VMware vRealize Configuration Manager Advanced Installation Guide

vRealize Configuration Manager 5.8

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-001816-00

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 *VCM Advanced Installation Guide* describes the steps to install vRealize Configuration Manager (VCM) in all supported installation configurations. This document includes detailed information that does not appear in the *VCM Installation Guide*.

This document contains the following information:

- Hardware requirements for VCM Collector machines
- Software and operating system requirements for VCM Collector machines
- System prerequisites to install VCM
- Secure Communication Certificates
- Single-tier, two-tier, and three-tier installation configurations
- Configuring SQL Server for VCM
- Hardware requirements for VCM managed machines

Read this document and follow the procedures to successfully install VCM on existing physical or virtual machines in your environment. The example procedures in this guide are based on Microsoft SQL Server 2008 R2, 2012, and 2014 versions.

The *VCM Advanced Installation Guide* applies to VCM 5.8, Foundation Checker 5.8, and Service Desk Connector 1.3.0.

Intended Audience

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

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

Document Feedback

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

VMware VCM Documentation

The VCM documentation consists of the *VCM Installation Guide*, *VCM Administration Guide*, *VCM Advanced Installation 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.

Achieving a Successful VCM Installation 1

Perform the requirements to successfully install VMware vRealize Configuration Manager (VCM), and then install VCM in any of the supported single-tier, two-tier, or three-tier installation configurations.

Determine your specific hardware and software requirements for VMware vRealize Configuration Manager (VCM). Perform the preparatory steps to install and configure your physical and virtual machines for a successful VCM installation.

To determine your hardware and software requirements, begin by answering several questions.

- How many vCenter Server, UNIX, Linux, and Windows servers and workstations will you license?
- How often will you collect data?
- How much data will you collect?
- How long will you retain the collected data and change data?
- What additional VCM components will you use? For available VCM components, see the Download VMware vRealize Configuration Manager Web site.
- Do you understand the VCM security requirements? See the *VCM Security Guide*.

To achieve a successful VCM installation, you must understand the hardware and software requirements for VCM Collector machines and VCM managed machines, prepare your environment for VCM installation, then install VCM.

Before you install VCM, use the following chapters to prepare for VCM installation. Perform the prerequisite steps and procedures in the order presented, configure resources, configure your installation environment, then install VCM.

After you install VCM, set the file growth for your VCM database, then create a maintenance plan.

VCM Collector and Agent OS Platform Support

All Agent and Collector OS platform support is specific to versions and editions indicated in the supported platforms table.

On the VCM Collector, OS vendor hardening recommendations are tested, and the resulting configuration is supported. Custom lock downs and hardening beyond the OS vendor recommendations described in the *VCM Security Guide* are not tested or supported.

Custom configurations might reduce or block the performance or functionality of VCM components. Customizations include changes by non-OS vendors, third parties, endpoint security products, site policies, custom lock downs, or restricted access to or from systems.

Troubleshooting and support of VCM components in custom reconfigured or locked down environments is not included under the standard product maintenance agreement, but support for such environments is available through an additional Professional Services engagement.

For details about VCM Collector machines, see "Hardware Requirements for Collector Machines" on page 11 and "Software and Operating System Requirements for Collector Machines" on page 17.

For details about VCM managed machines, see "Hardware and Operating System Requirements for VCM Managed Machines" on page 167.

Hardware Requirements for Collector Machines

2

Your VCM Collector hardware requirements depend on the number of physical and virtual managed machines in your environment.

Disk space requirements vary based on the following factors.

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

Determine the Size of Your Environment

In VCM, the term “managed machines” refers to the servers and workstations that VCM manages, and from which VCM collects data. If you use VCM for Microsoft Active Directory (AD), this total should also include AD objects that you plan to have in your environment in the next 12 to 24 months.

VCM hardware requirements are recommended based on whether your environment contains 1–1000, 1001–2000, 2001–5000, or more managed machines. To determine the number of managed machines on which to base your collector size, consider the number of vCenter Server instances, Windows servers and workstations, Linux or UNIX machines, and virtual machines that you are licensing. 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. In the following example, an enterprise environment contains machines and objects that represent 1377 managed machines.

Table 2–1. Sample Sizing Worksheet

Product	Description	Anticipated Number of Managed Machines in the Next 12–24 Months
VCM	Windows Servers	92
	vSphere/ESX/ESXi Servers	5
	Virtual Machines	50
	Linux or UNIX	100
	Mac	100
	Windows Workstations	920
VCM for Active Directory	Divide total number of AD objects by 100 to determine the approximate "machine count" for your AD environment.	10,000 AD Objects/100 = 100 managed machines to accommodate VCM for AD
	Total Managed Machines:	**1377**

Use the blank worksheet to calculate and record the managed machines in your environment.

Table 2–2. Blank Sizing Worksheet

Product	Description	Anticipated Number of Managed Machines in the Next 12–24 Months
VCM	Windows Servers	
	vSphere/ESX/ESXi Servers	
	Virtual Machines	
	Linux or UNIX	
	Mac	
	Windows Workstations	
VCM for Active Directory	Divide total number of AD objects by 100 to determine the approximate "machine count" for your AD environment.	
	Total Managed Machines:	

Identify Your Specific Hardware Requirements

Size your VCM Collector and database based on the requirements for managed vCenter Server instances and the number of machines managed by VCM.

Database Sizing for Managed vCenter Server Instances

Use the following requirements to size your SQL Server database depending on the number of hosts and guests per vCenter Server managed by VCM. Guest collections include only the virtual machine data that vCenter provides and do not include any in-guest data. In-guest collections are separate from vCenter collections.

These requirements are in addition to the base VCM storage requirements, and are based on an estimated 10% data change per day times 15 days of data retention.

Table 2–3. VCM Database Sizing per vCenter Server Instance

Hosts	Guests	Est. Daily Change	Data Retention in Days	Data Size
25	250	10%	15	3GB
50	500	10%	15	6GB
250	2500	10%	15	30GB

The best practice in production environments is to have the Managing Agent process requests for a single vCenter Server. Dedicate one Managing Agent machine for each vCenter Server. In a single vCenter Server instance environment, the VCM Collector can be the Managing Agent.

A single Managing Agent can manage multiple vCenter Server instances depending on your collection schedules and when potential job latency is not an issue, such as when a single Managing Agent must process multiple requests serially. A single Managing Agent can manage multiple vCenter Server instances as long as only one vCenter Server is collected at a time.

When job latency is not a problem, and depending on your collection schedules, you might dedicate a single Managing Agent for every five vCenter Server instances or 100 hosts. You could dedicate one Managing Agent to a vCenter Server that manages 100 hosts, or a collection of four vCenter Server instances that each manage 10 hosts could share a Managing Agent.

Hardware and Disk Requirements By Number of Managed Machines

Use the Minimum Hardware Requirements and Minimum Disk Configuration Requirements tables to determine your hardware and disk configuration requirements for a single-tier server installation.

Use the total number of managed machines from the Sizing Worksheet to locate your environment size (1–1000, 1000–2000, 2000–5000, or more). If you have more than 5000 machines in your environment, contact VMware Technical Support to help you determine your hardware requirements.

If you run SQL Server on a virtual machine, see *Microsoft SQL Server on VMware Best Practices Guide* at http://www.vmware.com/files/pdf/sql_server_best_practices_guide.pdf. If you run SQL Server in a Hyper-V environment, see *Best Practices and Performance Considerations for Running SQL Server 2008 in a Hyper-V Environment* on the Microsoft Web site.

The requirements listed in the following tables 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 change data.
- Simple recovery mode only.
- Daily VCM Patching collections.
- No applications other than VCM are running on your server.

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

Longer data retention, additional WMI, registry filters, and custom information collections also add to the requirements.

Table 2–4. Minimum Hardware Requirements to Support 1–1000 Managed Machines

	Single Tier	2-Tier Database	2-Tier Web/Collector	3-Tier Database	3-Tier Web	3-Tier Collector
Processor	Dual Xeon or single Dual Core 2GHz	Dual Xeon or single Dual Core 2GHz	Dual Xeon or single Dual Core 2GHz	Dual Xeon or single Dual Core 2GHz	Single processor 2GHz	Single processor 2GHz
RAM	8GB	8GB	4GB	8GB	4GB	4GB
Separate Disk Channels	2	2	1	2	1	1

Table 2–5. Minimum Hardware Requirements to Support 1001–2000 Managed Machines

	Single Tier	2-Tier Database	2-Tier Web/Collector	3-Tier Database	3-Tier Web	3-Tier Collector
Processor	Quad Xeon or two Dual Core 2GHz	Quad Xeon or two Dual Core 2GHz	Dual Xeon or single Dual Core 2GHz	Quad Xeon or two Dual Core 2GHz	Single processor 2GHz	Dual Xeon or single Dual Core 2GHz
RAM	12GB	12GB	4GB	12GB	4GB	4GB
Separate Disk Channels	3	3	2	3	1	2

Table 2–6. Minimum Hardware Requirements to Support 2001–5000 Managed Machines

	Single Tier	2-Tier Database	2-Tier Web/Collector	3-Tier Database	3-Tier Web	3-Tier Collector
Processor	Eight-way Xeon or four Dual Core 2GHz	Eight-way Xeon or four Dual Core 2GHz	Dual Xeon or single Dual Core 2GHz	Eight-way Xeon or four Dual Core 2GHz	Single processor 2GHz	Dual Xeon or single Dual Core 2GHz
RAM	16GB	16GB	8GB	16GB	4GB	8GB
Separate Disk Channels	4	4	2	4	1	2

The space allocations in the following table do not include space for backups. Allocate backup space that is equal to the size of the VCM data for a single full backup, or larger to keep multiple partial backups.

Table 2–7. 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
2001–5000	Channel 0 – RAID 1	OS	36GB
		Collector Data Files	113GB
	Channel 1 – RAID 1	TempDB	227GB
	Channel 2 – RAID 1	SQL Log Files	227GB
	Channel 3 – RAID 0+1 (recommended) or RAID 10	SQL Data Files	456GB

Software and Operating System Requirements for Collector Machines 3

Your VCM environment software configuration must meet the requirements to install VCM 5.8. The software requirements are based on the number of managed machines in your environment and your installation configuration.

The software requirements are organized into steps. You must perform the steps in the order specified to ensure a successful VCM installation.

All software requirements apply to the server in your single-tier installation. For more information about installation configurations, see "VCM Installation Configurations" on page 19.

Sizing Impact on Software Edition 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: 1–1000, 1001–2000, 2001–5000, or more. If you have more than 5000 machines in your environment, contact VMware Technical Support for your specific requirements.

VCM supports Standard, Enterprise, and Datacenter editions of SQL Server 2008 R2, 2012, or 2014 versions.

NOTE Do not run VCM in a production environment when using only an evaluation version of SQL Server. Evaluation versions are not supported for production.

