the file (recommended).

   Example

   ```
   vkimprt -pfx "CM Collector Certificate BBBBBB.spc" "CM Collector
   Certificate BBBBBB.pvk"
   ```

4. Remove your temporary files, especially the key file.
5. Move the PFX file containing the new Collector certificate and the Enterprise certificate export file to the new Collector machine.

   The Enterprise certificate file is located in the CollectorData folder of the initial Collector, typically `C:\Program Files\VMware\VCM\CollectorData`, or you can export it from the local machine trusted root system store. The export file has a .pem extension.

NOTE An alternative way to make a certificate for an additional Collector is to generate a key pair and certificate request on the additional Collector machine, and move only that.

Importing Certificates for Additional Collectors

After you create certificates for an additional Collector, import them to the additional Collector before you install VCM. See "Import a Certificate on Windows" on page 69

- Import the Enterprise certificate to the local machine trusted root store on the additional Collector.
- Import the Collector certificate to the local machine personal store on the additional Collector.

IMPORTANT If you are replacing certificates, also import the Enterprise certificate to the Agent certificate stores on managed machines. See "Delivering Initial Certificates to Agents" on page 66.

Makecert Options

When you use Makecert commands, you can use options to specify the results in the utility output.

NOTE VCM programmatically uses a long GUID, represented by AAAAAA or BBBBBB, to ensure that a name is unique. You do not need a long GUID in a manual process though. Any unique identifier is sufficient.

Table 13–1. Makecert Command-Line Options

Option	Description
-b, -e	Specify begin and end dates. Choose appropriate dates, or omit them. You cannot enter a time with the date. The time is always assumed to be 12:00 AM GMT. For example, if you choose the current day, the assumed time is probably very early that same morning, depending on your location.
-cy authority	Certificates are either *authority* or *end*. End certificates are not allowed to sign other certificates.
-eku 1.3.6.1.5.5.7.3.1	Server authentication OID, required only for the Collector certificate.
<*filename*>	Optional export file name. This file does not contain the private key. The file should have a .cer or .pem extension.
-h 2	Max height of certificate chains. A value of 2 for the Enterprise allows it to sign a Collector certificate that can sign Agent certificates.
-in <*name*>	Name of the signing certificate. The common name (CN field) of the Enterprise certificate when creating Collector certificates.
-ir LocalMachine	Account of the signing certificate. VCM and the examples use *LocalMachine*.
-is Root	Location of the signing certificate. *Root* is the trusted root store.
-len	Key length. Optional.
-n <*collector-cert-name*>	Subject of the Collector certificate. Must be a valid x509 identifier. Collector certificates generated by the VCM installer have the form: "CN=VMware VCM Collector Certificate AAAAAA, T=VMware VCM Certificate 7529006C-222F-4EBF-A7E7-F6AB15DB626F, O=<customer_name>" ■ CN: Generic name based on a GUID generated for each set of certificates created. Required. ■ T: Static field identifying VCM generated certificates and is the same for all generated certificates. Optional. ■ OU: Static field. Optional. ■ O: Contains the customer name identified in the license file. Optional.
-n <*enterprise-cert-name*>	Subject of the Enterprise certificate. Must be a valid x509 identifier. Enterprise certificates generated by

Option	Description
	the VCM installer have the form: "CN=VMware VCM Collector Certificate AAAAAA, T=VMware VCM Certificate 7529006C-222F-4EBF-A7E7-F6AB15DB626F, O=<customer_name>" ■ CN: Generic name based on a GUID generated for each set of certificates created. Required. ■ T: Static field identifying VCM generated certificates and is the same for all generated certificates. Optional. ■ OU: Static field. Optional. ■ O: Contains the customer name identified in the license file. Optional.
-pe	Make the private key exportable.
-r	Self sign the certificate.
-sk <*collector-key-name*>	Names the key container, for easy reference later. This name does not need to be related to the certificate name.
-sk <*enterprise-key-name*>	Names the key container, for easy reference later. This name does not need to be related to the certificate name.
-sky exchange	Use the key exchange key pair, rather than the signature key pair.
-sr LocalMachine	Specifies the subject's certificate store location. VCM and the examples use *LocalMachine*.
-ss My	Specifies the subject's certificate store name that stores the output certificate. *My* designates the personal certificate store.
-ss Root	Specifies the subject's certificate store name that stores the output certificate. *Root* designates the Trusted Root certificate store.
-sv <*collector-cert-key-file*>	Store the private key in a file instead of the CSP. The extension is usually .svk or .pvk.

