VMware vCenter Configuration Manager Hardware and Software Requirements Guide

vCenter Configuration Manager 5.4

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000484-00

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

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

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

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

Contents

About This Book

The *VMware vCenter Configuration Manager Hardware and Software Requirements Guide* describes the hardware and software requirements necessary for a successful VMware vCenter Configuration Manager (VCM) installation.

This document contains the following information:

- Hardware requirements for VCM Collector machines
- Hardware requirements for VCM Agent machines
- Software requirements and procedures for verifying or installing required components
- Supplemental reference information

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

The *VCM Hardware and Software Requirements Guide* applies to VCM 5.4, Foundation Checker 5.4, and Service Desk Connector 1.3.0.

Intended Audience

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

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

Document Feedback

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

VMware VCM Documentation

The vCenter Configuration Manager (VCM) documentation consists of the *VCM Hardware and Software Requirements Guide*, *VCM Foundation Checker User's Guide*, *VCM Installation and Getting Started Guide*, VCM online Help, and other associated documentation.

Technical Support and Education Resources

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

Online and Telephone Support

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

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

Support Offerings

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

VMware Professional Services

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

1 Overview

This manual helps you determine your specific hardware and software requirements for VMware vCenter Configuration Manager (VCM) and helps you install and configure the prerequisites necessary for a successful installation.

To determine your hardware and software requirements, you must begin by considering the answers to several questions. Worksheets are available later in this document to help you determine the answers to these questions.

- How many Windows Servers and Workstations and UNIX/Linux machines do you plan to license?
- How often do you intend to collect data?
- How much data do you intend to collect?
- How long do you plan to retain the data that you collect?
- What additional VCM components do you intend to use? See the Download VMware vCenter Configuration Manager Web site for more information about VCM components.
- Do you fully understand your VCM security requirements? See the VCM Security Environment Requirements Technical White Paper on the Download VMware vCenter Configuration Manager Web site.

To successfully install VCM, you must complete the preparatory tasks in order.

1. Understand how VCM and its related components are installed (described in this chapter).
2. Determine your VCM Collector hardware requirements based on the number of machines in your enterprise and the VCM components that you plan to license. See "Hardware Requirements for Collector Machines" on page 11.
3. Determine your VCM Agent hardware requirements based on the VCM components that you plan to license. A list of supported operating systems is included. See "Hardware and Operating System Requirements for Agent Machines" on page 15.
4. Prepare the Windows server to install VCM by installing and configuring the necessary software prerequisites. See "Software and Operating System Requirements for Collector Machines" on page 25.
5. Configure SQL Server to fine-tune the settings. See "Configure SQL Server for VCM" on page 47.

Complete each of the activities and procedures in the order in which they appear. After you complete these tasks, you can run Foundation Checker to ensure your system is ready to install VCM. Foundation Checker is a VCM application that scans the Collector machine for the necessary prerequisites.

If you have questions about the Windows server/workstation or UNIX machine configuration, or about any requirements not answered in this document, contact your VMware account representative or VMware Customer Support.

Agent and Collector Host OS Platform Support

All Agent and Collector host OS platform support is specific to versions and editions indicated in the supported platforms table in "Hardware and Operating System Requirements for Agent Machines" on page 15. All installations that have been tested use the vendor's default configuration, except as noted. A variety of vendor-supplied, third-party, and custom lock downs, endpoint security products, policies, and restricted system configurations can reduce or block the performance or functionality of VCM components. Troubleshooting and support of VCM components in such locked-down or reconfigured environments is not included under the standard product maintenance agreement. Support in such environments is available through an additional Professional Services engagement.

Understand the VCM Installation Manager

All VCM components and tools are installed with the VCM Installation Manager, which is a single tool that steps you through the process for installing components and tools.

The Installation Manager installs all VCM components on your machine, even if you have not purchased licenses for all of the components. Only the VCM components that are included in your VCM license file are activated during the installation process. This installation method allows you the flexibility to purchase more licenses and activate additional VCM components as needed. The components are already installed on the machine and need only be activated with additional licenses.

When preparing your system for a VCM installation, determine your requirements based on which components you plan to license within your configuration. Use the hardware requirement worksheet and associated tables in "Hardware Requirements for Collector Machines" on page 11 to assess your requirements based on your individual licensing plan. In addition, consider whether you will have a single-server or a multiple-server installation configuration.

Understand VCM Installation Configurations

VCM supports one installation configuration: the single server installation in which the Collector and the VCM databases (SQL Server databases) are installed on a single machine. See Figure 1-1: Typical VCM Enterprise-wide, single-server installation.

In addition to the Collector, the supported configuration includes an Operating System Provisioning Server. The OS Provisioning Server manages the OS provisioning actions as commanded by VCM. See Figure 1-2: VCM Collector with OS Provisioning Server. For complete hardware and software requirements for the OS Provisioning Server, see "Hardware and Software Requirements for the Operating System Provisioning Server" on page 41.