Table 3–1. Minimum Software Edition Requirements by Number of VCM Managed Machines

Software Component	Number of Managed Machines		
	1–1000	**1001–2000**	**2001–5000**
Operating System	Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2	Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2	Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2
SQL Version	SQL Server 2008 R2, 2012, or 2014, Standard, Enterprise, or Datacenter Edition (64-bit)	SQL Server 2008 R2, 2012, or 2014, Standard, Enterprise, or Datacenter Edition (64-bit)	SQL Server 2008 R2, 2012, or 2014, Standard, Enterprise, or Datacenter Edition (64-bit)
SSRS Version	SQL Server 2008 R2, 2012, or 2014 Reporting Services	SQL Server 2008 R2, 2012, or 2014 Reporting Services	SQL Server 2008 R2, 2012, or 2014 Reporting Services

Software Installation and Configuration Overview

VCM supports the Collector running on a Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system. Complete the preparatory steps to prepare your Windows Server 2008 R2, 2012, or 2012 R2 machine for a successful VCM installation. When you use VCM Installation Manager to install VCM, the system checks will run without error, indicating that you have met all of the requirements to install VCM.

VCM supports several installation configurations including single-tier, two-tier, and three-tier. You use Installation Manager to install VCM in these configurations. See "Preparing for Installation" on page 19.

To understand the requirements to upgrade or migrate your environment to the latest version of VCM, see "Upgrading or Migrating VCM" on page 137.

Preparing for Installation 4

Prepare your environment for a VCM installation by performing the prerequisites to include hardware, software, and physical and virtual machines before you install VCM components and tools.

VCM Installation Configurations

VCM supports several installation configurations including single-tier, two-tier, and three-tier. Use Installation Manager to install VCM in these configurations.

- Single-Tier Server Installation

  In a single-tier server installation, the VCM database server, Web server, and the VCM Collector components reside on a single Windows Server 2008 R2, 2012, or 2012 R2 machine, which is referred to as the VCM Collector. The installation installs all of the core VCM components, including the databases, console, and services. This configuration enables integrated security by default.

- Two-Tier Split Installation

  In a two-tier split installation, the VCM database resides on a Windows Server 2008 R2, 2012, or 2012 R2 database server machine, and the VCM Collector and Web components reside together on a separate Windows Server 2008 R2, 2012, or 2012 R2 machine.

- Three-Tier Split Installation

  In a three-tier split installation, the VCM databases, the Web applications, and the VCM Collector components reside on three different Windows Server 2008 R2, 2012, or 2012 R2 machines.

To perform the prerequisite steps for VCM installation, see "System Prerequisites to Install VCM" on page 21.

System Prerequisites to Install VCM 5

Perform the system prerequisites to prepare your physical or virtual machine for VCM installation. The prerequisites ensure that your machine meets the requirements for your environment to support a successful VCM installation.

After you perform the system prerequisites, during VCM installation the Installation Manager runs system checks on the database server, Web server, and VCM Collector machine in your installation configuration. These system checks verify that you have satisfied all of the prerequisites for a successful VCM installation. During the system checks, Foundation Checker verifies component-specific issues against VCM, captures common issues, and identifies any problems with the version of VCM being installed.

Foundation Checker might generate warnings, which you must review. In some cases, you might need to resolve the warnings before you install VCM, even though the warnings will not prevent you from starting the installation.

If Foundation Checker generates errors, you must resolve them before you install VCM. For more information about Foundation Checker, see the *VCM Foundation Checker User's Guide*.

Use the following topics to verify your system requirements.

- Verify that your environment meets the security requirements. See the *VCM Security Guide*.
- "Establish Local Administration Rights" on the next page

  Verify that the user account of the person who performs the VCM installation, upgrade, or migration has all of the required rights.
- "Verify Browser Compatibility" on the next page

  Verify that the target VCM Collector machine, and any other machines that will access the VCM Web console interface on the VCM Collector, have a compatible Web browser installed.
- "Verify the Default Network Authority Account" on the next page

  Define the network authority account in the Local Administrators group on the Collector machine before you install VCM. The network authority account must be a domain account. VCM uses the default network authority account to collect data from Windows Agent machines.
- "Specify the Collector Services Account" on page 23

  Specify the Collector Service account to use during VCM installation. The account can be a system administrator account and must exist in the Local Administrators group on the Collector machine. The account must not be the Local System account.
- "Verify the VCM Agent is Not Installed" on page 24

The target Windows machine must not have a VCM Agent installed before you install VCM. If an Agent is installed, you must uninstall the Agent for VCM to install.

- "Verify the SQLXML Version" on page 25

  SQLXML provides client-side XML functionality and enhancements to existing SQL features. Verify that the correct version is installed.

Establish Local Administration Rights

Verify that the user account of the person who performs the VCM installation, upgrade, or migration has all of the required rights.

The following rights are required.

- System administrator on the machines on which the installation or upgrade is performed.
- System administrator on the database instance to be used.
- Member of a domain.

The installing user account should not be the account used for VCM services, because the login of the VCM service account is disabled during installation.

After installation, do not create a VCM user that uses the SQL Server services account credentials.

What to do next

Verify the compatibility of your browser. See "Verify Browser Compatibility" below.

Verify Browser Compatibility

Verify that the target VCM Collector machine, and any other machines that will access the VCM Web console interface on the VCM Collector, have a compatible Web browser installed.

VCM supports the following browsers.

- Internet Explorer version 8 and 9.
- Internet Explorer version 10 and 11 in compatibility mode.
- Mozilla Firefox version 34 or later with the Internet Explorer IE Tab add-on. This add-on requires supported Internet Explorer to be installed on the machine.

What to do next

Verify the default Network Authority account. See "Verify the Default Network Authority Account" below.

Verify the Default Network Authority Account

Define the network authority account in the Local Administrators group on the Collector machine before you install VCM. The network authority account must be a domain account. VCM uses the default network authority account to collect data from Windows Agent machines.

You specify the default network authority account during VCM installation. The default network authority account can be a system administrator account, such as a Domain Admin in the Local Admin Group.

It is acceptable, but not preferred, to use the same account for the Collector, VCM Remote, vSphere Client VCM Plug-in, and Tomcat service accounts. If you use a single account, the permissions required for the Collector service account are sufficient. The account must be a local administrator, should not be a domain administrator, has bulk-insert permissions in SQL, and is a dbo of the VCM databases. In general, the Default Network Authority should be a different account, possibly a Domain Administrator with rights on more systems in the environment.

Procedure

1. On the Collector, 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. Verify that the user has Windows administrator rights issued by the network administrator.

To change the network authority account after installing VCM, click **Administration** and select **Settings > Network Authority**.

What to do next

Keep Server Manager open to specify the Collector Services account. See "Specify the Collector Services Account" below.

Specify the Collector Services Account

Specify the Collector Service account to use during VCM installation. The account can be a system administrator account and must exist in the Local Administrators group on the Collector machine. The account must not be the Local System account.

Logging in to VCM using a service account can lead to unexpected or inconsistent behavior. Services that use the same account as a logged in user might modify the logged in user's current role or the machine group, or log the user out of the system.

If the password for the account changes, you must change the password in the Services Management console and the Component Services DCOM Config console.

Procedure

1. In Server Manager, verify that the Groups menu is open.

   If not, expand **Configuration**, expand **Local Users and Groups**, and click **Groups**.
2. Double-click **Administrators** and verify that the account used for Collector Services is listed as a member of the Administrators group.

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

What to do next

Verify that the VCM Agent is not installed on the Collector machine. See "Verify the VCM Agent is Not Installed" on the next page.

Verify the VCM Agent is Not Installed

The VCM Collector installation includes an updated Agent. The target Windows machine must not have a VCM Agent installed before you install VCM. If an Agent is installed, you must uninstall the Agent for VCM to install.

Procedure

1. To determine whether a VCM Agent is installed on the Windows machine, verify whether the following folder exists.

   ```
   %windir%\CMAgent
   ```

   The `%windir%` environment variable specifies the directory where Windows is installed. This folder is the default location. The Agent installation directory is accessible in the registry at the following location.

   ```
   HKLM\Software\Configuresoft\ECM\4.0\Common\PathsRootDir
   ```

2. If a VCM Agent is installed, remove the Agent from the target Windows machine.
   1. If a working VCM Collector exists, use the VCM Web console to unlicense this machine and remove the VCM Agent.
   2. If a working VCM Collector does not exist, uninstall the Agent manually.
3. To uninstall the Agent manually, determine if the Agent was installed using the MSI installer.
   1. Search for the string `CMAgent` under the following registry key.

      ```
      HKEY_LOCAL_
      MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
      ```

      If an `Uninstall` registry subkey exists that has a GUID-named key and reference to the VCM Agent, such as `{7C51E2CA-C932-44EF-8B77-3C03356A24CC}`, the VCM Agent was installed using the MSI Installer.
   2. Examine the uninstall data to confirm that this is the VCM Agent.
   3. Open the setting `UninstallString` and copy the value.

      An example value is as follows.

      ```
      MsiExec.exe /X{7C51E2CA-C932-44EF-8B77-3C03356A24CC}
      ```
   4. If an `Uninstall` GUID registry key that references the VCM Agent does not exist, the Agent was installed using the manual installer.
4. Uninstall the VCM Agent.
   1. If the Agent was installed using the MSI installer, to uninstall the Agent click **Start** and click **Run** to execute the command line using the `UninstallString` registry value.

      An example value is as follows.

      ```
      MsiExec.exe /X{7C51E2CA-C932-44EF-8B77-3C03356A24CC}.
      ```
   2. If the Agent was installed using the manual installer, run the following command to uninstall the Agent.

      ```
      %windir%\CMAgent\Uninstall\Packages\CMAgentInstall\UnCMAgentInstall.exe /S
      INSTALL.LOG
      ```

What to do next

Verify that the correct version of SQLXML is installed. See "Verify the SQLXML Version" below.

Verify the SQLXML Version

SQLXML provides client-side XML functionality and enhancements to existing SQL features. Verify that the correct version is installed.

Procedure

1. Click **Start** and click **Control Panel**.
2. Click **Programs** and select **Programs and Features**.
3. Verify that SQLXML 4.0 SP1 appears in the list of installed programs.
4. If SQLXML 4.0 SP1 does not appear, install it from the Microsoft Download Center.

What to do next

- If you will install VCM on a virtual machine, configure the disk, CPU, and memory resources. See "Configure Resources to Install VCM on a Virtual Machine" on page 27.
- Understand the use of secure communications certificates and be prepared to specify the certificates during VCM installation. See Secure Communications Certificates in the *VCM Installation Guide*.

Configure Resources to Install VCM on a Virtual Machine

6

To install VCM on a virtual machine, you must prepare the virtual machine to be used as a VCM Collector. Because VCM can place heavy workloads on the database, you must understand your environment workloads to determine the resource requirements.