Update the Collector Certificate Thumbprint in the VCM Database

When you have a new certificate, update the Collector certificate thumbprint in the VCM database.

Procedure

1. In MMC, right click the Collector certificate and select **Open**.
2. Click the **Details** tab.
3. Scroll down to the **Thumbprint**. Copy the value to the clipboard or a text editor.
4. Create and run the following SQL script to update the certificate in the VCM Collector database. Replace xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx with your Collector certificate thumbprint.

```
use <insert your VCM SB name here>
update ecm_sysdat_configuration_values
set configuration_value = upper(replace(
'xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx'
,' ',''))
where configuration_name='config_security_certificate_fingerprint'
```

Managing the VCM UNIX Agent Certificate Store

The VCM UNIX Agent certificate store is a protected data storage area that holds Enterprise and Collector certificates for server authentication, and the Agent certificate and private key for mutual authentication. Although this store is not encrypted, it is protected from casual viewing.

Much of the interaction with the VCM UNIX Agent certificate store is taken care of for the user. VCM UNIX installation packages are updated with the Enterprise certificate if one is specified when the Collector is installed. This certificate is inserted into the certificate store during the VCM UNIX Agent installation process. The user can select an alternative certificate directory during the VCM UNIX Agent installation.

IMPORTANT The self-signed root of the trust chain for the Collector certificate is not always the Enterprise certificate. In Linux and UNIX, you also must manually add the self-signed root of the trust chain for the Collector certificate to the Agent certificate store, when the self-signed root is different than the Enterprise certificate.

Additionally, when VCM Collector certificates are updated with extended expiration dates, in many cases the new certificate is added to the store.

Using CSI_ManageCertificateStore

With the CSI_ManageCertificateStore command-line tool, you can view and modify the contents of the VCM UNIX Agent certificate store.

In these examples, the UNIX VCM Agent was installed to the default location of `/opt/CMAgent`. If your installation is different, adjust the instructions to fit your situation.

Environment Variables

Typically, CSI_ManageCertificateStore is run as root, but any login that is a member of the cfgsoft group can run it as well.

To use CSI_ManageCertificateStore, first set the following environment variables:

```
LD_LIBRARY_PATH=/opt/CMAgent/CFC/3.0/lib:/opt/CMAgent/ThirdParty/1.0/lib:$
LD_LIBRARY_PATH

export LD_LIBRARY_PATH

CSI_REGISTRY_PATH=/opt/CMAgent

export CSI_REGISTRY_PATH

PATH=/opt/CMAgent/CFC/3.0/bin:$PATH

export PATH
```

For HPUX platforms, use SHLIB_PATH in place of LD_LIBRARY_PATH.

For AIX platforms, use LIBPATH in place of LD_LIBRARY_PATH.

CSI_ManageCertificateStore Options

The following printout of the CSI_ManageCertificateStore manpage is useful in understanding the CSI_ ManageCertificateStore command options.

```
# CSI_ManageCertificateStore -?


Usage: /opt/CMAgent/CFC/3.0/bin/CSI_ManageCertificateStore
-[?h]
[-c certificate_store_name] -[adel] [-g fingerprint] [-s subject] [-f
filename]
[-c certificate_store_name] -[iu] -f filename
-h Display this help and exit
-? Display this help and exit
-c The name of the certificate store. This name includes the path. Defaults
to registry value
-a Perform action on all certificates in the store
-d Delete from the certificate store
-e Export certificate(s) and associated key(s) from the certificate store to
file(s) named fingerprint-cert.pem and fingerprint-key.pem ('fingerprint' is
the hex SHA1 hash of the certificate)
-f File that contains a certificate external to the certificate store to use.
The certificate in the file must be in PEM format
-g SHA1 hash fingerprint of the certificate in the store to act upon
-i Insert certificate into the certificate store
-k File that contains the private key associated with the certificate.
Private certificate keys are only used for mutual authentication. The key
must be in PEM format. Associating a key with a certificate will cause the
registry to be modified to setup mutual authentication
-l List entries from the certificate store
-n Common name of the certificates in the store to act upon
-p Passphrase for the private key. Needed if the private key PEM file was
passphrase protected, or if the exported key should be protected
-s Subject of the certificates in the store to act upon
-u Update certificate in the certificate store
-z Mark a certificate as authorized
```

Common Uses

(All commands are run from the /opt/CMAgent/CFC/3.0/bin/ directory.)