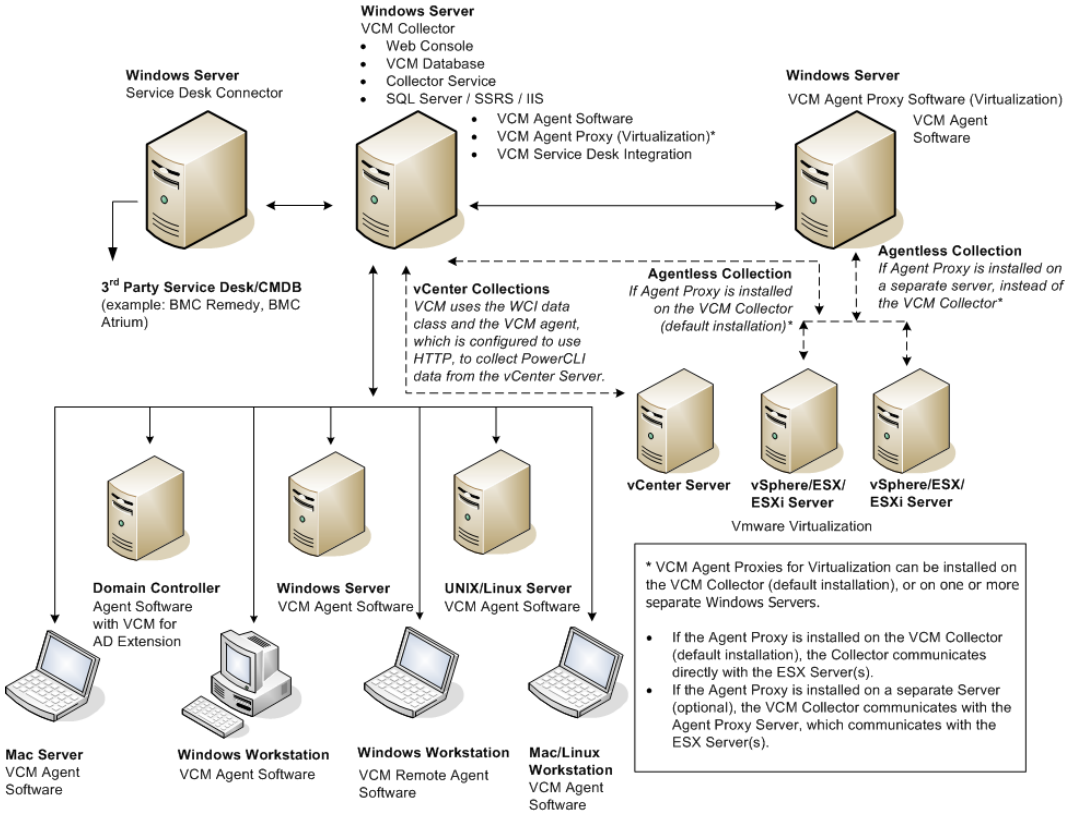


Figure 1-1: Typical VCM Enterprise-wide, single-server installation

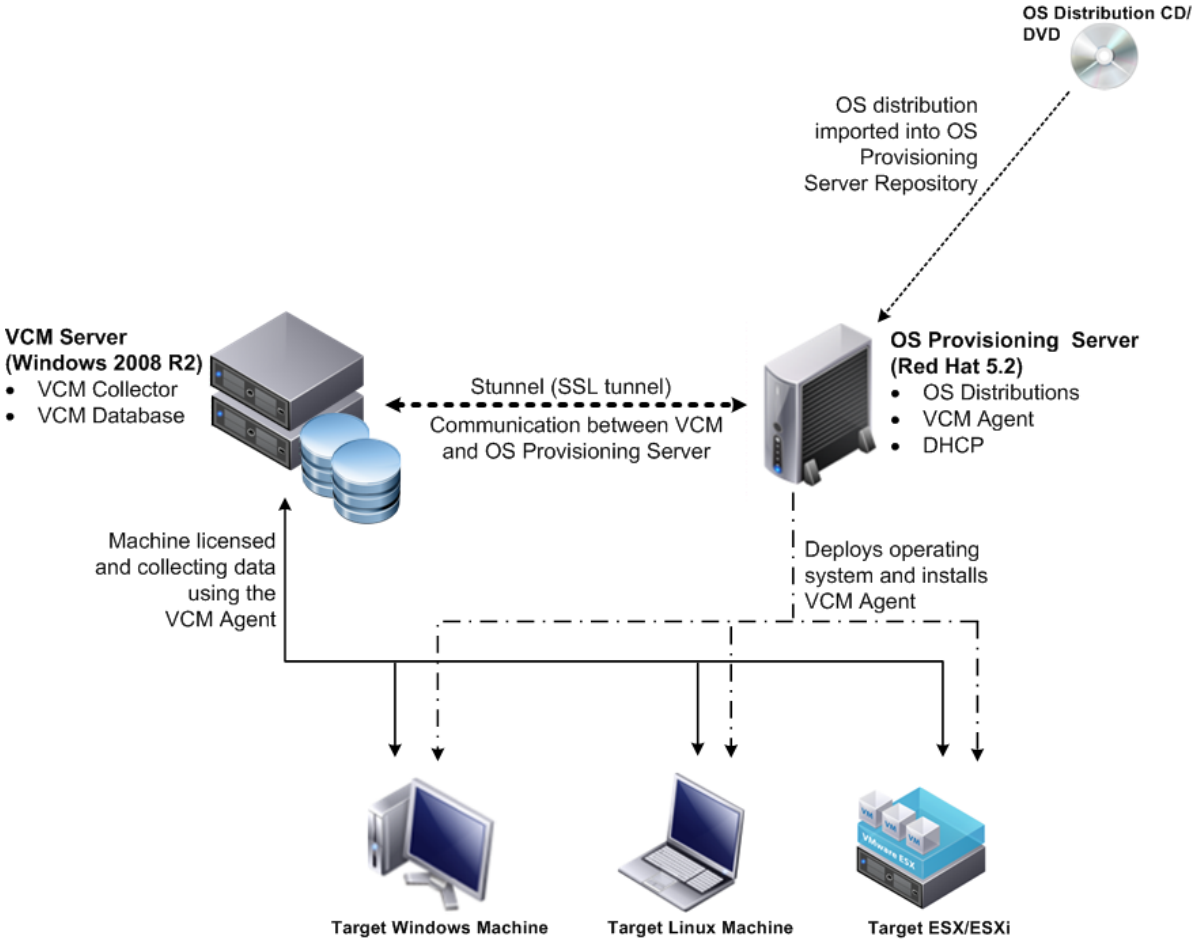


Figure 1-2: VCM Collector with OS Provisioning Server

Hardware Requirements for Collector Machines

2

VCM hardware requirements are dependent on the number of physical and virtual machines within your enterprise that you plan to license for use with VCM. Use the information in this chapter to determine how many machines you plan to manage and what VCM components you plan to license. Once you have this information, you will be able to continue using this chapter to determine the individual hardware requirements that you must satisfy in order to ensure a successful VCM installation.

Disk space requirements vary based on:

- Number of machines from which you are collecting data
- Type of data collected and filters used
- Frequency of collections
- Data retention

Determine the Size of Your Environment

VCM hardware requirements are recommended based on whether your enterprise contains 1 to 1,000, 1,000 to 2,000, 2,000 to 5,000, or more managed machines. To determine the number of managed machines on which to base your collector size, consider the number of Windows (servers and workstations), UNIX/Linux, and virtual machines that you are licensing. In addition, identify any other VCM components that you are licensing. To determine your total number of managed machines, enter data for your enterprise in the Sizing Worksheet.

Within VCM, the term “managed machines” indicates the servers and workstations that VCM manages, and from which VCM collects data. However, if you are licensing VCM for Microsoft Active Directory (AD), expand this definition to include AD objects that you plan to have in your environment within the next 12 to 24 months. Use the formulas in the worksheets to determine how your AD objects will increase your managed machine count and affect your final sizing requirements. Taking these considerations into account now ensures that you will have adequate disk space to accommodate VCM now and in the future.

After you complete the worksheet and determined the number of managed machines, you must size your Collector machine. See "Identify Your Specific Hardware Requirements" on page 12 for more information.

In this example, an enterprise contains machines and objects that represent 1177 managed machines and so is in the 1000 to 2000 managed machines category.

Table 2-1. Sizing Worksheet

Product	Description	Anticipated Number of Managed Machines within the Next 12-24 Months (See Note)
VCM	Windows Servers	
	ESX Servers	
	Virtual Machines (VM)	
	Windows Workstations	
VCM for AD	Divide total number of AD objects by 100 to get the approximate "machine count" for your AD environment.	
	TOTAL MANAGED MACHINES	

Table 2-2. Example of Sizing Worksheet with Sample Data

Product	Description	Anticipated Number of Managed Machines within the Next 12-24 Months
VCM	Windows Servers	92
	vSphere/ESX/ESXi Servers	5
	Virtual Machines (VM)	50
	Windows Workstations	920
VCM for AD	Divide total number of AD objects by 100 to get the approximate "machine count" for your AD environment.	10,000 AD Objects/100 = 100 managed machines to accommodate VCM for AD
		TOTAL 1177 managed machines

Identify Your Specific Hardware Requirements

Use the Minimum Hardware Requirements and Minimum Disk Configuration Requirements tables to determine your hardware and disk configuration requirements. Use the total number of managed machines from the Sizing Worksheet to locate your environment size (1 to 1,000, 1,000 to 2,000, 2,000 to 5,000, or more). If you have more than 2000 machines in your environment, contact VMware Customer Support to assist you in determining your hardware requirements.

The requirements listed in this table are based on the following assumptions:

- Daily VCM collections (using the default filter set with additional Microsoft AD security descriptors collected using VCM for AD)
- 15 days retention of data
- Simple recovery mode only
- Daily VCM Patching collections
- No applications other than VCM running on your server (if you intend to run other applications, contact VMware Customer Support to prevent conflicts)

VCM for AD collections cause the TempDB database to grow significantly. Increase your hardware requirements if you have a fully populated Microsoft Active Directory and plan to perform frequent AD collections.

Longer data retention, additional WMI, registry filters, and custom information collections also add to the requirements. For questions about how your specific requirements are affected, contact VMware Customer Support.

Table 2-1. Minimum Hardware Requirements by Number of Managed Machines

Requirements	Number of VCM Managed Machines		
	1-1000	**1000-2000**	**2000+ (See Note)**
Processors	Dual Xeon or single Dual Core 2GHz minimum	Quad Xeon or two Dual Core 2GHz minimum	Eight-way Xeon or four Dual Core 2GHz minimum
RAM	4GB+ minimum	6GB+ minimum	12GB+ minimum
Number of Separate Disk Channels	2	3	4

The space allocations in this table do not include space for backups. Backup space should be allocated equal to the size of the VCM data for a single full backup, or larger if you want to keep multiple partial backups.

Table 2-2. Minimum Disk Configuration Requirements by Number of Managed Machines

Number of VCM Managed Machines	RAID Channel and RAID Level	Partitions	Usable Space
1-500	Channel 0 -- RAID 1	OS	36GB
		Collector Data Files	36GB
		TempDB	36GB
		SQL Log Files	28GB
	Channel 1 -- RAID 0+1 (recommended) or RAID 10	SQL Data Files	56GB
501-1000	Channel 0 -- RAID 1	OS	36GB
		Collector Data Files	36GB
	Channel 1 -- RAID 1	TempDB	56GB
		SQL Log Files	56GB
	Channel 2 -- RAID 0+1 (recommended) or RAID 10	SQL Data Files	113GB
1001-2000	Channel 0 -- RAID 1	OS	36GB
		Collector Data Files	54GB
	Channel 1 -- RAID 1	TempDB	113GB
	Channel 2 -- RAID 1	SQL Log Files	113GB
	Channel 3 -- RAID 0+1 (recommended) or RAID 10	SQL Data Files	227GB

Hardware and Operating System Requirements for Agent Machines

3

Agent machines are managed machines from which VCM collects data. The Agent is supported on many different machine and operating system types.

VCM Agent Requirements

The amount of additional disk space required on a Windows, UNIX/Linux, Mac OS X,or AD managed machine running an Agent is fairly constant. Each machine requires no more than 200MB to run an Agent. However, the recommended memory to run the HP-UX Agent is 1GB.

This table provides the list of hardware platforms and operating systems supported by VCM. While it might be possible to install Agents on platforms or operating system versions other than those listed below, such configurations will not be supported. From time to time VMware introduces support for additional platforms and operating systems. If a particular combination of platform and operating system is not listed, contact VMware Customer Support to confirm whether the combination is supported by a later version of VCM.

The platforms indicated with an asterisk (*) that have agents prior to the 5.2.1 Agent may not correctly report the name of the operating system. You should upgrade these platform agents as soon as possible.

The platforms indicated with the "(up to the 5.2.1 Agent only)" note are supported only to the Agent version specified. You can install the 5.2.1 version of the Agent on the platforms specified, but you cannot install newer or the current Agent. This means that you will not be able to use the new features in this release on those platforms. Contact VMware Customer Support for the earlier supported Agents.

Table 3-1. Agent Operating System and Hardware Requirements

Agent	Supported Operating System	Supported Hardware Platform	Platforms to be Upgraded
Windows	Microsoft Windows 2000 (up to 5.2.1 Agent only)	x86	
	Microsoft Windows 2003	x86 and x64	
	Microsoft Windows 2003 R2	x86 and x64	
	Microsoft XP Professional (including SP3)	x86 and x64	
	Microsoft XP Professional (SP2 and earlier up to 5.2.1 Agent only)	x86 and x64	
	Microsoft Vista Business (including SP1)	x86 and x64	*
	Microsoft Vista Ultimate (including SP1)	x86 and x64	*
	Microsoft Vista Enterprise (including SP1)	x86 and x64	*
	Microsoft Windows Server 2008	x86 and x64	*
	Microsoft Windows Server 2008 R2	x86 and x64	*
	Microsoft Windows 7 Business	x86 and x64	
	Microsoft Windows 7 Ultimate	x86 and x64	
	Microsoft Windows 7 Enterprise	x86 and x64	*
UNIX/Linux	AIX 4.3.3 (up to 5.1.3 Agent only)	RISC	