For the VCM Collector to operate properly on a virtual machine, the virtual machine must satisfy several prerequisites to run SQL Server on a VMware virtual machine.You should provision the VCM virtual machine similar to a high throughput OLTP database application.

Use these guidelines to install VCM in development, test, or IT environments. For large scale environments, you might need to alter the requirements.

IMPORTANT Do not install VCM on a virtual machine on an ESX server that has over-allocated resources.

Prerequisites

- Follow the requirements for physical hardware.See the *VCM Installation Guide*.
- Perform the system prerequisite tasks. See the *VCM Installation Guide*.
- Follow the best practices to install SQL Server. See the *Microsoft SQL Server on VMware Best Practices Guide* available on the VMware Web site at http://www.vmware.com.

Procedure

1. "Configure the Disk to Install VCM on a Virtual Machine" on the next page

   Configure the disk for the virtual machine. For large scale environments, you might need to alter the requirements.

2. "Configure the CPU to Install VCM on a Virtual Machine" on the next page

   Configure the CPU for the virtual machine. For large scale environments, you might need to alter the requirements.

3. "Configure the Memory to Install VCM on a Virtual Machine" on page 29

   Allocate the memory for the virtual machine. For large scale environments, you might need to alter the requirements.

What to do next

Familiarize yourself with the certificate names in advance so that you can select them during installation. See the *VCM Installation Guide*.

Configure the Disk to Install VCM on a Virtual Machine

Configure the disk for the virtual machine. For large scale environments, you might need to alter the requirements.

Prerequisites

- Prepare the virtual machine to be used as a VCM Collector. See "Configure Resources to Install VCM on a Virtual Machine" on the previous page.
- Keep the spindle count consistent and allocate a sufficient number of spindles to the database files when you migrate VCM from a physical machine to a virtual machine.
- Place the database data files on multiple logical unit numbers (LUNs).
- Create a `TEMPDB` data file for each virtual CPU that is allocated to the VCM Collector.
- Use paravirtual SCSI (PVSCSI) controllers for the database disks to provide greater throughput and lower CPU utilization, which improves VCM performance.
- Maintain a 1:1 mapping between the number of virtual machines and the number of LUNs on a single ESX host to avoid disk I/O contention.

Procedure

1. Start vCenter Server.
2. Select your virtual machine.
3. Click the **Resource Allocation** tab.
4. In the CPU pane, click **Edit**.
5. In the Virtual Machine Properties dialog box, click the **Resources** tab.
6. In the Resource Allocation pane, click **Disk** and update the disk resource allocation to meet the needs of your environment.
7. Click **OK**.

What to do next

Configure the CPU for the virtual machine. See "Configure the CPU to Install VCM on a Virtual Machine" below.

Configure the CPU to Install VCM on a Virtual Machine

Configure the CPU for the virtual machine. For large scale environments, you might need to alter the requirements.

Prerequisites

- Prepare the virtual machine to be used as a VCM Collector. See "Configure Resources to Install VCM on a Virtual Machine" on the previous page.
- Test the workload in your planned virtualized environment to verify that the physical CPU resources on the ESX host adequately meet the needs of guest virtual machines.
- Provision multiple virtual CPUs only if the anticipated workload will use them. Over-provisioning might result in higher virtualization overhead.
- Install the latest version of VMware Tools on the guest operating system.

Procedure

1. Start vCenter Server.
2. Select your virtual machine.
3. Click the **Resource Allocation** tab.
4. In the CPU pane, click **Edit**.
5. In the Virtual Machine Properties dialog box, click the **Resources** tab.
6. In the Resource Allocation pane, click **CPU** and change the CPU resource allocation.
7. Click **OK**.

What to do next

Configure the memory for the virtual machine. See "Configure the Memory to Install VCM on a Virtual Machine" below.

Configure the Memory to Install VCM on a Virtual Machine

Allocate the memory for the virtual machine. For large scale environments, you might need to alter the requirements.

Prerequisites

- Prepare the virtual machine to be used as a VCM Collector. See "Configure Resources to Install VCM on a Virtual Machine" on page 27.
- Verify that the ESX host has sufficient cumulative physical memory resources to meet the needs of the guest virtual machines. Do not install VCM on an ESX server that has over allocated resources.
- On the ESX host, enable memory page sharing and memory ballooning to optimize memory.
- To reduce or avoid disk I/O, increase the database buffer cache.

Procedure

1. Start vCenter Server.
2. Select your virtual machine.
3. Click the **Resource Allocation** tab.
4. In the Memory pane, click **Edit**.
5. In the Virtual Machine Properties dialog box, click the **Resources** tab.
6. In the Resource Allocation pane, click **Memory** and change the memory resource allocation.
7. Click **OK**.

What to do next

Prepare your single-tier, two-tier, or three-tier installation configuration. See "Single-Tier Server Installation" on page 35, "Two-Tier Split Installation" on page 61, or "Three-Tier Split Installation" on page 91.

Secure Communications Certificates 7

During VCM installation, specify the Collector and Enterprise certificates. VCM uses Transport Layer Security (TLS) to secure all UNIX Agents and all Windows Agents using HTTP, and TLS uses certificates to authenticate the Collector and Agents to each other.

If you use your own certificates, you must familiarize yourself with the certificate names in advance so that you can select them during installation.

A valid Collector certificate must have the following attributes.

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

If you do not want to use your own certificates, you can have Installation Manager generate the Collector and Enterprise certificates for you, select the **Generate** option during the installation.

If you install more than one Collector that will communicate with the same Agents, or if you plan to replace or renew your certificates, follow the special considerations to generate and select certificates in VCM Installation Manager. See the *VCM Security Guide*.

Authenticating the Server to the Client

VCM supports Server Authentication to authenticate the server to the client. In VCM environments where TLS is used, VCM Agents verify the identity of the Collectors by verifying the certificates. If you use your own certificates, you must familiarize yourself with the certificate names in advance so that you can select them during installation.

The server typically authenticates a client or user by requiring information such as a user name and password. When Server Authentication is used, the client or user verifies that the server is valid. To accomplish this verification, the server provides a certificate issued by a trusted authority, such as Verisign. If your client Web browser has the Verisign Certified Authority certificate in its trusted store, the Web browser can trust that the server is actually the Web site you access.

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

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

Enterprise and Collector Certificates

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

Server authentication is required to establish a TLS connection with an Agent. All VCM Collectors should have a common Enterprise Certificate. Each Collector Certificate is issued by the Enterprise Certificate, and is capable of Server Authentication. Collector Certificates in VCM must adhere to the requirements for secure communications certificates. See "Secure Communications Certificates" on the previous page.

- The Collector Certificate initiates and secures a TLS communication channel with an HTTP Agent. The Agent must be able to establish that the Collector Certificate can be trusted, which means that the Collector Certificate is valid and the certification path starting with the Collector Certificate ends with a trusted certificate. By design, the Enterprise Certificate is installed in the Agent’s trusted store. The trust chain ends with the Enterprise Certificate.
- Self-signed Agent Certificates are generated during Agent installation, upon first contact from the Collector. Agent Certificates are used for Mutual Authentication only. VCM support for Mutual Authentication requires the administrator to manually verify the fingerprint of each Agent's certificate before marking those Agents as trusted in Administration > Certificates.
- The Collector Certificate and associated private key must be available to the Collector. This certificate is stored in the local machine personal system store.

Delivering Initial Certificates to Agents

VCM Agents use the Enterprise Certificate to validate Collector Certificates. The Agent must have access to the Enterprise Certificate as a trusted certificate. In most cases, VCM delivers and installs the Enterprise Certificate as needed during the HTTP Agent installation.

When you manually install Windows HTTP or VCM Remote client components, you must specify a path to the PEM file that provides the Enterprise Certificate and the Collector's public key.

Installing the Agent from a Disk (Windows only)

The VCM Installation DVD does not contain customer-specific certificates. If HTTP is specified, the manual VCM installer requests the location of the Enterprise Certificate file during the installation. You must have the Enterprise Certificate file available at installation time. You can copy the certificate file, which has a `.pem` extension, from the `CollectorData` folder on the Collector. You must copy the certificate file when you run the manual installer directly using `CMAgentInstall.exe` or when you use the **Agent Only** option in the DVD auto-run program.

Using CMAgentInstall.exe to install the Agent (Windows only)

The `CMAgentInstall.exe` or `CMAgent[version].msi` is the manual Agent installer program. The manual installer requests the location of the Enterprise Certificate file when HTTP is specified. You must have the Enterprise Certificate file available at installation time. You can copy the certificate file from the `CollectorData` folder on the Collector. For information about using the EXE and command line options to install the Agent, see the *VCM Administration Guide*.

Using the MSI Install Package

When you specify HTTP, the MSI Agent install package also requires access to the `.pem` file. For information about using the MSI and command line options to install the Agent, see the *VCM Administration Guide*.

Installing the Agent for Linux and UNIX

See Install the Agent on Linux and UNIX Machines in the *VCM Administration Guide*.

What to do next

Configure your installation configuration. See "Single-Tier Server Installation" on page 35, "Two-Tier Split Installation" on page 61, or "Three-Tier Split Installation" on page 91.

Single-Tier Server Installation 8

In a single-tier server installation, the VCM database server, Web server, and the VCM Collector components reside on a single Windows Server 2008 R2, 2012, or 2012 R2 machine, which is referred to as the VCM Collector. The installation installs all of the core VCM components, including the databases, console, and services. This configuration enables integrated security by default. Integrated security, also referred to as Windows Authentication or NT Challenge Response authentication, provides trusted logon to the Web console without having to configure Kerberos.

VCM 5.8 supports 64-bit environments that include 64-bit hardware, the 64-bit Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system, and SQL Server 2008 R2, or 2012, or 2014.