Insert a new certificate into the certificate store:

```
CSI_ManageCertificateStore -i -f filename
```

Insert a new certificate into the certificate store and mark it as authorized:

```
CSI_ManageCertificateStore -iz -f filename
```

Update an existing certificate in the certificate store:

```
CSI_ManageCertificateStore -u -f filename
```

Add a key to an existing certificate in the certificate store:

```
CSI_ManageCertificateStore -u -f filename -k key_filename
```

Delete an existing certificate from the certificate store:

```
CSI_ManageCertificateStore -d -f filename
```

or

```
CSI_ManageCertificateStore -d -g fingerprint
```

Delete existing certificates from the certificate store:

```
CSI_ManageCertificateStore -d -s subject
```

Delete all existing certificates from the certificate store:

```
CSI_ManageCertificateStore -d -a
```

Display an existing certificate from the certificate store:

```
CSI_ManageCertificateStore -l -f filename
```

or

```
CSI_ManageCertificateStore -l -g fingerprint
```

Display existing certificates from the certificate store:

```
CSI_ManageCertificateStore -l -s subject
```

Display all existing certificates from the certificate store:

```
CSI_ManageCertificateStore -l
```

Export an existing certificate and associated key from the certificate store:

```
CSI_ManageCertificateStore -e -f filename
```

or

```
CSI_ManageCertificateStore -e -g fingerprint
```

Export existing certificates and associated keys from the certificate store:

```
CSI_ManageCertificateStore -e -s subject
```

Export all existing certificates and associated keys from the certificate store:

```
CSI_ManageCertificateStore -e -a
```

CSI_ManageCertificateStore Output

To provide useful feedback to the user, CSI_ManageCertificateStore displays information about each certificate that the command acts on.

The displayed information is as follows:

{*Action*} `Certificate:`

`Fingerprint:` {*SHA1 hash fingerprint of the certificate*}

`Common Name:` {*Common name of the certificate*}

`Subject:` {*Subject of the certificate*}

Examples of CSI_ManageCertificateStore Use

The following are examples of CSI_ManageCertificateStore use, with additional explanation to give you a better sense of the tool features.

List Certificate Store Contents

By default, the `-l` option for listing certificates causes all certificates in the store to be listed. This behavior can be modified by specifying options that narrow the requested results. For example, `-g fingerprint` always limits the action to the single matching certificate.

```
# CSI_ManageCertificateStore -l


Certificate:
Fingerprint: 1C564431B9B28DC4D24BB920FD98B539FF57C0C2
Common Name: testca1.VMware.com
Subject : CN = testca1.VMware.com, ST = Colorado, C = US, emailAddress =
ca1@VMware.com, O = VMware, Inc., OU = Testing
Certificate:
Fingerprint: 779403A8D53B1258F3EB09E62A8D17B14CD81DC3
Common Name: Enterprise Certificate 9ACD1B00-42CF-4794-B4E8-B6BDBEC1D4B6
Subject : O = CSI-SE, OU = VMware vCenter Configuration Manager, title = VCM
Certificate 7529006C-222F-4EBF-A7E7-F6AB15DB626F, CN = Enterprise Certificate
9ACD1B00-42CF-4794-B4E8-B6BDBEC1D4B6
Certificate:
Fingerprint: 0041AB5ECF869E1D6A38389A6B834D5768932397
Common Name: Enterprise Certificate 2CA82018-20E1-4487-8A02-DA7A2CFD4304
Subject : O = VMware, Inc., OU = VMware vCenter Configuration Manager, title
= VCM Certificate 7529006C-222F-4EBF-A7E7-F6AB15DB626F, CN = Enterprise
Certificate 2CA82018-20E1-4487-8A02-DA7A2CFD4304
Certificate:
Fingerprint: 765831AFF8E15332F78D7CBC805F1C68089C8640
Common Name: Enterprise Certificate 7780CB3B-281F-47DF-B48B-5BDE5806C156
Subject : O = QAT, OU = VMware vCenter Configuration Manager, title = VCM
Certificate 7529006C-222F-4EBF-A7E7-F6AB15DB626F, CN = Enterprise Certificate
7780CB3B-281F-47DF-B48B-5BDE5806C156
```