Agent	Supported Operating System	Supported Hardware Platform	Platforms to be Upgraded
	AIX 5L 5.1	RISC	
	AIX 5L 5.2	RISC	
	AIX 5L 5.3	RISC	
	AIX 6L 6.1 (5.2 Agent or later)	RISC and PowerPC	
	Debian 4.0 (Package LSB-Release is required)	x86 and x64	
	ESX 4.1 Update 1		
	ESXi 4.1 Update 1		
	HP-UX 11i v1.0 (11.11) (If you are installing on HPUX 11.11, Patch PHSS_30966 is required.) Supported in trusted mode.	PA-RISC	
	HP-UX 11i v2.0 (11.23)	Itanium	
	HP-UX 11i v2.0 (11.23)	PA-RISC	
	HP-UX 11i v3.0 (11.31)	Itanium	
	HP-UX 11i v3.0 (11.31)	PA-RISC	
	Red Hat Enterprise Linux 2.1 (ES/AS) (up to 5.1.3 Agent only)	x86	
	Red Hat Enterprise Linux 3 (ES/AS) including Desktop with Workstation edition	x86	
	Red Hat Enterprise Linux 4 (ES/AS) including Desktop with Workstation edition	x86 and x64	
	Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, Server, Desktop with Workstation, and Advanced Platform	x86 and x64	
	Solaris 2.5 (up to 5.1.3 Agent only)	Sparc	
	Solaris 2.6 (up to 5.2.1 Agent only)	Sparc	
	Solaris 8	Sparc and Sparc-V9	
	Solaris 9	Sparc and Sparc-V9	
	Solaris 10 (certified and verified on Solaris 10 zfs and custom information data class collections on both zfs and vxfs)	Sparc, Sparc-V9, x86, and x64	
	SUSE Linux Enterprise Server (SLES) 9	x86 and x64	
	SUSE Linux Enterprise Server (SLES) 10	x86 and x64	
	SUSE Linux Enterprise Server (SLES) 10.2	x86 and x64	
	SUSE Linux Enterprise Server (SLES) 10.3	x86 and x64	
	SUSE Linux Enterprise Server (SLES) 11	x86 and x64	
Mac OS X (servers and workstations)	Mac OS X 10.4	Intel and PowerPC	
	Mac OS X 10.5	Intel and PowerPC	
Oracle 9i	Solaris 9	Sparc and Sparc-V9	
	Solaris 10	Sparc and Sparc-V9	
Oracle 10g	Solaris 9	Sparc-V9	
	Solaris 10	Sparc-V9, x86, and x64	
Active Directory	Microsoft Windows 2000	x86	
	Microsoft Windows 2003	x86 and x64	
	Microsoft Windows 2003 R2	x86 and x64	
	Microsoft Windows 2008	x86 and x64	
VCM Remote	VCM Remote supports the same platforms as the Windows Agent		

These x64 platforms have been tested:

- For Windows: Intel64 and AMD64
- For Linux: Intel64 and AMD64
- For Solaris: Intel64

Itanium is not supported for either Windows or UNIX/Linux, except for HP-UX for Itanium servers.

Windows Custom Information Supports PowerShell 2.0

PowerShell version 2.0 is required for Windows Custom Information (WCI). VMware recommends that you upgrade from PowerShell 1.0 to PowerShell 2.0, which introduced several useful functions.

Because of the additional ability to set the execution policy at the process level, PowerShell 2.0 is the base requirement for WCI in VCM. The default script type command line used for script based filters in WCI includes options to set the process-level execution policy to Remote Signed. This usage allows WCI to execute collection scripts against systems whose machine and user level signing policies might be anything, without having to change the setting. Out-of-the-box, non-in-line collection filters for VCM Windows Custom Information will fail if executed against PowerShell 1.0 client systems.

PowerShell 2.0 is supported on all platforms that support PowerShell 1.0. For more information, see the online Help.

Supported OS Provisioning Target Systems

You use OS provisioning to install the following operating system on machines with at least 1 GB RAM.

Table 3-1. Supported Operating Systems

Operating System	Versions
ESX	4.0u1/u2, 4.1
ESXi	4.1
Windows 2008	R2 - 64-bit - Std, Ent, Web, DC, StdCore, EntCore, WebCore, DCCore
	SP1 - i386 and 64-bit - Std, Ent, DC, StdCore, EntCore, DCCore
	SP2 - i386 and 64-bit - Std, Ent, DC, StdCore, EntCore, DCCore
Windows 7 Pro	i386 and 64-bit
Windows 2003	R2 SP2 - i386 and 64-bit - Std, Ent
SUSE Linux Enterprise Server	10 (SP3 only) 32- and 64-bit and 11 (SP1 only) 32- and 64-bit
Red Hat Enterprise Linux	(Server only) 5.0, 5.2, 5.4, 5.5 32- and 64-bit

See "Hardware and Software Requirements for the Operating System Provisioning Server" on page 41 for more information about configuring the OS Provisioning Server for installation. Instructions for installing the OS Provisioning Server and using the OS provisioning options in VCM are available in *VCM Installation and Getting Started Guide*.

Software Provisioning Requirements

VCM Software Provisioning provides the components to create software provisioning packages, publish the packages to repositories, and install and remove software packages on target machines.

Table 3-1. Software Provisioning Operating System and Hardware Requirements

Supported Operating System	Supported Hardware Platform
Microsoft Windows 7	x86, x64
Microsoft Windows Server 2008 R2	x64
Microsoft Windows Server 2008 SP2	x86, x64
Windows Vista SP2	x86, x64
Microsoft Windows XP SP3	x86
Microsoft Windows XP SP2	x64
Microsoft Windows Server 2003 R2 SP2	x86, x64
Microsoft Windows Server 2003 SP2	x86, x64

Software Provisioning Component Software Requirements

The VCM Software Provisioning components and their software requirements are listed here.

Table 3-2. Software Provisioning Component Requirements

Software Provisioning Component	Description	Requires
VMware vCenter Configuration Manager Package Studio	Application used to the create the software packages.	.NET 3.5.1 or higher
Software Repositories	File system used to store the shared software packages.	.NET 3.5.1 and IIS 6, 7, or 7.5
Package Manager	Application on each managed machine that downloads packages from repositories, and installs and removes the software contained in the packages.	.NET 3.5.1 or higher

You can use any virtual machine guest on VMware ESX and ESXi Servers that meets these requirements for any of the VCM Software Provisioning components.

UNIX/Linux Patch Assessment and Deployment Requirements

UNIX patch assessments and deployments are currently supported for the following platforms. The associated assessment PLS files require at least 20MB.

Table 3-1. UNIX/Linux Patch Assessment and Deployment Operating System and Hardware Requirements

Supported Operating System	Supported Hardware Platform
AIX 5L 5.1	RISC and PowerPC
AIX 5L 5.2	RISC and PowerPC
AIX 5L 5.3	RISC and PowerPC
AIX 6.1	RISC and PowerPC
HP-UX 11iV1 (11.11)	PA-RISC
HP-UX 11iv2.0	Itanium
HP-UX 11i v2.0	PA-RISC
HP-UX 11i v3.0 (11.31)	Itanium

Supported Operating System	Supported Hardware Platform
HP-UX 11i v3.0 (11.31)	PA-RISC
Mac OS X 10.4	Intel and PowerPC
Mac OS X 10.5	Intel and PowerPC
Red Hat Enterprise Linux 3 (ES/AS) including Desktop with Workstation edition	x86 (includes Intel and AMD architectures, excludes Itanium)
Red Hat Enterprise Linux 4 (ES/AS) including Desktop with Workstation edition	x86 and x64 (includes Intel and AMD architectures, excludes Itanium)
Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5 Server, Desktop with Workstation, and Advanced Platform	x86 and x64 (includes Intel and AMD architectures, excludes Itanium)
Solaris 8	Sparc and Sparc-V9
Solaris 9	Sparc and Sparc-V9
Solaris 10	Sparc, Sparc-V9, x86, and x64
SUSE Linux Enterprise Server (SLES) 9	x86 and x64 (includes Intel and AMD architectures, excludes Itanium)
SUSE Linux Enterprise Server (SLES) 10	x86 and x64 (includes Intel and AMD architectures, excludes Itanium)
SUSE Linux Enterprise Server (SLES) 11	x86 and x64 (includes Intel and AMD architectures, excludes Itanium)

Agent Proxy Requirements for VMware ESX and ESXi

The VCM Agent is not installed directly on the ESX and ESXi Servers; instead, collections are accomplished using what is referred to as "agentless collections". The agentless collection uses an Agent Proxy.

When collecting from ESX/ESXi Servers, you must configure at least one VCM Agent Proxy machine. You can configure the Collector as the Agent Proxy or configure standalone Agent Proxy machines. The Collector communicates with the Agent Proxy and the Agent Proxy then directly communicates with the ESX/ESXi Servers using SSH and/or Web Services for necessary data collection actions. The data is processed by the Agent Proxy and relayed to the Collector.

The minimum operating system and hardware requirements for each Agent Proxy machine are based on:

- Number of machines from which you are collecting data
- Type of data collected and filters used
- Frequency of collections
- Data retention

Minimum Operating System Requirements

The VCM for Virtualization Agent Proxy machine must be running Windows Server 2008 R2 or Windows Server 2003 SP2. For more information to install and configure the Agent Proxy, see "Install and Configure a Windows Server 2008 R2 Operating System" on page 26.

Minimum Hardware Requirements

The VCM for Virtualization Agent Proxy is installed on the Collector by default. Although the Virtualization Agent Proxy is available on the Collector, it requires special configuration to operate. You must configure an Agent Proxy server to collect data from ESX servers. If more than 50 ESX servers are managed, additional Agent Proxy servers must be configured to maintain the ratio of one agent proxy for each 50 ESX servers.

The designated VCM for Agent Proxy servers should meet the following minimum requirements for physical hardware or virtual machines. An Agent Proxy server meeting these requirements can manage approximately 50 ESX Servers.

Physical Requirements

- **Processor.** Single Xeon or single-core 2 GHz minimum
- **RAM.** 4 GB minimum
- **Disk Space.** Each VCM for Virtualization Agent Proxy requires an additional 93 MB of disk space, above the 200 MB required for the standard Agent. In addition, you will also need:
  - 4 MB per ESX server for data model storage
  - 150 MB per ESX server for Agent master files

Virtual Requirements

- **CPU.** One virtual CPU, 2GHz, on a supported ESX host machine.
- **RAM.** 4 GB minimum reservation on a supported ESX host machine.
- **Storage.** Each VCM for Virtualization Agent Proxy requires an additional 93MB of disk space, above the 200 MB required for the standard Agent on a supported ESX platform. In addition, you will also need:
  - 4 MB per ESX server for data model storage
  - 150 MB per ESX server for Agent master files

Supported vCenter Server Collections

VCM supports collecting data from vCenter Server 4, 4.0.x, and 4.1. Collections.

When collecting from vCenter Server, you must license and install a VCM Windows Agent, PowerShell, and vSphere PowerCLI 2.0 on the machine running vCenter. The Agent runs the vCenter collection using vSphere PowerCLI to access the vSphere API on the vCenter Servers. The data is relayed to the Collector and added to the database.

FIPS Requirements

If your organization must conform to the Federal Information Processing Standards (FIPS), the following tables list the VCM-supported standards.