Figure 8–1. Single-Tier Server Installation Components

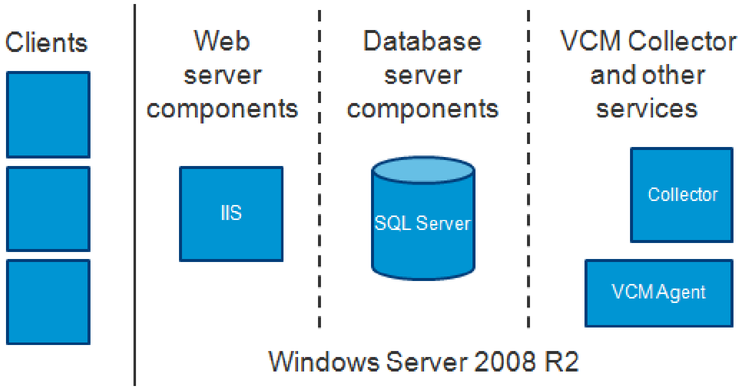
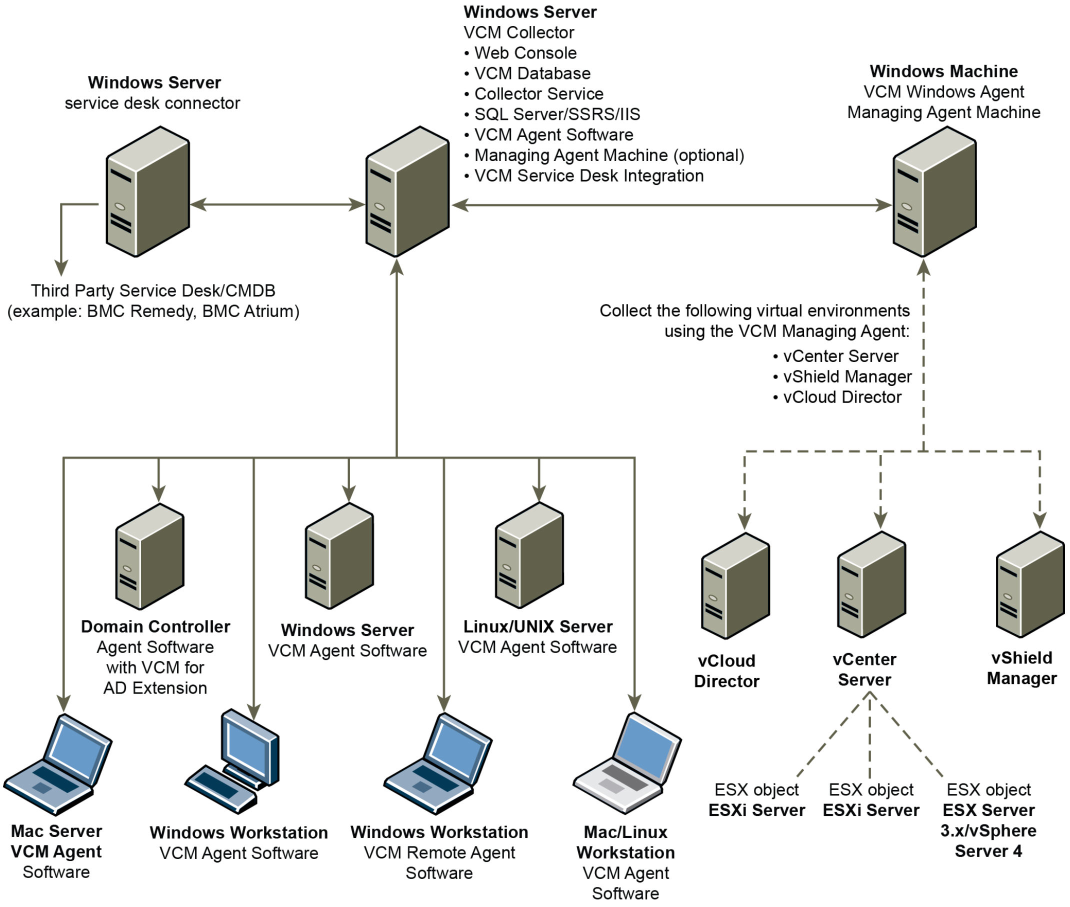


Figure 8–2. Typical VCM Enterprise-Wide, Single-Server Installation



VCM Agent Proxies for Virtualization can be installed on the VCM Collector, which is the default installation, or on one or more separate Windows Servers.

- If the Agent Proxy is installed on the VCM Collector, which is the default installation, the Collector communicates directly with the ESX Servers.
- If the Agent Proxy is installed on a separate Server, which is optional, the VCM Collector communicates with the Agent Proxy Server, which communicates with the ESX Servers.

Configure a Single-Tier Installation Environment

In a single-tier installation configuration, you configure the single Windows Server 2008 R2, 2012, or 2012 R2 machine for the Database, Web, and VCM Collector components, then install VCM. The machine can be a physical or virtual Windows machine.

Prerequisites

- Perform the general system prerequisites. See "System Prerequisites to Install VCM" on page 21.
- Connect the single Windows Server 2008 R2, 2012, or 2012 R2 VCM Collector machine to your domain.
- Obtain the installation media for the Enterprise, Standard, or Datacenter edition of SQL Server 2008 R2, 2012, or 2014, or verify access to a file share where the installer resides.
- Verify that the single-tier server machine has at least 11 GB of free disk space and 2GB of RAM.

Procedure

1. "Verify that the Installing User is an Administrator" below

   The user who installs Windows Server 2008 R2, 2012, or 2012 R2 operating system must be an Administrator and a domain account.

2. "Install and Configure Windows Server Operating System" on the next page

   Install the Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system on each Windows machine that serves as a tier in your configuration.

3. "Install the .NET Framework" on page 40

   To support library and language interoperability, the VCM Collector must have the required versions of the .NET Framework installed.

4. "Configuring the Database Components of the VCM Collector" on page 41

   To ensure that the installation creates the VCM databases, you must configure the database components of the VCM Collector before you install VCM. In a single-tier installation configuration, the VCM database resides on the VCM Collector. The databases include VCM, VCM_Coll, VCM_Raw, and VCM_UNIX.

5. "Configure the Web Components" on page 49

   The Web components of the VCM Collector contain Web applications such as IIS and SQL Server Reporting Services (SSRS), other services, and VCM software components. Before you install VCM, you must configure the Web components of the VCM Collector.

6. "Configure SSRS on the VCM Collector" on page 54

   SQL Server Reporting Services (SSRS) is a server-based report generation software system that is administered using a web interface and used to deliver VCM reports.

7. "Configure the VCM Collector Components" on page 59

   The VCM Collector contains the VCM software application and VCM services. To prepare the VCM Collector components for VCM installation, configure the required utilities.

What to do next

Review the DCOM and port requirements, and use VCM Installation Manager to install the VCM components. See "Installing VCM" on page 125.

Verify that the Installing User is an Administrator

The user who installs Windows Server 2008 R2, 2012, or 2012 R2 operating system must be an Administrator and a domain account.

Procedure

1. Verify that the user is an Administrator.

   a. Click **Start** and select **All Programs** > **Administrative Tools** > **Computer Management**.
   b. Expand **System Tools**, expand **Local Users and Groups**, and click **Users**.
   c. Right-click the user and click **Properties**.
   d. Click the **Member Of** tab and verify that **Administrators** is listed.
   e. If **Administrators** is not listed, add the user to the Administrators group.
   f. Click **Check Names** and click **OK**.

2. Verify that the user is a domain account.
   a. Click **Groups**.
   b. Right-click **Administrators** and click **Properties**.
   c. Verify that the Domain User is listed in the Members area.

What to do next

Prepare your Windows machine for VCM installation. See "Install and Configure Windows Server Operating System" below.

Install and Configure Windows Server Operating System

Install the Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system on each Windows machine that serves as a tier in your configuration.

Prerequisites

- Determine whether you require Windows Server 2008 R2, 2012, or 2012 R2 operating system. See "Sizing Impact on Software Edition Requirements" on page 17.
- The user who installs Windows Server 2008 R2, 2012, or 2012 R2 operating system must be an Administrator and a domain account. See "Verify that the Installing User is an Administrator" on page 37.
- Decide on a valid DNS computer name with no underscores for use when the Windows installation prompts for a machine name. If you attempt to change the machine name after a machine is identified as a Collector, problems might occur with VCM, SQL Server, and SQL Server Reporting Services.

Procedure

1. Install Microsoft Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 on your Windows machine.
2. During the installation, you can configure several options.

Option	Description
Regional and Language Options	Determines how numbers, dates, currencies, and time settings appear. ■ Language: Setting for your language. The default is English. ■ Time and currency format: Determines how numbers, dates, currencies, and time settings appear. The default is English (United States). ■ Keyboard or input method: Allows text entry for multiple languages. The default is US.
Disk Configuration	Allows you to separate the machine disk drive into partitions to store data in different partitions. You can create new disk partitions and delete existing partitions. After you configure the disk, select a partition on which to install Windows Server 2008 R2, 2012, or 2012 R2 Edition.
Product Key	When the installation prompts, enter your product key.
Licensing Modes	Windows Server 2008 R2, 2012, or 2012 R2 supports a single license that is included with the product key.
Administrator Password	The installation setup creates an account called administrator. To log in, you must create a password that complies with the criteria. The password must have the following attributes. ■ Minimum of six characters ■ Does not contain “administrator” or “admin” ■ Contains uppercase letters ■ Contains lower case letters ■ Contains numbers ■ Contains at least one non-alphanumeric character

3. Perform the initial configuration tasks to set the time zone and the computer name.

Disable the Remote Desktop Session Host

A Remote Desktop Session Host server hosts Windows-based programs for Remote Desktop Services clients.

If the Remote Desktop Session Host role service is enabled, you must disable it to avoid changes to settings for new connections, modifications of existing connections, or removal of connections.

Procedure

1. Click **Start** and select **All Programs** > **Administrative Tools** > **Server Manager**.
2. In the navigation pane, expand **Roles** and click **Remote Desktop Services**.
3. In the Remote Desktop Services pane, scroll down to Role Services.
4. Click the **Remote Desktop Session Host** role service to highlight it.
5. Click **Remove Role Services**.
6. Deselect the Remote Desktop Session Host role service and follow the prompts to finish disabling the Remote Desktop Session host role.

Enable DCOM

The Distributed Component Object Model (DCOM) protocol allows application components to interact across Windows machines. DCOM must be enabled on the Windows machine to install and run VCM.

Although DCOM is enabled by default when Windows Server 2008 R2, 2012, or 2012 R2 is installed, DCOM might have been disabled by a custom installation or a lock-down script.

Procedure

1. Click **Start** and select **All Programs** > **Administrative Tools** > **Component Services** to open Component Services.
2. In the Component Services navigation pane, expand **Component Services** and expand **Computers**.
3. Right-click the computer and click **Properties**.
4. Click the **Default Properties** tab.
5. Select **Enable Distributed COM on this computer** and click **OK**.

What to do next

Install the .NET framework. See "Install the .NET Framework" below.

Install the .NET Framework

To support library and language interoperability, the VCM Collector must have the required versions of the .NET Framework installed.

VCM 5.8 requires the .NET 3.5.1 Framework. If you use Package Studio, the VCM Collector must have .NET 3.5.1 installed. If you use Package Manager, the VCM Collector must have .NET 3.5.1 or .NET 4.0 installed.

Determine the installed version of the .NET Framework. If one of the .NET Framework versions is missing, install the version from the Microsoft download Web site.

Procedure

1. Click **Start** and select **All Programs** > **Administrative Tools** > **Server Manager**.
2. Click **Features**.
3. Verify that .NET Framework 3.5.1 appears in the feature summary.
4. If .NET Framework 3.5.1 does not appear, under Features select **Add Features** and select **.NET 3.5.1**.

Verify the ASP.NET Client System Web Version

To support client programming, verify the ASP.NET Client System Web version to confirm that the .NET framework is installed correctly, and install it if the version is not correct.