Delete a Certificate from the Store

The following example shows how to delete a certificate using CSI_ManageCertificateStore.

```
# CSI_ManageCertificateStore -d -f Enterprise_Certificate_2CA82018-20E1-4487-
8A02-DA7A2CFD4304.pem


Deleting Certificate:
Fingerprint: 0041AB5ECF869E1D6A38389A6B834D5768932397
Common Name: Enterprise Certificate 2CA82018-20E1-4487-8A02-DA7A2CFD4304
Subject : O = VMware, Inc., OU = VMware vCenter Configuration Manager, title
= VCM Certificate 7529006C-222F-4EBF-A7E7-F6AB15DB626F, CN = Enterprise
Certificate 2CA82018-20E1-4487-8A02-DA7A2CFD4304
```

NOTE The command `CSI_ManageCertificateStore -d -g 0041AB5ECF869E1D6A38389A6B834D5768932397` would have produced the same result.

Insert a Certificate into the Store

The following example shows how to insert a certificate using CSI_ManageCertificateStore.

```
# CSI_ManageCertificateStore -i -f Enterprise_Certificate_2CA82018-20E1-4487-
8A02-DA7A2CFD4304.pem
```

```
Inserting Certificate:
Fingerprint: 0041AB5ECF869E1D6A38389A6B834D5768932397
Common Name: Enterprise Certificate 2CA82018-20E1-4487-8A02-DA7A2CFD4304
Subject : O =VMware, Inc., OU = VMware vCenter Configuration Manager, title =
VCM Certificate 7529006C-222F-4EBF-A7E7-F6AB15DB626F, CN = Enterprise
Certificate 2CA82018-20E1-4487-8A02-DA7A2CFD4304
```

Export Certificates from the Store

By default, the `-e` option for exporting certificates causes all certificates in the store to be exported. This behavior can be modified by specifying options that narrow the requested results. For example, `-g fingerprint` always limits the action to the single matching certificate.

```
# CSI_ManageCertificateStore -e


Exporting Certificate:
Fingerprint: 1C564431B9B28DC4D24BB920FD98B539FF57C0C2
Common Name: testca1.VMware.com
Subject : CN = testca1.VMware.com, ST = Colorado, C = US, emailAddress =
ca1@VMware.com, O =VMware, Inc., OU = Testing
Exporting Certificate:
Fingerprint: 779403A8D53B1258F3EB09E62A8D17B14CD81DC3
Common Name: Enterprise Certificate 9ACD1B00-42CF-4794-B4E8-B6BDBEC1D4B6
Subject : O = CSI-SE, OU = VMware vCenter Configuration Manager, title = VCM
Certificate 7529006C-222F-4EBF-A7E7-F6AB15DB626F, CN = Enterprise Certificate
9ACD1B00-42CF-4794-B4E8-B6BDBEC1D4B6
Exporting Certificate:
Fingerprint: 0041AB5ECF869E1D6A38389A6B834D5768932397
Common Name: Enterprise Certificate 2CA82018-20E1-4487-8A02-DA7A2CFD4304
Subject : O =VMware, Inc., OU = VMware vCenter Configuration Manager, title =
VCM Certificate 7529006C-222F-4EBF-A7E7-F6AB15DB626F, CN = Enterprise
Certificate 2CA82018-20E1-4487-8A02-DA7A2CFD4304
Exporting Certificate:
Fingerprint: 765831AFF8E15332F78D7CBC805F1C68089C8640
Common Name: Enterprise Certificate 7780CB3B-281F-47DF-B48B-5BDE5806C156
Subject : O = QAT, OU = VMware vCenter Configuration Manager, title = VCM
Certificate 7529006C-222F-4EBF-A7E7-F6AB15DB626F, CN = Enterprise Certificate
7780CB3B-281F-47DF-B48B-5BDE5806C156
```

This command produced the following files:

```
0041AB5ECF869E1D6A38389A6B834D5768932397-cert.pem
1C564431B9B28DC4D24BB920FD98B539FF57C0C2-cert.pem
765831AFF8E15332F78D7CBC805F1C68089C8640-cert.pem
779403A8D53B1258F3EB09E62A8D17B14CD81DC3-cert.pem
```

When the certificate in the store has an associated private key for mutual authentication, an additional file named `fingerprint-key.pem` is created. The fingerprint used in the name is the fingerprint of the associated certificate.