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 3-1. 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

Operating System	Version	Hardware Platform	FIPS Module Certificate
Windows XP	SP1	x86	240
Windows XP	Gold	x86	240
Windows XP	Gold	x86	238
Windows 2000	All	x86	103
Windows 2008	1	x86 and 64-bit; Itanium is not supported.	See "Cryptographic RSA Enhanced Validated Modules" on page 21 and "Cryptographic DSS Enhanced Validated Modules" on page 21.
Windows 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 3-1. RSA Enhanced Validated Modules

RSAENH Validated Operating Systems	Validated Versions (Links to Security Policy)	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 3-1. DSS Enhanced Validated Modules

DSSENH Validated Operating Systems	Validated Versions (Links to Security Policy)	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	#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

DSSENH Validated Operating Systems	Validated Versions (Links to Security Policy)	FIPS Certificate #	FIPS Version Validated
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.

Agent Sizing Information

The VCM-related file size on the disk varies depending on the platform and the actual data collected. The tables below identify data files for default collections only. Approximate sizes are in megabytes.

NOTE Use the information in the tables as a general guideline. While VMware makes every effort to validate the numbers, quoted factors such as the types of data collected will affect the sizing. VMware cannot guarantee that the sizing information quoted will be accurate for all installations.

Table 3-1. Windows Agents and Components File Sizes

Agent Type	Installed file size	Data File Size (after collecting data using default filter set)	Projected Data File Size (determined by collected data types and actions)
VCM Agent with Extension for Provisioning (default Agent)	130-135MB	10-20 MB	The projected data file sizing information can vary greatly depending on your collection filter set. The size can vary from 10-20MB to more than 100MB. The most likely data types to cause large data growth are File System-File Structure and System Logs.
VCM Agent without Extension for Provisioning	70-76MB	10-20MB	See above information.
Agent Proxy for Virtualization	VCM Agent +40MB	See VCM Agent data file sizes	See above information.
Active Directory Agent	VCM Agent +30MB	See VCM Agent data file sizes	See above information.
VCM Remote Client	VCM Agent +2MB (installs or upgrades Agent)	See VCM Agent data file sizes	See above information.
Patching Agent	VCM Agent +2MB	See VCM Agent data file sizes	See above information.
Package Manager (installed with VCM Agent Extension for Provisioning), which includes the database and cratecache	Package Manager 4MB	n/a	**Package Manager.** The application that installs and removes packages. Size remains fixed. **Database.** Metadata about packages. Increased size based on number of installed packages. For example, installing one package increased the size from 140KB to 141KB. **Cratecache.** Packages downloaded to the machine from

Agent Type	Installed file size	Data File Size (after collecting data using default filter set)	Projected Data File Size (determined by collected data types and actions)
	Database 140KB Cratecache 0MB		Software Repository. Increased sized is based on the number of installed packages and the size of the packages. The size of cratecache changes if packages are "cleaned" from the cratecache after package installation or removal.
Package Studio	5MB	n/a	Increased size of the files depends on which *.prj and *.crate files are saved locally.
Software Repository	5KB	n/a	Increased size of the files is based on the number of packages published to the repository from Package Studio.

UNIX/Linux Machines

Table 3-2. UNIX/Linux Agents File Sizes

Agent Type	Installed file size	Data File Size (after collecting data using default filter set)	Projected Data File Size (determined by collected data types and actions)
CMAgent.5.1.0.AIX.4	76MB	5-15MB	The projected data file sizing information can vary greatly depending on your collection filter set. The size can vary from 10-20 MB to 100+ MB. The most likely data types to cause large data growth are File System-File Structure, and System Logs.
CMAgent.5.1.0.Linux.2.1	41MB	5-70MB	See above information.
CMAgent.5.3.0.AIX.5	60-80MB	5-20MB	See above information.
CMAgent.5.3.0.HP-UX.11.ia64	80MB	5-16MB	See above information.
CMAgent.5.3.0.HP-UX.11.pa	80MB	5-16MB	See above information.
CMAgent.5.3.0.Linux	30-50MB	5-70MB	See above information.
CMAgent.5.3.0.SunOS	40-50MB	5-30MB	See above information.
CMAgent.5.3.0.SunOS.x86.5.10	40-50MB	5-30MB	See above information.

Mac OS X Machines

Table 3-3. Mac OS X Agent File Sizes

Agent Type	Installed file size	Data File Size (after collecting data using default filter set)	Projected Data File Size (determined by collected data types and actions)
CMAgent.5.3.0.Darwin	97MB	5-30MB	The projected data file sizing information can vary greatly depending on your collection filter set. The size can vary from 10-20MB to more than 100MB. The most likely data types to cause large data growth are File System-File Structure and System Logs.

Software and Operating System Requirements for Collector Machines

4

Your system must meet these software requirements before you install VCM. The requirements are divided into steps, with several requirements consolidated under a general step. Each step must be performed in the order specified to ensure a smooth and efficient VCM installation. The final step in preparing your VCM Collector is to download and run the Foundation Checker tool. Running Foundation Checker helps you verify that you have satisfied all of the software requirements necessary to install VCM.

All software requirements apply to your single server. For more information about installation configurations, see "Understand VCM Installation Configurations" on page 8.

Sizing Impacts on Software Requirements

Use the total number of managed machines that you identified in "Determine the Size of Your Environment" on page 11 to locate your environment size (1 to 1,000, 1,000 to 2,000, 2,000 to 5,000, or more). If you have more than 2000 managed machines on a single Collector, contact VMware Customer Support for your specific requirements.

If you are deploying VCM in an environment with more than 5,000 managed machines, contact VMware for software component recommendations.

Table 4-1. Minimum Software Requirements by Number of VCM Managed Machines

Software Component	Number of Managed Machines		
	1-1,000	**1,000-2,000**	**2,000-5,000**
Operating System	Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2 Enterprise Edition
SQL Version	SQL Server 2008 R2 Standard Edition (64-bit)	SQL Server 2008 R2 Standard Edition (64-bit)	SQL Server 2008 R2 Standard Edition (64-bit)
SSRS Version	SQL Server 2008 Reporting Services	SQL Server 2008 Reporting Services	SQL Server 2008 Reporting Services

Standard and Enterprise editions of SQL Server 2008 R2 are supported.

Software Installation and Configuration Overview

You must complete the preparatory steps to prepare your machine for a successful VCM installation. Follow the precise configuration procedures noted in each section. When you have completed these steps successfully, Foundation Checker should also run without error, indicating that you have met the requirements necessary to install VCM.

VCM supports a Collector that is running on a Windows Server 2008 R2 operating system.

Upgrade Considerations

To upgrade to the current version of VCM, you must have version 4.11.1 or later installed and running. Detailed upgrade procedures are provided in the *VCM Installation and Getting Started Guide*.

Configuring a 64-bit Operating System for a VCM Installation

To prepare your 64-bit system for a successful VCM installation, complete the procedures in the order they are presented.

You must check each procedure against your system to ensure that all of the necessary components are properly installed and configured.

Install and Configure a Windows Server 2008 R2 Operating System

Install the correct operating system on your Collector and verify that the settings are configured for VCM operation. See "Sizing Impacts on Software Requirements" on page 25 to determine whether you require the Enterprise or Standard Edition.

1. After you install the operating system, confirm that the computer name settings for your Collector machine meet the required naming convention for VCM.

   The computer name must be a valid DNS machine name with no underscores. Verify that the name is correct before you proceed. If you attempt to change the machine name after the machine is identified as a Collector, problems may arise with VCM, SQL Server, and SQL Server Reporting Services.

2. Verify that the person who performs these procedures uses a domain account with local administrator rights.
3. Install Microsoft Windows Server 2008 R2.

Configure the Operating System Locale Settings

Verify that your Windows Server Locale Setting is configured correctly for a VCM installation.

1. In Windows Explorer, select **Start > Control Panel > Clock, Language, and Region**.
2. Click **Region and Language**.
3. In the Region and Language dialog box, click the **Administrative** tab and verify that the Language for non-Unicode programs area displays **English (United States)**.

Set the Terminal Services Mode to Remote Desktop for Administration

If Terminal Services are enabled, use the following procedure to verify that your Windows Terminal Services setting is configured correctly for a VCM installation.

1. Select **Server Manager > Roles > Remote Desktop Services**.
2. Select **Remove Role Services**.
3. Clear the **Remote Desktop Session Host** setting and follow the online instructions.

Enable DCOM

DCOM (Distributed Component Object Model) is a protocol used to interact between application components across Windows machines. Windows operating systems include DCOM.

To interact locally with Collector components, VCM Collectors require DCOM, which provides an option to manage Windows VCM managed machines.

VCM managed machines do not require DCOM. Instead, you can use HTTP on VCM managed machines if you do not want to use DCOM or if it is blocked by firewalls or disabled on the clients.

You must ensure that DCOM is enable on the Collector to successfully install and run VCM. Although DCOM is enabled by default when Windows Server 2008 R2 is installed, DCOM can be disabled by a custom installation or a lock-down script.

1. Open **Component Services**.
2. Click **Computers**, right-click the computer, and click **Properties**.
3. Click **Default Properties**.
4. Select **Enable Distributed COM on this computer** and click **OK**.

Install and Configure IIS

The VCM Collector must be running IIS 7.5, which is installed automatically when you install Windows Server 2008 R2.

Configure IIS Settings

To ensure correct settings for IIS 7.5, you must:

- Verify the correct IIS 7.5 Role Services are enabled on the Web server.
- Configure the IIS 7.5 settings.

To verify the correct IIS 7.5 Role Services are enabled on the Web server

1. Open Server Manager.
2. Expand **Roles** and click **Web Server (IIS)**.
3. In the Web Server (IIS) pane, scroll down to **Role Services**.
4. Make sure these Role Services on the IIS Web server are **Installed**:

Table 4-1. IIS Web Server Role Services Installed

Common HTTP Features	Static Content
	Default Document
	Directory Browsing
	HTTP Errors
	HTTP Redirection
Application Development	ASP.NET
	.NET Extensibility
	ASP
	ISAPI Extensions
	ISAPI Filters
	Server Side Includes
Health and Diagnostics	HTTP Logging
	Logging Tools
	Request Monitor
	Tracing
Security	Basic Authentication
	Windows Authentication
	Digest Authentication
	Client Certificate Mapping Authentication
	IIS Client Certificate Mapping Authentication
	URL Authorization
	Request Filtering
	IP and Domain Restrictions
Performance	Static Content Compression
	Dynamic Content Compression
Management Tools	IIS Management Console
	IIS Management Scripts and Tools
	Management Service

If any of the Role Services are not enabled, click **Add Role Services**, mark the check boxes of the services that need to be installed, and click **Install**.