1. Click **Start** and select **All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand **<server name>** and click **Sites**.
3. Expand **Default Web Site**, expand **aspnet_client**, and expand **system_web**.
4. Verify that the version is **2_0_50727**.

Verify the ASP Role Service

To support client programming, verify the status of the ASP Role Service to confirm that the .NET framework is installed correctly.

Procedure

1. Click **Start** and select **All Programs > 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 whether the role service is installed.
6. If the role service is not installed, click **Add Role Services** and add the ASP role service.

Verify the ASP.NET Role Service

To support client programming, verify the status of the ASP.NET Role Service to confirm that the .NET framework is installed correctly.

Procedure

1. Click **Start** and select **All Programs > 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 role service is installed.
6. If the role service is not installed, click **Add Role Services** and add the ASP.NET role service.

What to do next

Configure the database components. See "Configuring the Database Components of the VCM Collector" below.

Configuring the Database Components of the VCM Collector

To ensure that the installation creates the VCM databases, you must configure the database components of the VCM Collector before you install VCM. In a single-tier installation configuration, the VCM database resides on the VCM Collector. The databases include VCM, VCM_Coll, VCM_Raw, and VCM_UNIX.

Use of a shared SQL Server is supported for VCM. However, VCM makes heavy use of SQL Server for query and transaction processing. You must ensure that you have or can add enough capacity to a shared SQL Server so that VCM and any other databases on the shared server do not experience poor performance.

VCM operates with a Standard, Enterprise, or Datacenter edition of SQL Server. You must install the 64-bit SQL Server 2008 R2, or 2012, or 2014 version on your designated database server machine and verify that the settings are configured correctly for a VCM installation.

If you plan to change the communication port that SQL Server uses 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 change the port after installation, you must configure additional SSRS settings to repair the configuration.

Install SQL Server on the VCM Collector

In a single-tier installation configuration, the VCM database server resides on the same server on which you install VCM. The database server contains the VCM, VCM_Coll, VCM_Raw, and VCM_UNIX databases. You must configure the VCM database server before you install VCM in a single-tier installation configuration.

NOTE Do not run VCM in a production environment when using only an evaluation version of SQL Server. Evaluation versions are not supported for production.

Prerequisites

- Obtain the installation media for the Enterprise, Standard, or Datacenter edition of SQL Server 2008 R2, 2012, or 2014, or verify access to a file share where the installer resides.

Procedure

1. Start the SQL Server installation.
2. Perform the following actions to install SQL Server.

For SQL Server 2008 R2

Wizard Page	Action
SQL Server Installation Center	Click **New installation or add features to an existing installation**.
Setup Support Rules	Click **Install** and verify that all of the rules pass. To view the detailed system configuration check report, click the link.
Setup Support Files	Click **Install** to install the setup support files.
Setup Support Rules – for SQL Server Setup support files	Verify that all of the rules passed.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.

Wizard Page	Action
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: ■ Database Engine Services ■ Reporting Services Shared Features: ■ Client Tools Connectivity ■ SQL Server Books Online ■ Management Tools - Basic and Management Tools - Complete
Installation Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Disk Space Requirements	Review the disk usage summary.
Server Configuration	Click **Use the same account for all SQL Server services** and enter the NT AUTHORITY\SYSTEM account and password. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Database Engine Configuration	Select **Windows authentication** and click **Add Current User** to add the account to the SQL Server administrators.
Reporting Services Configuration	Specify the reporting services configuration mode. Select **Install the native mode default configuration**.
Error Reporting	Review the summary information.
Installation Configuration Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

For SQL Server 2012

Wizard Page	Action
SQL Server Installation Center	Click **New SQL Server stand-alone installation or add features to an existing installation**.
Setup Support Rules	Click **Install** and verify that all of the rules pass. To view the detailed system configuration check report, click the link.
Product Updates	Check for SQL Server updates.
Install Setup Files	Verify that all rules are passed.
Setup Support Rules – for SQL Server Setup support files	Verify that all of the rules passed.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: ▪ Database Engine Services ▪ Reporting Services Shared Features: ▪ Client Tools Connectivity ▪ Management Tools - Basic and Management Tools - Complete
Installation Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Disk Space Requirements	Review the disk usage summary.
Server Configuration	Browse the accounts for all SQL services and enter the NT AUTHORITY\SYSTEM account. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.

Wizard Page	Action
Database Engine Configuration	Select **Windows authentication** and click **Add Current User** to add the account to the SQL Server administrators.
Reporting Services Configuration	Specify the reporting services configuration mode. Select **Install and Configure**.
Error Reporting	Review the summary information.
Installation Configuration Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

For SQL Server 2014

Wizard Page	Action
SQL Server Installation Center	Click **New SQL Server stand-alone installation or add features to an existing installation**.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Microsoft Update	Use this option to check for Microsoft updates.
Install Setup Files	Verify that all rules are passed.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: ■ Database Engine Services ■ Reporting Services Shared Features: ■ Client Tools Connectivity ■ Management Tools - Basic and Management Tools - Complete
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.

Wizard Page	Action
Server Configuration	Browse the accounts for all SQL services and enter the NT AUTHORITY\SYSTEM account. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Database Engine Configuration	Select **Windows authentication** and click **Add Current User** to add the account to the SQL Server administrators.
Reporting Services Configuration	Specify the reporting services configuration mode. Select **Install and Configure**.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

What to do next

- Reboot the single-server machine.
- Configure the SQL Server properties. See "Verify and Configure the SQL Server Properties" below.

Verify and Configure the SQL Server Properties

To ensure that SQL Server will operate with VCM, 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 Administration Guide*.

Procedure

1. Launch **SQL Server Management Studio**.
2. Right-click the SQL instance and select **Properties**.
3. Confirm the General page server property of Version as 10.50.1600.1 or some later build of version 10.50.
4. Select and confirm the Security page server properties.
   a. Select Windows Authentication mode, which is recommended.
   b. Although SQL Server and Windows Authentication mode is acceptable for VCM, select Windows Authentication mode, which is recommended.
5. Select and confirm the Database Settings page server properties.
   a. For 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 keep 20% free space available in each index page.
   b. For Recovery interval (minutes), type or select 5.
6. Click **OK** to save your changes.

What to do next

To ensure that SQL Server and VCM operate correctly together, verify that the SQL Server name matches the Windows machine name. See "Verify Matching SQL Server and Computer Names" below.

Verify Matching SQL Server and Computer Names

To ensure that SQL Server and VCM operate correctly together, you must verify that the SQL Server name matches the Windows machine name. If you recently installed SQL Server, you do not need to verify that the names match. If you obtained a machine that was renamed after the operating system and SQL Server were installed, verify and reset the SQL Server server name.

Procedure

1. Launch **SQL Server Management Studio**.
2. Click **Database Engine Query**.
3. In the **SQL Query** pane, type **`SELECT @@Servername`** and click **Execute**.
4. Verify that the resulting SQL Server name matches the Windows machine name.
5. If the SQL Server name does not match the Windows machine name, reset the SQL Server name.
    a. In the SQL Query pane, type the following command and replace `NewServerName` with the server name.

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

    b. Click **Execute**.

    c. To restart the SQL Server services, click **Start** and select **Programs > Microsoft SQL Server {version} > Configuration Tools > SQL Server Configuration Manager > SQL Server {version} Services**.

    d. Right-click **SQL Server** and click **Restart**.
6. Reboot the database server machine.

What to do next

Verify that the SQL Server Agent service account has the SQL Server `sysadmin` role. See "Verify the SQL Server Agent Service Account is a sysadmin" below.

Verify the SQL Server Agent Service Account is a sysadmin

The SQL Server Agent service account that runs scheduled jobs in SQL Server must be a sysadmin.

Procedure

1. Launch **SQL Server Management Studio**.
2. Expand the server, expand **Security**, expand **Server Roles**.
3. Double-click `sysadmin` and view the members of the sysadmin role.
4. Verify that the account to use for the SQL Server Agent service is a member of the `sysadmin` fixed role.
5. If the account is not a member of the `sysadmin` fixed role, add this role to the account.

What to do next

Verify that the SQL Server Agent service is configured to start automatically. See "Verify that the SQL Server Agent Service Starts Automatically" below.

Verify that the SQL Server Agent Service Starts Automatically

VCM uses the SQL Server Agent service to run all scheduled jobs and SSRS reports, including dashboards. Set the service to automatically start on the VCM server.

Procedure

1. On the VCM server, click **Start** and select **Administrative Tools** > **Services**.
2. Right-click **SQL Server Agent**, and select **Properties**.
3. From the **Startup type** menu, select **Automatic**.
4. Click **OK**, and close the Services window.

What to do next

Select the SQL Server Agent service account See "Select the SQL Server Agent Service Account" below.

Select the SQL Server Agent Service Account

SQL Server Agent is a service that runs scheduled jobs in SQL Server and runs as a specific user account. Verify that the SQL Server Agent service account that you provided during the SQL Server installation is a SQL Server sysadmin.

Prerequisites

- Verify that the account you provide for the SQL Server Agent service has permission to log in as a service and the required additional permissions. See the online Microsoft Developer Network for more information.
- Understand the supported service account types for non-clustered and clustered servers. VCM 5.8 supports Active/Active SQL clusters. See the online Microsoft Developer Network for more information.
- Verify that the account you will use for the SQL Server Agent service account has the `sysadmin` privilege. See "Verify the SQL Server Agent Service Account is a sysadmin" on page 47.

Procedure

1. On the VCM database server machine, click **Start** and select **All Programs**.
2. Click **Microsoft SQL Server {version}** > **Configuration Tools > SQL Server Configuration Manager**.

3. Click **SQL Server Services**.
4. Right-click **SQL Server Agent (MSSQLSERVER)** and click **Properties**.
5. On the Log On tab, select a log in option and provide the account information.

Option	Description
Built-in account	In a single-tier installation, you can select the Local System account, which has unrestricted access to all system resources. In a split installation environment, do not select the built-in Local System account. This account is a member of the Windows Administrators group on the local machine.
This account	In a split installation, the SQL Server Agent must be running as a user account. Select a Windows domain account for the SQL Server Agent service account. This option provides increased security. Select this option for jobs that require application resources across a network, to forward events to other Windows application logs, or to notify administrators through email or pagers.

6. Type or select an account name that has the `sysadmin` privilege.
7. Click **OK**.

What to do next

Establish SQL Server administration rights. See "Establish SQL Server Administration Rights" below.

Establish SQL Server Administration Rights

Members of the SQL Server `sysadmin` fixed server role can perform any activity in the server. The user who installs VCM must have SQL Server `sysadmin` rights.

Procedure

1. Launch **SQL Server Management Studio**.
2. Expand the server instance, select **Security** and select **Logins**.
3. Right-click the login ID 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, select the **sysadmin** check box.
6. Click **OK** to save the settings and close the window.