14 Supplemental References

This chapter provides reference information about VCM and its security implementation.

Cryptography

If your organization must conform to the Federal Information Processing Standards (FIPS) for cryptography, use the standards that VCM supports.

FIPS for Windows

For the following Windows platforms, VCM uses the Microsoft CryptoAPI and the Microsoft Cryptographic Service Providers (CSPs), which is included with Microsoft Windows.

Table 14–1. FIPS Support for Windows Machines

Operating System	Version	Hardware Platform	FIPS Module Certificate
.NET	3	cil	894
Windows Vista	1	x86	899
Windows Vista	1	x86 and 64-bit	894
Windows Vista	1	x86 and 64-bit	893
Windows Vista	1	x86 and 64-bit	892
Windows 2003	SP2	x86 and 64-bit	875
Windows 2003	SP1	x86 and 64-bit	382
Windows 2003	SP1	x86 and 64-bit	381
Windows 2003	Gold	x86 and 64-bit	382
Windows 2003	Gold	x86 and 64-bit	381
Windows XP	SP2	x86	240
Windows XP	SP2	x86	238
Windows XP	SP1	x86	240
Windows XP	Gold	x86	240
Windows XP	Gold	x86	238

Operating System	Version	Hardware Platform	FIPS Module Certificate
Windows 2000	All	x86	103
Windows 2008	1	x86 and 64-bit; Itanium is not supported.	See "Cryptographic RSA Enhanced Validated Modules" on page 82 and "Cryptographic DSS Enhanced Validated Modules" on page 82.
Windows Server 2008 R2	RTM		
Windows All	2000	x86	76

Cryptographic RSA Enhanced Validated Modules

The Microsoft Cryptography API (CAPI) supports the following validated versions of RSA enhanced modules, and the operating systems for which the testing is valid.

Table 14–2. RSA Enhanced Validated Modules

RSAENH Validated Operating Systems	Validated Versions	FIPS Certificate #	FIPS Version Validated
Windows 2000	5.0.2150.1	#76	140–1
Windows 2000 SP1	5.0.2150.1391	#103	140–1
Windows 2000 SP2	5.0.2195.2228	#103	140–1
Windows 2000 SP3	5.0.2195.3665	#103	140–1
Windows XP	5.1.2518.0	#238	140–1
Windows XP SP1	5.1.2600.1029	#238	140–1
Windows XP SP2	5.1.2600.2161	#238	140–1
Windows XP Professional SP3	5.1.2600.5507	#989	140–2
Vista Ultimate Edition	6.0.6000.16386	#893	140–2
Vista Ultimate Edition SP1	6.0.6001.22202	#1002	140–2
Windows Server 2008	6.0.6001.22202	#1010	140–2

Cryptographic DSS Enhanced Validated Modules

The Microsoft Cryptography API (CAPI) supports the following validated versions of DSS enhanced modules, and the operating systems for which the testing is valid.

Table 14–3. DSS Enhanced Validated Modules

DSSENH Validated Operating Systems	Validated Versions	FIPS Certificate #	FIPS Version Validated
Windows 2000	5.0.2150.1	#76	140–1
Windows 2000 SP1	5.0.2150.1391	#103	140–1

DSSENH Validated Operating Systems	Validated Versions	FIPS Certificate #	FIPS Version Validated
Windows 2000 SP2	5.0.2195.2228	#103	140–1
Windows 2000 SP3	5.0.2195.3665	#103	140–1
Windows XP	5.1.2518.0	#240	140–1
Windows XP SP2	5.1.2600.2133	#240	140–1
Windows XP Professional SP3	5.1.2600.5507	#990	140–2
Vista Ultimate Edition	6.0.6000.16386	#894	140–2
Vista Ultimate Edition SP1	6.0.6001.18000	#1003	140–2
Windows Server 2008	6.0.6001.18000	#1009	140–2

FIPS Used by VCM Agent Proxies

The VCM Agent Proxy uses the OpenSSL FIPS v1.1.2, which is validated to the 918 certificate.