To Configure the IIS 7.5 settings

1. Open Internet Information Services (IIS) Manager.
2. Expand the **Server Manager (<server name>)**, expand **Sites**, and click **Default Web Site**.
3. In the **Actions** area, under **Edit Site**, click **Bindings**.
4. Click **Add** and set the **Port** to **80** and the **IP address** to **All Unsigned**.
5. Save the settings and close the Site Bindings dialog box.
6. In the **Actions** area, under **Manage Web Site**, click **Advanced Settings**.
7. Expand **Connection Limits** and set **Connection Time-out (seconds)** to **3600**.

Verify and Enable the IWAM Account Name

You must verify that the IWAM account is listed as a built-in account.

1. In Windows Explorer, right-click **Computer** and select **Manage**.
2. Expand **Configuration > Local Users and Groups**.
3. Select **Users** and confirm the **IWAM_AccountName** account is listed.
4. Right-click the account and select **Properties**.
5. Verify that the **IWAM_AccountName** account is described as the built-in account.

   If the account does not exist, you must reinstall IIS.

Install .NET Framework

The VCM Collector requires .NET 3.5 Service Pack 1, which also installs .NET 2.0 and .NET 3.0. VCM 5.4 also supports .NET 4.0.

Verify that the Collector has the required versions of .NET Framework installed. If a .NET version is missing, install the version from the Microsoft download Web site.

Verify the .NET Installed Versions

You must verify that the correct .NET version is installed.

.NET Framework Version 3.5 Service Pack 1 is installed as part of Windows Server 2008 R2.

To verify the installed versions of the .NET Framework

1. Open Server Manager and click **Features**.
2. View the feature summary, and confirm that .NET Framework 3.5.1 appears.

Verify the ASP.NET Client System Web Version

You must verify the ASP.NET Client System Web version.

1. Open Internet Information Services (IIS) Manager.
2. Expand **Server Manager (<server name>)** and **Sites**.
3. Expand **Default Web Site**, **aspnet_client**, and **system_web**.
4. Verify the version is **2_0_50727**.

Verify the ASP Role Service

You must verify the status of the ASP Role Service.

To verify the ASP Role Service

1. Select **Start > Administrative Tools > Server Manager**.
2. Expand **Server Manager (<server name>)** and expand **Roles**.
3. Click **Web Server (IIS)**.
4. Scroll down to **Role Services**.
5. Locate **ASP** and verify that the status is **Installed**.
6. If the status of the ASP Role Service is **Not Installed**:
   a. Click **Add Role Services**.
   b. On the Select Role Services page, select the **ASP** role service.
   c. Complete the wizard to install the ASP role service for Web Server (IIS).

Verify ASP.NET Role Service

You must verify the status of the ASP.NET Role Service.

To verify the ASP.NET Role Service

1. Select **Start > Administrative Tools > Server Manager**.
2. Expand **Server Manager (<server name>)** and expand **Roles**.
3. Click **Web Server (IIS)**.
4. Scroll down to **Role Services**.
5. Locate **ASP.NET** and verify that the status is **Installed**.

Verify the IIS Server-Side Includes Role Service

The IIS ServerSideIncludes Role Service must be installed.

To verify the IIS ServerSideIncludes Role Service

1. Select **Start > Administrative Tools > Server Manager**.
2. Expand **Server Manager (<server name>)** and expand **Roles**.
3. Click **Web Server (IIS)**.
4. Scroll down to **Role Services**.
5. Locate **IIS ServerSideIncludes** and verify that the status is **Installed**.
6. If the status of the ServerSideIncludes Role Service is **Not Installed**:
   a. Click **Add Role Services**.
   b. On the Select Role Services page, select the **IIS ServerSideIncludes** role service.
   c. Complete the wizard to install the IIS ServerSideIncludes role service for Web Server (IIS).

Verify the ISAPI Extensions

Expected Value

The ISAPI Extensions Role Service must be installed.

To verify the ISAPI Extensions Role Service

1. Select **Start > Administrative Tools > Server Manager**.
2. Expand **Server Manager (<server name>)** and expand **Roles**.
3. Click **Web Server (IIS)**.
4. Scroll down to **Role Services**.
5. Locate **ISAPI Extensions** and verify that the status is **Installed**.

Install and Verify SQL XML 3.0 SP3

You must install SQLXML 3.0 SP3. Although SQL Server 2008 R2 installs SQLXML4, SQLXML 3.0 SP3 is also required.

1. Download and install SQLXML 3.0 Service Pack 3.

   The application is available as a download from Microsoft at http://www.microsoft.com/downloads/en/details.aspx?FamilyID=51d4a154-8e23-47d2-a033-764259cfb53b.
2. To verify the version, in the Control Panel select **Programs > Programs and Features**.
3. Verify that **SQLXML 3.0 SP3** appears in the list of installed programs.
4. Verify the exact version number is at least `3.30.3457.0`.
5. If the list displays only SQLXML 3.0 or the version number is not at least `3.30.3457.0`, you must install the correct version.

Install and Configure SQL Server

VCM operates with a Standard or Enterprise edition of SQL Server. You must install SQL Server 2008 R2 (64-bit), English (United States) version on your designated Collector and verify that the settings are configured correctly for a VCM installation.

If you plan to change the communication port used by SQL from the default port of 1433 to a nonstandard port number, make the changes during the installation of SQL Server and SQL Server Reporting Services (SSRS). Changing the port after you install SSRS disables SSRS communication with SQL Server, which causes an SSRS validation error during the VCM installation process. If you do change the port after installation, you must configure additional SSRS settings to repair the configuration. If you need assistance, contact VMware Customer Support.

Before you begin the SQL Server 2008 R2 installation, make sure you have performed all of the preparatory tasks. Check for Windows updates to your machine and install them. If you do not ensure your machine is updated with all Windows updates before starting the installation, the SQL Server 2008 R2 installation process requires you to remove the SQL Server components that were flagged for installation when you clicked setup.exe. You must then begin the SQL Server 2008 R2 installation process again.

Install SQL Server

To install SQL Server, you must complete the steps in the order presented. The installation details are focused on SQL Server installation options that are related to VCM. The are not intended as a complete SQL Server installation guide. For additional details about the installation, see the SQL Server documentation.

When you install SQL Server, use the default settings in the Microsoft SQL Server Setup wizard, except where specified. Do not select any settings other than the settings specified and the default settings unless you are familiar with the SQL Server installation settings.

Prerequisites to install SQL Server 2008 R2

Before you can install SQL Server 2008 R2, complete these preparatory steps:

- Enable the IIS Role and enable the ISAPI Filters, ISAPI Extensions, and .NET Extensibility roles.
- Install .NET 3.5.1. VCM 5.4 also supports .NET 4.0.

  When you install .NET 3.5.1, use the Role Management Tool to install or configure the .NET Framework.
- Turn off the Windows firewall.
- Depending on your environment, you might need to turn of Internet Explorer Enhanced Security Mode for Administrators and Users, as described in the *VCM Installation and Getting Started Guide*.
- Check for Windows updates and install them, and then restart the machine and allow Windows to configure the updates.

CAUTION Before you begin the SQL Server 2008 R2 installation, make sure you have performed all of the preparatory tasks. Check for Windows updates to your machine and install them. If you do not ensure your machine is updated with all Windows updates before starting the installation, the SQL Server 2008 R2 installation process requires you to remove the SQL Server components that were flagged for installation when you clicked setup.exe, and you must begin the SQL Server 2008 R2 installation process again.

To install SQL Server 2008 R2

1. Run `setup.exe` to begin the SQL Server 2008 R2 installation.
2. In the SQL Server Installation Center, review the list of **Planning** options.

   You do not need to run the SQL System Configuration Checker. When you install VCM later, the VCM Installation Manager will run the VCM Foundation Checker to ensure your system is ready for the VCM installation.
3. Click **Installation** and review the installation options.

   Do NOT select Install Upgrade Advisor, even if you upgrade from SQL Server 2005.

   The SQL installation might require you to click **Search** for product updates, which installs updates to Windows Server 2008 R2. If updates are available, download and install them to prepare your machine for the SQL Server 2008 R2 installation.
4. (Optional) If Windows updates were required and installed successfully, restart the machine.
5. (Optional) If Windows updates were installed, run `setup.exe` again to begin the SQL Server 2008 R2 installation.
6. Click **Installation** and confirm that all of the installation options are available.

   Do NOT select Install Upgrade Advisor.
7. Select **New installation or add features to an existing installation**.
8. After the Setup Support Rules complete, click **OK** and wait for the process to complete.
9. Enter the **Product Key**.
10. Accept the **License Terms**.
11. On the Setup Support Files page, click **Install**.

    The results of the setup support rules must pass.
12. On the Setup Role page, select **SQL Server Feature Installation**.
13. On the Feature Selection page, select these features and tools:

    Instance Features. Database Engine Services and Reporting Services

    Shared Features. Client Tools Connectivity and SQL Server Books online

    Management Tools. Management Tools - Basic and Complete
14. On the Installation Rules page, wait for the operation to complete. If desired, review the detailed report.
15. On the Instance Configuration page, select **Default instance**.
16. On the Disk Space Requirements page, review the summary of disk usage to ensure the machine has enough space.
17. On the Server Configuration page, click **Use the same account for all SQL Server services**.
18. In the Account Name drop-down, select the **NT AUTHORITY\SYSTEM account**.
19. On the Database Engine Configuration page, ensure that **Windows authentication**, which is the default, is selected.

    Although SQL Server and Windows Authentication mode is allowed, Windows Authentication mode is recommended.
20. On the Reporting Services Configuration page, select **Install the native mode default configuration**.

21. On the Error Reporting page, you do not have to take action and can proceed to the next page.
22. On the Installation Configuration Rules page, correct any errors that might have occurred before you proceed.
23. When the rules pass, proceed to the next page.
24. On the Ready to Install page, review the features to be installed and click **Install**.
25. After the installation completes reports that SQL Server 2008 R2 installed successfully, close the wizard.

Verify and Configure the SQL Server Properties

You must verify the SQL Server property settings and set the server-wide SQL database settings in preparation to install VCM. For information about server-wide and database-specific SQL Server database settings, see the *VCM Installation and Getting Started Guide*.