What to do next

Configure the Web components of the VCM Collector. See "Configure the Web Components" below.

Configure the Web Components

The Web components of the VCM Collector contain Web applications such as IIS and SQL Server Reporting Services (SSRS), other services, and VCM software components. Before you install VCM, you must configure the Web components of the VCM Collector.

The Windows machine that hosts the Web components must be running Internet Information Services (IIS) 7.5. IIS is installed when you install Windows Server 2008 R2, 2012, or 2012 R2.

The SQL Server license includes SQL Server Reporting Services (SSRS). In your installation configuration, when you run SSRS and SQL Server on the same machine, the SQL Server database machine can take on the role of the Report Server (SSRS).

VCM 5.8 supports running SSRS on the Web server or on the database server in a split installation. Depending on the separation of services in your environment, you might want to install SSRS on the Web server machine in a split installation, because SSRS has its own Web server.

If you install SSRS on the Web server, it requires an additional SQL Server license, because you are installing SSRS on a Windows Server 2008 R2, 2012, or 2012 R2 machine that is separate from the SQL Server database services. If you run SQL Server Enterprise Edition, all SQL Server services running in guests on a single virtual machine host are covered by the Enterprise Edition license.

Prerequisites

- Perform the prerequisite tasks for your installation configuration.
- Place the Web server in the Internet Explorer Trusted Zone so that Internet Explorer can delegate the VCM user's credentials to the Web service for use with SQL Server. See "Place the Web Server in the Internet Explorer Trusted Zone" on page 107.
- If the domain firewall is turned on, verify that any required ports are open. If the database server is blocked from communicating with the Collector, problems can occur when you submit jobs. VCM displays an error about the SAS service, and the VCM Debug Event Log displays failures when calling `ecm_sp_collector_control`.
- Verify that .NET Framework 3.5.1 is installed on Windows Server 2008 R2, 2012, or 2012 R2 machines where Package Studio will be installed.
- Verify that you have an Internet connection to check for patch bulletin updates.
- On the Windows Server 2008 R2, 2012, or 2012 R2 Web server machine, verify that the following .NET Framework components are installed.
  - Windows Process Activation Service
  - Process Model
  - .NET Environment
  - Configuration APIs

Procedure

1. Restart the Web server machine.
2. Click **Start** and select **All Programs > Administrative Tools > Server Manager**.
3. Click **Roles** and verify that the Web Server (IIS) role appears.
4. If the Web Server (IIS) role does not appear, in the Roles Summary area, click **Add Roles** and add the Web Server (IIS) role.
5. On the Select Server Roles page, select **Web Server (IIS)** and select the Web Server components to add.

Option	Action
Common HTTP Features	Select these options: ■ Static Content ■ Default Document ■ Directory Browsing ■ HTTP Errors
Application Development	Select these options: ■ ASP .NET ■ .Net Extensibility ■ ASP ■ ISAPI Extensions ■ ISAPI Filters ■ Server Side Includes
Health and Diagnostics	Select these options: ■ HTTP Logging ■ Request Monitor
Security	Select these options: ■ Basic Authentication ■ Request Filtering
Performance	Select: ■ Static Content Compression

Configuring IIS

To ensure that the Web components are correctly configured, verify that the correct role services are enabled, the bindings are set correctly, and the default Web site is correct.

Verify the IIS 7.5 Role Services are Enabled

Verify that the correct IIS 7.5 Role Services are enabled on the VCM Collector.

Procedure

1. On the Collector, click **Start** and select **All Programs > Administrative Tools > Server Manager**.
2. Expand **Roles** and click **Web Server (IIS)**.
3. If the Web Server (IIS) role does not appear in the list of Roles, scroll to Role Services, click Add Role Services and add the Web Server (IIS) Role.

   When you installed IIS, the ASP Role Service, ASP.NET Role Service, and IIS ServerSideIncludes Role Service were installed.

4. In the Web Server (IIS) pane, scroll to **Role Services** and verify that the status is set to **Installed** for the following Role Services.

Role Service Category	Role Service
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 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

5. If any of the Role Services are not installed, click **Add Role Services**, select the check boxes of the services to install, and click **Install**.

Configure the IIS 7.5 Settings

IIS settings configure the information required for requests to communicate with a Web site. To support VCM interaction with IIS, configure the settings for the IIS 7.5 bindings on the VCM Collector machine to ensure that the settings are correct.

Procedure

1. Click **Start** and select **All Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Expand **<server name>**, expand **Sites**, and click **Default Web Site**.
3. In the Actions pane, under Manage Web Site and Browse Web Site, click **Advanced Settings**.
4. Expand **Connection Limits** and set Connection Time-out (seconds) to `3600`.
5. Click **OK**.

Verify the IIS 7.5 Default Web Site

IIS 7.5 provides a default Web site that defines the default authentication settings for applications and virtual directories. Verify that the IIS 7.5 default Web site has the correct settings.

Procedure

1. Click **Start** and select **All Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Expand **<server name>**, expand **Sites**, and click **Default Web Site**.
3. In the Default Web Site Home pane, locate the IIS options.
4. Double-click **Authentication** and set the authentication.

Option	Action
Anonymous Authentication	Set to **Disabled**.
ASP.NET Impersonation	Set to **Disabled**.
Basic Authentication	Set to **Enabled**.
Forms Authentication	Set to **Disabled**.

Verify the ISAPI Extensions

The ISAPI Extensions role provides support for dynamic Web content development. You must verify that the role service is installed, and install it if needed.

Procedure

1. Click **Start** and select **All Programs** > **Administrative Tools** > **Server Manager**.
2. Expand **Server Manager (<server name>)** and expand **Roles**.
3. Click **Web Server (IIS)**.
4. Scroll to Role Services.
5. Locate ISAPI Extensions and verify that the role service is installed.
6. If the role service is not installed, click **Add Role Services** and add the ISAPI Extensions role service.

What to do next

Prepare SQL Server Reporting Services (SSRS) to generate VCM reports. See "Configure SSRS on the VCM Collector" on the next page.

Configure SSRS on the VCM Collector

SQL Server Reporting Services (SSRS) is a server-based report generation software system that is administered using a web interface and used to deliver VCM reports.

Back Up Your SSRS Key

The `rskeymgmt` utility manages the symmetric keys used by a report server. This utility provides a way to delete encrypted content that can no longer be used if you cannot recover or apply the key.

Use the Microsoft command-line utility to back up the symmetric key to an encrypted file.

Prerequisites

- See the online Microsoft Support center for details about how to use the `rskeymgmt` utility.

Procedure

1. On the Collector file system, locate the `rskeymgmt.exe` utility at `c:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn` or the directory where you installed SQL Server.
2. To copy your SSRS key set to a removable media device and store it in a secure location, open a command line prompt and run the `rskeymgmt.exe` utility with the appropriate options.

Disable IE Protected Mode for SSRS

On the VCM Collector, when User Account Control (UAC) is turned on and Internet Explorer Protected Mode is enabled, SSRS user permissions errors and Web service errors on dashboards and node summaries can occur. UAC and Internet Explorer Protected Mode also block access to the http://localhost/reports SSRS administration interfaces. If you use another machine to access the VCM Web console interface, this problem does not occur.

CAUTION Do not use the VCM Collector Web console interface for general Internet access, because doing so causes VCM SSRS dashboard errors. If you access the Internet through the VCM Collector Web console interface, to enable the SSRS dashboards you must either disable Internet Explorer Protected Mode for the zone of the Collector or run Internet Explorer as administrator.

Do not modify the Internet Explorer Protected Mode setting in other circumstances, because doing so reduces the protection on the Collector and can increase the exposure of the Collector to attacks through Internet Explorer.

Procedure

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

Configure SSRS

Configure SSRS manually in your installation configuration, because the SSRS command-line configuration tool does not perform these steps.

SSRS might require HTTPS during installation. If HTTPS is required, you manually export a self-signed certificate and import it to the VCM Collector machine's root certificate store. If you do not manually export the certificate, a manual import of a VCM report might fail. If the manual import fails, run the import from the VCM Collector machine. For more information, see the Microsoft IIS Resource Kit Tools.

Prerequisites

- Back up your SSRS key. See "Back Up Your SSRS Key" on the previous page.
- Disable the Internet Explorer Protected Mode. See "Disable IE Protected Mode for SSRS" on the previous page.

Procedure

1. On your single server, start SQL Server 2008 R2, 2012, or 2014 Reporting Services Configuration Manager.
   a. Click **Start**, select **Run**, and type `rsconfigtool.exe`.
   b. In the Reporting Services Configuration Connection dialog box, click **Connect** to connect and log in to SQL Server Reporting Services.
2. Update the SQL Server database.
   a. In the navigation pane, click **Database** and click **Change Database**.
   b. In the Report Server Database Configuration pane, verify that **Action** is selected.
   c. On the Change Database page, select **Create a new report server database** and click **Next**.
   d. Change the server name of your database server to the database machine and database instance where SSRS will connect.
   e. Verify that the authentication type is set to **Current User – Integrated Security** and click **Test Connection**.
   f. When the test message is successful, close the Test Connection dialog box and click **Next**.
   g. On the Database pane, enter a name for the Database.
   h. Set the Report Server Mode to **Native Mode** and click **Next**.
   i. In the Credentials pane, change the Authentication Type to **Windows Credentials**, specify an account, and click **Next**.

      Specify an account that has permission to connect from the Web service on the single server to the database on the single server, and specify the password for the account.
   j. In the Summary pane, review the selections and click **Next**.
   k. In the Progress and Finish pane, resolve any errors, and click **Finish**.
3. Update the encryption keys.
   a. In the navigation pane, click **Encryption Keys**.
   b. In the Delete Encrypted Content area, click **Delete** and accept the prompt to delete all encrypted data.
   c. In the Change area, click **Change** to replace the encryption key, and click **OK**.
4. Configure the Web Service URL.

a. In the navigation pane, click **Web Service URL**.

b. Verify or configure the settings and click **Apply** to activate the Report Server Web Service URL.

Option	Action
Virtual Directory	Set to **ReportServer**.
IP Address	Set to **All Assigned (Recommended)**.
TCP Port	Set to `80` if you are not using HTTPS.
SSL Certificate	Not Selected

c. In the Results area, confirm that the virtual directory is created and that the URL is reserved.

5. Confirm the Report Manager URL.

   a. In the navigation pane, click **Report Manager URL** and click **Apply** to activate the Report Manager URL.

   b. Verify that the virtual directory was created and that the URL was reserved in the Results area.

   c. Click the default URL and verify that it opens SQL Server Reporting Services.

6. Click **Exit** to close SQL Server 2008 R2, 2012, or 2014 Reporting Services Configuration Manager.

What to do next

To authenticate users and client applications against the report server, configure Basic Authentication on the report server. See "Configure Kerberos Authentication" on page 57.