Export Considerations

VCM 5.5 is subject to U.S. Export Administration Regulations and is classified as follows:

Export Control Classification number (ECCN)	5D002 / ENC (ENCRYPTION)
Commodity Classification Automated Tracking System (CCATS)	N/A
Harmonized Tariff Schedule Number (HTS)	8523.40.2020
Export Registration Number (ERN) applicable	Yes, #100235

The following technologies are included or supported in VCM 5.5.

- Asymmetric algorithms, such as RSA or Diffie-Hellman, and associated key lengths:

  RSA 1024, 2048, 3096

- Encryption modes, such as cipher feedback or cipher block chaining:

  Electronic Codebook Mode (ECB)
  Cipher Block Chaining Mode (CBC)
  Cipher Feedback Mode (CFB)

- Encryption algorithm implementations or integrations; such as statically or dynamically linked, integrated into the object code, standalone library files, or hard wired into a device:

  VCM does not implement cryptography; it uses purchased, open source, or preinstalled libraries. The following libraries are dynamically linked:

  OpenSSL-FIPS, OpenSSL, mcrypt, nss

  RSAENH
  DSSENH
  RSABASE
  DSABASE

  The following modules are statically linked into some components:

OpenSSL-FIPS, OpenSSL, libssh2

- Communication protocols; such as TCP, Telnet, X.25, IEEE 802.11, IEEE 802.16, or SIP:

  Communication takes place over TCP/IP within encrypted channels using Microsoft DCOM, SSL, or TLS (SSL v3.1+). The following protocols are used within or to construct the channels:

  TCP
  UDP
  HTTP
  FTP
  TFTP
  DHCP
  SNMP

- Encryption protocols; such as SSL, TSL, SSH, IPSEC, IKE, SRTP, ECCN, MD5, SHA, X.509, or PKCS standards:

  TLS (Transport Level Security, considered to be Secure Socket Layer v3.1)
  SSL (Secure Socket Layer v3.0)
  SSH (Secure shell)
  HTTPS (HTTP over an SSL channel)
  DCOM (Microsoft Distributed COM)
  PKCS 1 (RSA Encryption Standard)
  PKCS 7 (Cryptographic Message Format)
  PKCS 10 (Certificate Signing Request)
  SHA
  MD5
  X509 Certificates

VCM Ports

VCM uses the following ports.

Table 14–4. VCM Port Usage

Port	Transport	Usage
21	TCP	File Transfer Protocol (FTP)
53	TCP, UDP	Domain Name System (DNS)
68	UDP	OS Provisioning Server bootpd/DHCP
69	UDP	OS Provisioning Server TFTP
80	TCP	OS Provisioning Server HTTP
88	TCP, UDP	Kerberos
123	TCP	Network Time Protocol (NTP)
135	TCP, UDP	Remote procedure call (RPC) endpoint mapper (EPMAP)
137	TCP, UDP	Network basic input/output system (NetBIOS) name service
138	UDP	NetBIOS Datagram Service
162	UDP	Simple Network Management Protocol (SNMP)

Port	Transport	Usage
389	TCP, UDP	Lightweight Directory Access Protocol (LDAP)
443	TCP	HTTPS (HTTP over SSL/TLS)
445	TCP, UDP	Server message block (SMB) over IP (Microsoft-DS)
500	TCP, UDP	Internet Security Association and Key Management Protocol (ISAKMP)
636	TCP	LDAP over SSL
1433	TCP	SQL Server
1434	UDP	SQL Server Database Management System Monitor
2383	TCP, UDP	SQL Server Analysis Services
3268	TCP	Global Catalog LDAP
3269	TCP	Global Catalog LDAP SSL
3389	TCP, UDP	Remote Desktop Protocol (RDP)
4500	TCP, UDP	Network Address Translation (NAT)
5355	TCP, UDP	Link Local Multicast Name Resolution (LLMNR) protocol
8882	TCP	EMC Ionix
21307		OS Provisioning Server Repository Server
21309		OS Provisioning Server Hardware Discovery
26542		Agent HTTP communication (default that can be changed)
40610		OS Provisioning Server
47001		DCOM dynamic port
49152		DCOM dynamic port
49153		DCOM dynamic port
49154		DCOM dynamic port
49176		DCOM dynamic port
49178		DCOM dynamic port
49179		DCOM dynamic port
54294		DCOM dynamic port
58613		DCOM dynamic port
58615		DCOM dynamic port
61615		DCOM dynamic port

Index