1. Click **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Right-click the SQL instance, and then select **Properties**. The **Server Properties** dialog box appears.
3. Select and confirm each of the following settings:
    - **General page** (You cannot configure these options.)
        - **Version:** 10.50.1600.1
        - **Language:** English (United States). If not correct, you might need to uninstall and install the correct version.
        - **Server Collation:** SQL_Latin1_General_CP1_CI_AS. If not correct, uninstall and reinstall SQL Server.
    - **Security page** (You can configure these options.)
        - **Windows Authentication mode:** Recommended. Select this mode.
        - **SQL Server and Windows Authentication mode:** Although this setting is acceptable for VCM, Windows Authentication mode is recommended.
    - **Database Settings page** (You can configure these options.)
        - **Default index fill factor:** Type or select a percentage value, which specifies the amount of free space in each index page when the page is rebuilt. Set the fill factor to 80% to leave 20% free space available in each index page.
        - **Recovery interval (minutes):** Type or select 5.
4. Click **OK** to save your changes.

Verify Matching SQL Server and Computer Names

You must verify that the SQL Server name matches the computer name. If you just installed SQL Server 2008 R2, this step is not necessary. However, if you obtained a machine that was renamed after both the operating system and SQL Server 2008 R2 were installed, verify and reset the server name.

1. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Click the **Database Engine Query** button.
3. In the **SQL Query** pane, type `SELECT @@Servername` and click **Execute**.
4. Verify that the resulting server name matches the machine name. If the server name does not match the machine name, you must reconfigure your machine so that the machine name matches the server name described in Reset the SQL Server Name.

Reset the SQL Server Name

If the SQL Server server name does not match the Collector machine name, reset the SQL Server name. You cannot perform this procedure after you install VCM.

NOTE If you reset the SQL Server name, you must reconfigure SSRS to connect to the new SQL Server instance.

---

1. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Click the **Database Engine Query** button.
3. In the **SQL Query** pane, type this command and replace NewServerName with the desired server name:

   ```
   exec sp_dropserver @@SERVERNAME
   exec sp_addserver 'NewServerName', 'local'
   ```

   NOTE You cannot install VCM on a machine where the machine name or SQL Server server name includes an underscore.

4. Restart the SQL Server service. Select **Start > Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Configuration Manager > SQL Server 2008 R2 Services**.
5. Right-click **SQL Server** (MSSQLSERVER or your named instance) and select **Restart**.

Use SQL Server 2008 Reporting Service (SSRS)

You do not need to configure SQL Server 2008 Reporting Services because the settings are configured for you during installation. If you need to manage SQL Server 2008 Reporting Services or change any settings, open the Reporting Services Configuration Manager.

Before you use SSRS, back up your configurations using the instructions described in Back Up Your SSRS Key.

Internet Explorer Protected Mode and SSRS

On the VCM Collector, when User Account Control (UAC) is turned on and Internet Explorer Protected Mode is enabled, errors related to SSRS user permissions and web service errors on dashboards and node summaries can occur. If you access the VCM Web console from any machine other than the Collector, this issue does not occur. Access to the SSRS administration interfaces, `http://localhost/reports`, is also blocked by Protected Mode and UAC.

VMware recommends that you do not use the VCM Web console from the Collector itself because either the VCM SSRS dashboards will not be usable or Internet Explorer security on the Collector must be reconfigured to allow the dashboards to operate. To enable SSRS dashboards on the Collector, either disable Internet Explorer Protected Mode for the zone of the Collector itself or run Internet Explorer as administrator. Do not use these options for general use because they can increase the exposure of the Collector to attacks through Internet Explorer.

1. In Internet Explorer, click **Tools**.
2. Click **Internet Options** and the **Security** tab.
3. Click **Local intranet** and clear the **Enable Protected Mode (requires restarting Internet Explorer)** check box.
4. Click **Apply** and **OK**, and close all instances of Internet Explorer.

Back Up Your SSRS Key

Use the Microsoft command line utility, `rskeymgmt.exe`, to back up the symmetric key to an encrypted file. Use `rskeymgmt.exe` to copy your SSRS key set to a removable media device and store it in a secure location.

The command line utility provides a way to delete encrypted content that can no longer be used if you cannot recover or apply the key. For details about how to use `rskeymgmt.exe`, see http://support.microsoft.com/kb/842425.

Prepare for VCM Installation

Before you install VCM, you must verify that you have established or identified all the accounts necessary for a successful VCM installation.

Establish Local Administration Rights

Verify that the User ID of the person who performs the VCM installation or upgrade is a domain account in the Local Administrators group on the machine where the user installs or upgrades VCM.

Establish SQL Server Administration Rights

The user who installs VCM must have SQL Server sysadmin rights.

1. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Expand the server instance, **Security**, and **Logins**.
3. Right-click the login of the user who installs VCM and select **Properties**.
4. In the Select a page area, select **Server Roles**.
5. In the Server roles area, check the **sysadmin** check box.
6. Click **OK** to save the settings and close the window.

Verify Browser Compatibility

Verify that you have installed a VCM-compatible web browser on the Collector and any other machines that will be accessing the Web Console. VCM supports:

- Internet Explorer version 7.0 or 8.0. If you use IE 7, turn off the status bar for better results.
- Mozilla Firefox version 2.0 or later with the Internet Explorer add-on: IE Tab. The add-on requires Internet Explorer 6.0 to be installed on the machine.

Identify Secure Communications Certificates

VCM uses Transport Layer Security (TLS) to communicate securely over HTTP connections. TLS uses certificates to authenticate the Collector and Agents to each other.

During the installation process, you must specify certificates for the Collector and for the Enterprise. You can have Installation Manager generate the certificates for you, or you can use your existing certificates. If you plan to use your own certificates, familiarize yourself with the certificate names so that you can select those certificates from your certificate store during installation.

A Collector certificate must meet certain criteria to be valid:

- The Collector certificate must be located in the local machine personal certificate store.
- The Collector certificate must be valid for Server Authentication. If any Enhanced Key Usage extension or property is present, it must include the Server Authentication OID 1.3.6.1.5.5.7.3.1. If the Key Usage extension is present, it must include DIGITAL_SIGNATURE.
- The Collector certificate must not be expired.

NOTE If you provide your own certificates, refer to the *Transport Layer Security (TLS) Implementation for VCM White Paper* on the VMware Web site.

Identify Default Network Authority Account

The Installation Manager requires that you specify the default network authority account during the installation process. VCM uses the default network authority account to collect data from Windows Agent machines. The default network authority account, which is often the system administrator's account, must be set up in the local administrators group on each machine prior to installation and needs administrator rights on the Agent machines.

NOTE You can change the network authority account later in VCM at **Administration > Settings > Network Authority**.

1. Right-click **Computer** and select **Manage** to open Server Manager.
2. Expand **Configuration**, expand **Local Users and Groups** and click **Groups**.
3. Double-click **Administrators** and verify that the network authority account is listed as a member of the Administrators group.

   If the user or administrator's group is not listed, add the user or group to the list. Also ensure that the user has Windows administrator rights issued by the network administrator.

Identify VMware Application Services Account

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

1. Right-click **Computer** and select **Manage** to open Server Manager.
2. Expand **Configuration**, expand **Local Users and Groups** and click **Groups**.
3. Double-click **Administrators** and verify that the application services account is listed as a member of the Administrators group.

   If the user or administrator's group is not listed, add the user or group to the list. Also ensure that the user has Windows administrator rights issued by the network administrator.

Assign ASP.NET Permissions to the VMware Application Services Account

The VMware Application Services Account is a custom service account that requires appropriate permissions to access the IIS metabase and file system folders that are used by ASP.NET. Use the `Aspnet_regiis.exe` utility to grant these permissions.

1. Open a command prompt window.
2. Set permissions for the Application Services Account, where <DomainName> is the domain name, and <AccountName> is your user account name.

   ```
   cd %windir%\Microsoft.NET\Framework\v2.0.50727\
   aspnet_regiis -ga <DomainName>\<AccountName>
   ```

Set Virtual Directory Permissions for Installation

VCM uses virtual directories for several functions. Before starting Installation Manager, ensure that the user who installs VCM has local administration rights for the Default Web Site.

1. Select **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand the server node and the **Sites** node.
3. Right-click **Default Web Site** and select **Edit Permissions**.
4. Click **Security** and verify that the user is listed with full rights or is a member of the Administrators group.

Verify No Agent is Currently Installed

The target Collector machine must not have an Agent installed.

To determine if an Agent is installed, look for the folder: `%systemroot%\CMAgent` (this location is the default; your location may vary). If the folder exists, use the steps below to uninstall the Agent components.

If you know the Agent was not installed using the MSI installer, to uninstall the Agent enter the single command:

```
%systemroot%\CMAgent\Uninstall\Packages\EcmAgentInstall\ UnEcmAgentInstall.exe /S
INSTALL.LOG
```

If the Agent was installed using the MSI installer, or if you do not know how the Agent was installed, contact VMware Customer Support for alternative instructions.

Run Foundation Checker

Foundation Checker is a tool that runs system checks on the VCM Collector machine. Foundation Checker automatically checks the machine to verify that all of the prerequisites are satisfied for a successful installation of VCM.

Installation Manager runs Foundation Checker automatically during the VCM installation. Running Foundation Checker as part of the Installation Manager process captures common issues that are difficult to remediate as well as issues related to specific components and the version of VCM being installed. Because Foundation Checker verifies component-specific issues against VCM, you should use Installation Manager to run Foundation Checker.

You can run Foundation Checker as a separate tool on an existing VCM machine to ensure that the machine meets the requirements for an upgrade. However, when you run Foundation Checker as a standalone tool, the checks will not capture all of the component-specific issues related to VCM. If you are confident that the machine meets the requirements for a VCM installation, it is better to use Installation Manager to perform the detailed checks.

The standalone version of Foundation Checker is available for download from the Download VMware vCenter Configuration Manager. To run Foundation Checker before you receive the VCM installation package, you can download the program.

1. Download the Foundation Checker files from the Download VMware vCenter Configuration Manager Web site at http://downloads.vmware.com/d/info/datacenter_downloads/vmware_vcenter_configuration_manager/5_0.
2. Review the *Foundation Checker User's Guide* that is included in the self-extracting zip (.exe). The guide provides instructions to run the standalone Foundation Checker.
3. Run Foundation Checker on your Collector. Follow the instructions provided to resolve any problems that might arise.