Configure Basic Authentication on the Report Server

SQL Server Reporting Services (SSRS) provides several options to authenticate users and client applications against the report server. When you install VCM in a single-tier split installation and use Basic authentication, you must allow direct access to the Reports virtual directory.

Update the `rsreportserver.config` file so that VCM can authenticate users who use the VCM Web console, and users can launch SSRS reports. To configure Basic authentication on the report server, edit the XML elements and values in the RSReportServer.config file.

Procedure

1. On the Windows machine where you installed SSRS, stop the SSRS service.

2. Navigate to the `rsreportserver.config` file.

   By default: `C:\Program Files\Microsoft SQL Server\{`*`reporting-services-instance`*`}\Reporting Services\ReportServer\rsreportserver.config`

3. Open `rsreportserver.config` in a text editor.

4. Locate the `<AuthenticationTypes>` XML code.

```
<Authentication>
   <AuthenticationTypes>
      <RSWindowsNegotiate/>
      <RSWindowsNTLM/>
   </AuthenticationTypes>
   ...
</Authentication>
```

5. Replace any existing `<AuthenticationTypes>` parameters with one `<RSWindowsBasic/>` parameter.

   ```
   <Authentication>
      <AuthenticationTypes>
         <RSWindowsBasic/>
      </AuthenticationTypes>
      ...
   </Authentication>
   ```

6. Save and close `rsreportserver.config`.
7. Start the SSRS service.

What to do next

To authenticate VCM reports with Kerberos, see "Configure Kerberos Authentication" below.

Configure Kerberos Authentication

The Kerberos network protocol uses secret-key cryptography to ensure security in your VCM applications. To authenticate VCM Reports, you must use Basic Authentication with HTTPS or Kerberos Authentication.

When you configure Kerberos Authentication in your installation, configure it on the database server.

Prerequisites

- Verify that your Windows Server 2008 R2, 2012, or 2012 R2 machine has Active Directory management tools installed. If the tools are not installed, install them. See Microsoft TechNet online. This configuration requires an Active Directory domain running at Windows Server 2003 or later domain functional level.
- If SQL Server Reporting Services is running on a different Windows machine than the VCM Collector in a single-tier installation, verify that the Application Pool account is a local administrator.

Procedure

1. Log in to your Windows Server 2008 R2, 2012, or 2012 R2 machine as a user who has domain administrator privileges.
2. Start **Active Directory Domain Services** and select **Active Directory Users and Computers**.
3. Verify whether AD accounts exist in your domain for the SQL Server service and the VCM IIS Application Pool.
4. If the accounts do not exist, create them.
   a. Set the database account to be a local administrator on the database server.
   b. Make the Application Pool account a local administrator on the VCM Collector in a single-tier installation.
5. Select the Computers container and locate the Web system.
   a. Open the properties for Web system.
   b. Click the **Delegation** tab.
   c. Select **Trust this computer for delegation to any service**.
6. Open IIS manager and set the identity of the `CMAppPool` application pool to the IIS account.

7. In Reporting Services Configuration Manager, configure the SQL Server Reporting Services service to run as the IIS Application Pool account.

8. Change SQL Server to run as the SQL Server Domain account.

   a. In Reporting Services Configuration Manager, click **Encryption Keys** and click **Delete** to delete encrypted content.

   b. In the navigation pane, click **Service Account** and enter the `app_pool_account` account for the database connection.

9. Open a command prompt to set the service principal names directory property for the Active Directory service accounts.

   a. Click **Start**, select **All Programs > Accessories**, right-click **Command Prompt**, and select **Run as administrator**.

   b. Type: **`Setspn -a MSSQLSvc/db_server_name domain\sql_server_account_name`** and press **Enter**.

   c. Type: **`Setspn -a MSSQLSvc/db_server_name:1433 domain\sql_server_account_name`** and press **Enter**.

   d. Type: **`Setspn -a MSSQLSvc/db_server_fqdn domain\sql_server_account_name`** and press **Enter**.

   e. Type: **`Setspn -a MSSQLSvc/db_server_fqdn:1433 domain\sql_server_account_name`** and press **Enter**.

10. Verify whether SSRS is running on the SQL Server and if it is not running, locate and update the Report Server configuration file named `rsreportserver.config`.

    a. Locate the `AuthenticationTypes` XML element.

    b. Remove `<RSWindowsNTLM/>` and `<RSWindowsBasic/>`.

    c. Add `<RSWindowsNegotiate/>` and `<RSWindowsKerberos/>`.

    The default location for the configuration file is `C:\Program Files\Microsoft SQL Server\{`*`reporting-services-instance`*`}\Reporting Services\ReportServer\rsreportserver.config`.

11. In SQL Server Management Studio, grant the Application Pool user access to the VCM and VCM_Unix databases, with membership in the VCM__SelectRole_General role in each database.

12. (Optional) If you did not configure the SQL Server Reporting Services service to run as the IIS Application Pool account before installing VCM, start Internet Explorer as administrator and set the report settings.

    a. Click **Start**, select **All Programs**, right-click **Internet Explorer** and select **Run as administrator**.

    b. Connect to `http://localhost/Reports/Pages/Folder.aspx`.

    c. Click **ECM Reports** and click the **ECM** data source to display the properties menu.

    d. To use integrated authentication, type the following text into the Connection string text box and click **Apply**.

    ```
    Integrated Security=SSPI;Data Source=db_server_name;Initial
    Catalog=VCM;LANGUAGE=us_english;
    ```

    e. Click the back button to return to the ECM Reports view.

13. Select **Folder Settings**, select **Security**, select the new SSRS user or group, and click **New Role Assignment**.

14. Click **Browser** to allow the VCM SSRS user or group to view folders and reports and subscribe to reports, and click **OK**.
15. In Server Manager, set the authentication mode.
    a. In the navigation pane, select **Roles > Web Server (IIS)** and click **Add Role Services** in the Role Services area.
    b. In the Select Role Services wizard, locate the Security (Installed) section, click **Windows Authentication**, and follow the prompts to install the service.
    c. In the navigation pane, select **Roles > Web Server (IIS)**.
    d. Under `server_name`, select `Sites\Default Web Site\VCM`, double-click **Authentication**, and verify that Windows Authentication is the only option enabled.
    e. Under `server_name\Sites\Default Web Site`, double-click **Authentication**, click **Windows Authentication**, verify that Windows Authentication is enabled, and click **Advanced Settings**.
    f. Verify that Kernel Mode Authentication is disabled and click **OK**.
16. In Windows Explorer, update the configuration files.
    a. Open the configuration file at `Windows\System32\inetsrv\config\applicationhost.config` and locate the `<authentication>` section.
    b. Verify that Windows authentication is enabled, and if it is not enabled, enable it.
    c. Save any changes and close the file.
17. Open a command prompt to set the property for the Active Directory service accounts for the service principal names directory.
    a. Click **Start** and select **All Programs > Accessories**.
    b. Right-click **Command Prompt** and select **Run as administrator**.
    c. Type **`Setspn -a http/web_server_name domain\Application Pool Account Name`** and press **Enter**.
    d. Type **`Setspn -a http/web_server_fqdn domain\Application Pool Account Name`** and press **Enter**.
18. Open the properties for the SQL Server and Application Pool accounts, click the **Delegation** tab, and select **Trust this user for delegation to any service**.

What to do next

Configure the VCM Collector Components before you install VCM. See "Configure the VCM Collector Components" on page 59.

Configure the VCM Collector Components

The VCM Collector contains the VCM software application and VCM services. To prepare the VCM Collector components for VCM installation, configure the required utilities.

In your single-tier installation configuration, configure the Web server and VCM Collector components on the same machine.

NOTE This procedure is required only if you did not install the complete set of Management Tools and support components earlier.

Prerequisites

- Perform the prerequisite tasks for your installation configuration. See "Single-Tier Server Installation" on page 35.
- From the VCM Collector, verify that you can access the Microsoft Download Center, Microsoft SQL Server Feature Pack to download SQLXML 4.0 SP1 in the following procedure. See the online Microsoft Download Center.
- Verify that you can access the Microsoft Download Center, Microsoft SQL Server Feature Pack to download and install the Native Client (`sqlncli.msi`) in the following procedure. See the online Microsoft Download Center. The SQL Command Line Tools in the SQL Server Feature Pack are required.
- Install .NET Framework 3.5.1 on the Windows Server 2008 R2, 2012, or 2012 R2 machines where Package Studio will be installed.

Procedure

1. Download and install SQLXML 4.0 SP1, x64 Package.
2. Download and install SQL Server Command Line Utilities, which includes the `SQLCMD` utility, x64 Package (`SqlCmdLnUtils.msi`).

   The SQL Command Line Tools in the SQL Server 2008 R2, 2012, or 2014 Feature Pack are required.
3. Download and install the SQL Server Native Client, x64 Package (`sqlncli.msi`).

   The Native Client from the SQL Server Feature Pack is required.
4. Reboot the VCM Collector.

What to do next

Review the DCOM and port requirements, and install VCM. See "Installing VCM" on page 125.

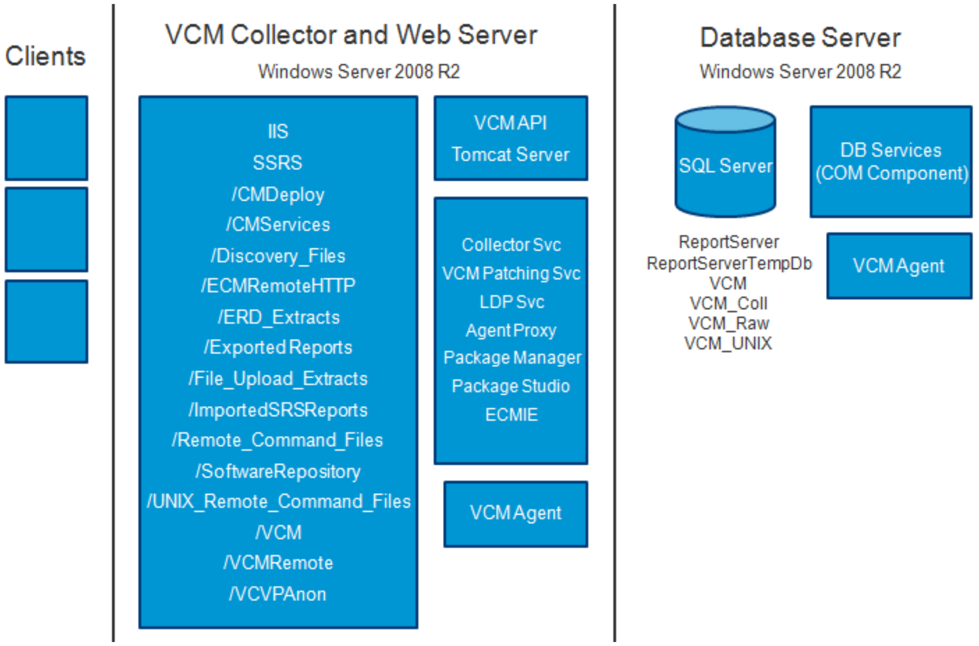
Two-Tier Split Installation 9

In a two-tier split installation, the VCM database resides on a Windows Server 2008 R2, 2012, or 2012 R2 database server machine, and the VCM Collector and Web components reside together on a separate Windows Server 2008 R2, 2012, or 2012 R2 machine.