Hardware and Software Requirements for the Operating System Provisioning Server 5

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

You must first configure the server to meet the prerequisites provided here, and then install the OS Provisioning Server application as specified in *VCM Installation and Getting Started Guide*.

Supported Platform

The OS Provisioning Server can be installed on Red Hat Enterprise Linux version 5.2, 32- or 64-bit.

System Requirements

The machine on which you are installing the OS Provisioning Server must meet the following minimum requirements:

- **Memory:** For physical machines, 4 GB RAM is the minimum requirement; 8 GB RAM is recommended. For virtual machines, assign 1 GB to 4 GB to the virtual machine.
- **CPU:** For physical and virtual machines, two multi-core processors are recommended. The multitasking required to do OS provisioning is better served by a multiprocessor server.
- **Disk Space**: For physical and virtual machines, 100 GB minimum disk space to store the OS provisioning application and the repository database. Plan on an additional 20 GB for each operating system family you are importing into the repository.
- **Networking:** For optimal functionality, configure two network interfaces. One interface on the public network, and the second interface on the private provisioning network. Also, as a requirement of the system license policy, the hostname of the OS Provisioning Server must resolve to an IP address when pinged. The address can be assigned using DNS or specified in the /etc/hosts file. Use either method as appropriate for your local network requirements.

Software Requirements

In order for OS provisioning to function correctly, the machine on which you are installing the OS Provisioning Server requires the presence of some packages while others conflict and are not allowed. Verify the required and disallowed packages, making certain the required packages are present and remove any disallowed packages.

Required Packages

The Development Tools and Legacy Software Development package groups can be installed from Red Hat media. These packages are found in the Legacy Software Development option for Red Hat and include these components:

- cURL
- libstdc++.so.5, which is typically installed as part of compat-libstdc++-33
- libstdc++libc6.2-2, which is typically installed as part of compat-libstdc++-296
- libtool
- libtool-ltdl
- libtool-ltdl-devel
- kernel: If your Red Hat machine has 2 CPUs and 4 GB memory, install kernel-devel-2.6.18-92.el5. If your machine has 2 CPUs and 8 GB memory, install kernel-PAE-devel-2.6.18-92.el5.

Disallowed Packages

OS Provisioning depends on specific versions of certain system software packages that might differ from the version included by Red Hat. The OS Provisioning Server installation process provides the correct version of these software packages. You must uninstall other version of these packages before installing the OS Provisioning Server's provided versions. The packages are the following:

- fuse
- tftp-server
- system-config-netboot
- Any existing IBM Java2-SDK support

VCM Agent

Installing the VCM Agent on the OS Provisioning Server is optional; however, the Agent will help you manage the server, including monitoring disk space usage.

To install the Agent, see Add, License, and Install UNIX/Linux Machines.

Patching the OS Provisioning Server

You should exclude the OS Provisioning Server from automated patching in VCM. Patching the operating system will elevate the minor version and may leave the OS Provisioning Server in an unsupported state.

Network Requirements

Configure the following network settings to ensure proper OS Provisioning Server installation and functionality.

Provisioning Network Interface

When provisioning machines, a private network interface is easier to configure and more secure to use; however, you can also use a public network.

The provisioning network interface must be associated with the hardware interface named **eth1**.

Configure the provisioning network interface on the machine you are using as the OS Provisioning Server with a static IP address so that the OS Provisioning Server can act as a DHCP server. The following are the default and preferred values used throughout OS Provisioning Server installation process:

- **IP Address:** 10.11.12.1
- **Netmask:** 255.255.255.0.

Provisioning Network Port Usage

During the installation of OS distributions, internal application and services must communicate between the OS Provisioning Server and the target machines. If there are firewalls or routers between the OS Provisioning Server and the target machines, they must be configured to allow the following ports.

Table 5-1. OS Provisioning Ports

Application or Service	Port	Description
bootpd/DHCP	UDP 68	Provides address and server location of PXE configuration files.
TFTP	UDP 69	Downloads initial PXE/kernel.
http	TCP 80	Downloads kickstart and package files.
http	TCP 11080	Downloads kickstart and package files.
https	TCP 443	Helps create Windows deployment environment.
SSL	TCP 18821	SSL deployment service.
OS Provisioning Server	21310	Communication with the nodes, including messages and registration requests.
Stunnel	40607	Open on OS Provisioning Server so VCM's stunnel client can connect to the OS Provisioning Server stunnel server.
OS Provisioning Server	40610	Allows nodes to communicate with OS Provisioning Server, including messages and registration requests.
OS Provisioning Server Repository Server	21307	OS Provisioning Server web service listening for provisioning requests from VCM.
OS Provisioning Server Hardware Discovery	21309	Used by the hardware discovery program to communicate with the inventory daemon to add new machines into the OS Provisioning Server database.

Table 5-2. VCM Ports

Application or Service	Port	Description
OS Provisioning ServerRepository Server	21307	Local port connecting to the OS Provisioning Server web service listening for provisioning requests from VCM.

Provisioning Network Firewall Configuration

The following command is an alternative to setting the specific ports specified above.

Add the following entry in the /etc/sysconfig/iptables firewall configuration file to allow traffic on all ports on the provisioning network.

```
-A RH-Firewall-1-INPUT -i eth1 -j ACCEPT
```

Configure the OS Provisioning Server Firewall

Configure the firewall on the OS Provisioning Server to allow proper communication on the required ports.

NOTE If IPTABLES_SAVE_ON_STOP or IPTABLES_SAVE_ON_RESTART are set to "yes" in iptables-config, you should ensure that you do not accidentally lose your iptables changes.

Procedure

1. Log on to the designated OS Provisioning Server as root.
2. Change directory to /etc/sysconfig.
3. Open the iptables file and add the following line to allow communication on port 40607:

   …

   ```
   -A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 40607 -j ACCEPT
   ```

   …

   For example (Note highlighted example below):

   ```
   # Generated by iptables-save v1.3.5 on Fri Dec 3 14:51:10 2010
   *filter
   :INPUT ACCEPT [0:0]
   :FORWARD ACCEPT [0:0]
   :OUTPUT ACCEPT [468:43292]
   :RH-Firewall-1-INPUT - [0:0]
   -A INPUT -j RH-Firewall-1-INPUT
   -A FORWARD -j RH-Firewall-1-INPUT
   -A RH-Firewall-1-INPUT -i lo -j ACCEPT
   -A RH-Firewall-1-INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
   -A RH-Firewall-1-INPUT -p esp -j ACCEPT
   -A RH-Firewall-1-INPUT -p ah -j ACCEPT
   -A RH-Firewall-1-INPUT -d 224.0.0.251 -p udp -m udp --dport 5353 -j ACCEPT
   -A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
   -A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
   -A RH-Firewall-1-INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
   -A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
   -A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 40607 -j ACCEPT
   ```

```
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Fri Dec 3 14:51:10 2010
```

4. Restart the iptables service using the following command:

```
service iptables restart
```

Configure SQL Server for VCM

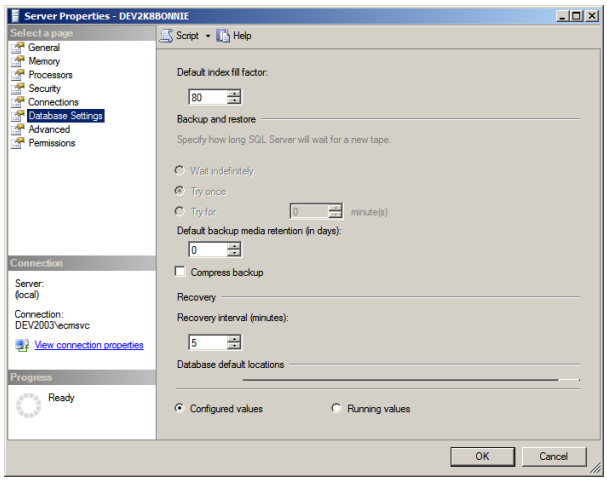
6

SQL Server 2008 R2 is user friendly and designed so that even a novice Database Administrator (DBA) can set up and operate a high performing database system. However, because VCM places such a heavy load on the database, changes are required to the default settings to optimize SQL Server performance. By understanding the SQL Server actions, a DBA can tune SQL Server for use with VCM.

For details about the SQL Server setting related to the VCM databases, see the *VCM Installation and Getting Started Guide*.

SQL Server Database Settings

1. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Right-click the SQL instance that you installed and select **Properties**.
3. In the Select a page area, select **Database Settings**.



4. In the right pane, configure the following:
   - **Default index fill factor:** Type or select a percentage value, which specifies the amount of free space in each index page when the page is rebuilt.

     Set the fill factor to 80% to leave 20% free space available in each index page. Normally this setting is specified as part of the maintenance plan wizard. If you configure the default fill factor using this setting, remember to leave free space in an index when running a maintenance plan.

- **Recovery interval (minutes):** Type or select 5. This setting configures the approximate amount of time that SQL Server takes to run the recovery process.

  The default setting is 0, which means that the system automatically adjusts this value. If you allow SQL Server to automatically adjust the recovery interval, it will base the values on the historical operation of the server. Because VCM constantly changes how it interacts with SQL Server (for example, activities differ between an inspection request and a compliance run), the server spends a lot of time constantly adjusting this value. By setting the recovery interval to 5 minutes, you allow SQL Server to forget about tuning this value. In large environments, the recovery interval can affect the overall performance of VCM.

5. Click **OK** to save the settings.

SQL Server Processor Settings

In multi-processor environments, it is very important to configure the SQL Servers use of the processors correctly by reserving a processor (removing it from SQL Server) for other functions such as the Collector service and IIS.

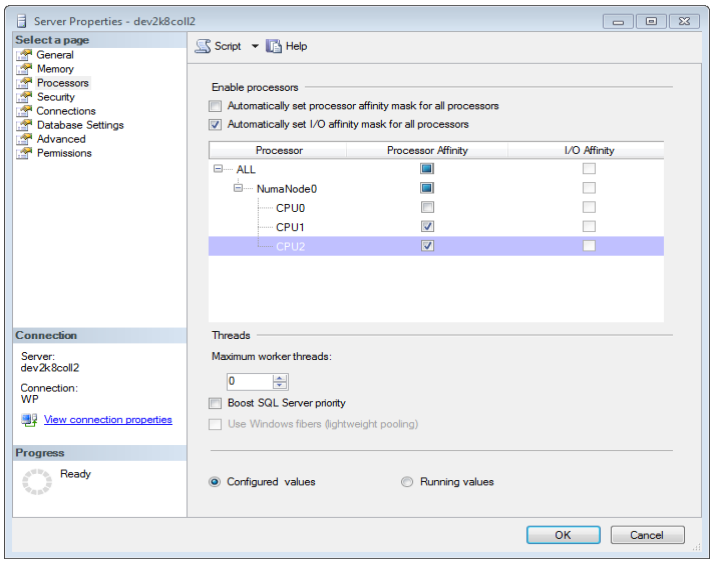
NOTE IIS cannot make use of processor "affinity" in multi-processor machines, so it uses them all equally.

Hyper-threading is a machine-level setting that must be controlled via BIOS settings. The main disadvantage of hyper-threading is that the two threads that run concurrently in one core share the same cache. If these threads are performing calculations, they will not interfere with each other and will run significantly faster than a single thread. However, if the threads are each working with a relatively large block of data, as when processing a SQL query, their activities will step on each other's cache, which can cause the two threads to accomplish less work than could be accomplished by a single thread.

Configuring SQL Server Processor Settings

To set the maximum worker threads or boost the SQL Server priority, configure the SQL Server Processor settings.

1. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Right-click the SQL instance that you installed and select **Properties**.
3. In the Select a page area, select **Processors**.



4. Select the **Automatically set I/O affinity mask for all processors** check box, located below the processor list, and then select all **I/O Affinity** check boxes for all processors in the **Enable processors** list.
5. In the right pane, configure the following, as needed:
   - To remove a processor from SQL Server, simply clear the check box next to the processor you want to reserve for the OS. It is best if you remove the processor that the network card will utilize so network communication will not affect SQL Server. Most cards use the first processor, although some Intel cards do use the last processor. It is important to remember that the SQL Server service must be restarted for the changes to take effect.
   - If Hyper-threading is enabled, then the list of processors will normally start at 0 through the number of physical cores and repeat to cover the Hyper-thread-created "processors." So, to unlink the first core from SQL in a four-CPU Hyper-threaded system (eight processors according to the OS), clear the check boxes next to CPU 0 and CPU 4.

     NOTE This is the preferred logical processor enumeration sequence recommended to BIOS vendors by Intel as part of it's Netburst architecture. There are, however, some BIOSes that do utilize this preferred sequence, and instead would show the two threads of the first Hyper-threaded CPU as logical CPU's 0 and 1. To be absolutely sure which algorithm is used may require checking with the BIOS vendor, or comparing SQL Server processor affinity options with and without Hyper-threading enabled.

6. Click **OK** to save the settings.

SQL Server IO Configuration

IT organizations do not analyze the technical drivers behind Disk IO subsystems, SQL Server installations can result in configurations that have RAID 5 arrays, which are not preferred for SQL Server because of a compromise between write performance and data redundancy. The more redundant a system is, the more work is required to write data.

Because SQL Server is extremely disk-write intensive, performance suffers when SQL is configured with RAID 5. Understanding the RAID levels can help SQL DBAs configure the disk IO subsystem in the most efficient manner.

- **RAID 0.** "Striping Without Parity". In this configuration, each block of data is written to each disk in the array in a "round robin" fashion, which means each disk in the array holds only a portion of the total data written. Depending on the array configuration, this drastically improves read performance because data can be read in small parallel chunks. This method also provides improved write performance because data can be written in parallel. However, time is required to break the data into the "stripe" that will be written. Because no fault-tolerance exists in this model, when a drive fails in the array, the entire array fails. A minimum of 2 drives is required for RAID 0, and the resulting size of the array is calculated by adding the sizes of the drives together.
- **RAID 1.** "Disk Mirroring" or "Disk Duplexing", which means mirroring on a single channel, duplexing when multiple channels are used. In this configuration, each bit of data that is written to a single disk is duplicated on the second disk in the array. RAID 1 is limited to 2 physical disks, which means the array is capable of increasing the read performance. In a duplexed environment, the performance is theoretically doubled, while at the same time providing fault tolerance in case a drive fails. Write performance is not affected by RAID 1. Only 2 drives can participate in a RAID 1 array, and the size of the array is the same as a single disk.
- **RAID 5.** "Disk Striping with Parity". As with RAID 1, data is written to each disk in the array in a "round robin" fashion, but an additional block of data written as "parity" also exists. This parity information can be used to rebuild the array in case of a disk failure. RAID 5 is the most popular RAID configuration in data centers and represents an effective compromise between read performance and fault tolerance. Because time is required to calculate the parity stripe, write performance is not as good as RAID 0. A minimum of 3 disks is required for RAID 5. The size of the array is calculated by taking the added size of the total disks and subtracting the size of 1 disk. For example, 80GB + 80GB + 80GB is equal to the total array size of 160GB.
- **RAID 0+1.** "Mirror of Stripes". In this configuration, 2 RAID 0 arrays are mirrored with RAID 1, which provides the fast read and write performance of RAID 0 and the fault tolerant features of RAID 1, which addresses performance first and then fault tolerance.
- **RAID 10.** "Stripe of Mirrors". In this configuration, multiple RAID 1 arrays are also striped, which addresses fault tolerance first and then performance.

When you examine the RAID levels for use with SQL Server, follow these guidelines.

- SQL Server Log Files work best on RAID 10, and should never be used on RAID 5. If RAID 10 is not available, RAID 1 should be used.
- SQL Server Data Files work best on RAID 0+1, but can be used on RAID 5 with little degradation in performance.
- Multiple Disk channels are preferred. At the minimum, SQL Server Log files should be on a separate physical channel from the SQL Server Data files, and if possible, neither should be mixed with OS or Application files. For example, at a minimum SQL Server prefers 3 separate disk channels.

In addition to selecting the appropriate RAID configuration, consider disk interface and disk drive performance. VCM data storage needs are usually low enough relative to commonly available drives that the smallest drives are sufficient. Fast drives that have fast interfaces are important, along with having a good number of "spindles" (drives) per RAID to distribute read, write, and seek activity across devices. Most high-end drives are available in 10,000 RPM or 15,000 RPM spin rates. The faster spinning drives usually seek faster and can achieve a higher sustained data throughput because more of the platter surface area passes under the heads in each second. Two primary interface technologies are suitable for use in high-throughput RAIDS:

- Ultra 320 SCSI, or U320 supports up to 320MB/s throughput per channel. The HP SmartArray 6404 can support multiple U320 channels (four in the case of the SA6404) and on-board, battery-backed-up cache. The cache provides for increased read and write performance because it allows the controller to batch requests to the drives.
- Serial Attached SCSI (SAS) uses special 2.5" drives, and has a higher data rate than the U320, up to 600MB/s for newer controllers. SAS controllers typically have more ports than the channels in U320 controllers. Ports and channels are similar because they provide parallel data paths through the controller. For example, an HP P600 provides 8 ports and each port is capable of 300MB/s.

For U320, the interface capacity is often the bottleneck. With SAS, the drives themselves can be the bottlenect. SAS seems to provide better performance, flexibility, and scalability than U320 for VCM installations. In addition to being faster and usually less expensive, SAS drives, although smaller, allow for more spindles in the same rack space.

Regardless of the technology used, a consideration when designing RAIDs is that it is generally best to utilize multiple channels or ports for high-throughput logical drives. For example, an 8-drive RAID 1+0 on a single U320 channel provides 320MB/s of sustained throughput, while the same drives in a RAID with four on each channel of a two-channel U320 controller (striped within the channels and mirrored between channels) provides 640MB/s sustained throughput and offers additional fault tolerance to controller channel or cable problems. If each quad of drives is in a different cabinet, this setup also provides fault tolerance for cabinet failures.

An alternative to local storage for VCM is to use SAN storage. A common problem with SANs and VCM previously was that many SANs are designed for file server or mailbox use and are not well-suited to high-throughput OLTP-type activities. For a SAN to provide good performance with VCM, it must be properly configured internally, and all devices between the SAN and the Collector must be adequate for the task. A 4Gb HBA is capable of slightly higher throughput than the single Ultra 320 SCSI channel. For write activities, since mirroring and striping is handled internally at the SAN, the throughput of the 4Gb HBA is more comparable to two and a half U320 channels. Getting that throughput depends also on the switches and links between the Collector and the SAN and between the drives and the controllers in the SAN.

When considering SAN storage for VCM, throughput (read and write speed) and access latency should be considered. Both are important because VCM performs many relatively small reads and writes. If the latency is too high, performance will be impacted as SQL Server waits for responses to these small queries before it can perform the next task.

After you have installed a Collector, analyze performance of the disk subsystem using Performance Monitor. The main counters of interest are the Physical Disk object's Disk Bytes/sec and Average Disk Queue Length counters. You can monitor both of these counters on a per-instance basis to determine the throughput and the number of threads that are queued for each logical drive that is associated with VCM activity.

The Disk Queue Length value is the best initial indicator about whether a logical drive has sufficient throughput and access speed for the tasks being required. Typically, the Disk Queue Length should not be more than twice the number of processors in the system for more than very short periods of time. When viewing this counter, a logical drive that is also used by the page file may show high queuing due to insufficient RAM in the system, but this counter can be very useful in determining whether disk subsystem resources are appropriate and whether the resources are optimally arranged, such as disks per channel, RAID type, etc.

Use SQLIO to Determine IO Channel Throughput

SQLIO is a tool that determines the I/O capacity of a SQL configuration. To predict how well VCM will function on a particular IO configuration, and to obtain a baseline of how well the IO subsystem functions, run SQLIO before you install VCM.

After you install SQLIO, configure these SQLIO settings to ensure an accurate report of IO throughput:

- 64K Block Size
- 4 Threads
- 2GB File Size minimum
- Sequential IO

When executing SQLIO, ensure that you create baseline information for each IO channel (logical disk) that will be used for VCM data as well testing both Read and Write operations.

Download SQLIO from the Microsoft download site.

Index