VCM 5.8 supports 64-bit environments that include 64-bit hardware, the 64-bit Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system, and SQL Server 2008 R2, or 2012, or 2014.

CAUTION A two-tier installation configuration uses basic authentication with HTTPS by default. Be aware of the risks to exposure of sensitive data if you use basic security without HTTPS. Optionally, you can use Kerberos Authentication.

Figure 9–1. Two-Tier Split Installation



You must install SQL Server Reporting Services (SSRS) on either the database server or the combined VCM Collector and Web server.

The VMware Knowledge Base includes information about sizing your hardware environment for a two-tier installation of VCM. See http://kb.vmware.com/kb/2033894.

Configuring a Two-Tier Split Installation Environment

In a two-tier installation environment, you configure the database server first, then configure the combined VCM Collector and Web server before you install VCM. All machines are physical or virtual Windows machines.

Your VCM database server and combined Web and VCM Collector server need the following components.

Database Server Components	Combined Web and VCM Collector Server Components
VCM Database Components	VCM Web Console
VMware VCM Package Manager for Windows	VCM Collector Components
SSRS 2008 for VCM Reports (Optional if you install it on the combined Web and VCM Collector)	(Optional) SSRS 2008 for VCM Reports
(Optional) Other Tools	Import/Export Utility
	Foundation Checker
	VMware VCM Package Manager for Windows
	VMware VCM Package Studio

Prerequisites

- Perform the general system prerequisite steps. See "System Prerequisites to Install VCM" on page 21.
- Connect the database server machine to the domain.
- Connect the combined VCM Collector and Web server machine to the domain.
- Obtain the installation media for the Enterprise, Standard, or Datacenter edition of SQL Server 2008 R2, 2012, or 2014, or verify access to a file share where the installer resides.

Procedure

1. "Verify that the Installing User is an Administrator" on the facing page

   The user who installs Windows Server 2008 R2, 2012, or 2012 R2 operating system must be an Administrator and a domain account.

2. "Install and Configure Windows Server Operating System" on the facing page

   Install the Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system on each Windows machine that serves as a tier in your configuration.

3. "Configuring the VCM Database Server" on page 65

   To ensure that the installation creates the VCM databases, you must configure the VCM database server before you install VCM. In a two-tier split installation configuration, the VCM database server resides on a separate machine. The databases include VCM, VCM_Coll, VCM_Raw, and VCM_UNIX.

4. "Configure the Combined VCM Collector and Web Server" on page 74

   In a two-tier split installation configuration, the VCM Collector and the Web server components reside together on a dedicated Windows Server 2008 R2, 2012, or 2012 R2 machine, and the VCM database server resides on a separate Windows Server 2008 R2, 2012, or 2012 R2 machine.

5. "Configure the Web Components" on page 75

   The combined VCM Collector and Web server contains Web applications such as IIS and SQL Server Reporting Services (SSRS), other services, and VCM software components. Before you install VCM,

6. "Configure the VCM Collector Components" on page 88

   The combined VCM Collector and Web server contains the VCM software application and VCM services. To prepare the VCM Collector components of the combined VCM Collector and Web server for VCM installation, configure the required utilities.

What to do next

Review the DCOM and port requirements, and use VCM Installation Manager to install the VCM components. See "Installing VCM" on page 125.

Verify that the Installing User is an Administrator

The user who installs Windows Server 2008 R2, 2012, or 2012 R2 operating system must be an Administrator and a domain account.

Procedure

1. Verify that the user is an Administrator.
   a. Click **Start** and select **All Programs** > **Administrative Tools** > **Computer Management**.
   b. Expand **System Tools**, expand **Local Users and Groups**, and click **Users**.
   c. Right-click the user and click **Properties**.
   d. Click the **Member Of** tab and verify that **Administrators** is listed.
   e. If **Administrators** is not listed, add the user to the Administrators group.
   f. Click **Check Names** and click **OK**.
2. Verify that the user is a domain account.
   a. Click **Groups**.
   b. Right-click **Administrators** and click **Properties**.
   c. Verify that the Domain User is listed in the Members area.

What to do next

Prepare your Windows machine for VCM installation. See "Install and Configure Windows Server Operating System" below.

Install and Configure Windows Server Operating System

Install the Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system on each Windows machine that serves as a tier in your configuration.

Prerequisites

- Determine whether you require Windows Server 2008 R2, 2012, or 2012 R2 operating system. See "Sizing Impact on Software Edition Requirements" on page 17.
- The user who installs Windows Server 2008 R2, 2012, or 2012 R2 operating system must be an Administrator and a domain account. See "Verify that the Installing User is an Administrator" on page 63.
- Decide on a valid DNS computer name with no underscores for use when the Windows installation prompts for a machine name. If you attempt to change the machine name after a machine is identified as a Collector, problems might occur with VCM, SQL Server, and SQL Server Reporting Services.

Procedure

1. Install Microsoft Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 on your Windows machine.
2. During the installation, you can configure several options.

Option	Description
Regional and Language Options	Determines how numbers, dates, currencies, and time settings appear. ■ Language: Setting for your language. The default is English. ■ Time and currency format: Determines how numbers, dates, currencies, and time settings appear. The default is English (United States). ■ Keyboard or input method: Allows text entry for multiple languages. The default is US.
Disk Configuration	Allows you to separate the machine disk drive into partitions to store data in different partitions. You can create new disk partitions and delete existing partitions. After you configure the disk, select a partition on which to install Windows Server 2008 R2, 2012, or 2012 R2 Edition.
Product Key	When the installation prompts, enter your product key.
Licensing Modes	Windows Server 2008 R2, 2012, or 2012 R2 supports a single license that is included with the product key.
Administrator Password	The installation setup creates an account called administrator. To log in, you must create a password that complies with the criteria. The password must have the following attributes. ■ Minimum of six characters ■ Does not contain “administrator” or “admin” ■ Contains uppercase letters ■ Contains lower case letters ■ Contains numbers ■ Contains at least one non-alphanumeric character

3. Perform the initial configuration tasks to set the time zone and the computer name.

Disable the Remote Desktop Session Host

A Remote Desktop Session Host server hosts Windows-based programs for Remote Desktop Services clients.

If the Remote Desktop Session Host role service is enabled, you must disable it to avoid changes to settings for new connections, modifications of existing connections, or removal of connections.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Server Manager**.
2. In the navigation pane, expand **Roles** and click **Remote Desktop Services**.
3. In the Remote Desktop Services pane, scroll down to Role Services.
4. Click the **Remote Desktop Session Host** role service to highlight it.
5. Click **Remove Role Services**.
6. Deselect the Remote Desktop Session Host role service and follow the prompts to finish disabling the Remote Desktop Session host role.

Enable DCOM

The Distributed Component Object Model (DCOM) protocol allows application components to interact across Windows machines. DCOM must be enabled on the Windows machine to install and run VCM.

Although DCOM is enabled by default when Windows Server 2008 R2, 2012, or 2012 R2 is installed, DCOM might have been disabled by a custom installation or a lock-down script.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Component Services** to open Component Services.
2. In the Component Services navigation pane, expand **Component Services** and expand **Computers**.
3. Right-click the computer and click **Properties**.
4. Click the **Default Properties** tab.
5. Select **Enable Distributed COM on this computer** and click **OK**.

What to do next

Configure the database server. See "Configuring the VCM Database Server" below.

Configuring the VCM Database Server

To ensure that the installation creates the VCM databases, you must configure the VCM database server before you install VCM. In a two-tier split installation configuration, the VCM database server resides on a separate machine. The databases include VCM, VCM_Coll, VCM_Raw, and VCM_UNIX.

Use of a shared SQL Server is supported for VCM. However, VCM makes heavy use of SQL Server for query and transaction processing. You must ensure that you have or can add enough capacity to a shared SQL Server so that VCM and any other databases on the shared server do not experience poor performance.

The SQL Server license includes SQL Server Reporting Services (SSRS). In your two-tier split installation configuration, when you run SSRS and SQL Server on the same machine, the SQL Server database machine can take on the role of the Report Server (SSRS).

VCM 5.8 supports running SSRS on the Web server or on the database server in a split installation. Depending on the separation of services in your environment, you might want to install SSRS on the Web server machine in a split installation, because SSRS has its own Web server.

If you install SSRS on the Web server, it requires an additional SQL Server license, because you are installing SSRS on a Windows Server 2008 R2, 2012, or 2012 R2 machine that is separate from the SQL Server database services. If you run SQL Server Enterprise Edition, all SQL Server services running in guests on a single virtual machine host are covered by the Enterprise Edition license.

VCM operates with a Standard, Enterprise, or Datacenter edition of SQL Server. You must install the 64-bit SQL Server 2008 R2, or 2012, or 2014 version on your designated database server machine and verify that the settings are configured correctly for a VCM installation.

If you plan to change the communication port that SQL Server uses 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 change the port after installation, you must configure additional SSRS settings to repair the configuration.

Disable the Firewall or Add an Exception for SQL Server Port 1433

On the machine that is running SQL Server, to access SQL Server through a firewall, you must configure the firewall or add an exception for port 1433. Port 1433 is the SQL Server default instance running over TCP.

Procedure

1. To turn off the Windows domain firewall, follow these steps.
   a. Click **Start** and select **Control Panel**.
   b. Click **System and Security**.
   c. Click **Windows Firewall**.
   d. Click **Turn Windows Firewall on or off**.
   e. Under Domain network location settings, click **Turn off Windows Firewall**.
2. To add an exception for SQL port 1433, follow these steps.
   a. In Windows Firewall in the Control Panel, click **Advanced Settings** to open the Windows Firewall with Advanced Security dialog box.
   b. Click **Inbound Rules** and click **New Rule**.
   c. Click **Port** and **Next**.
   d. Click TCP, click **Specific local ports**, type **1433**, and click **Next**.
   e. Click **Allow the connection** and click **Next**.
   f. Click **Domain**, uncheck **Private**, uncheck **Public**, and click **Next**.
   g. Type a name for the rule and click **Finish**.

Install SQL Server on the Database Server

In a two-tier split installation configuration, the VCM database server resides on a separate machine. The database server contains the VCM, VCM_Coll, VCM_Raw, and VCM_UNIX databases. You must configure the VCM database server before you install VCM in a two-tier split installation configuration.

NOTE Do not run VCM in a production environment when using only an evaluation version of SQL Server. Evaluation versions are not supported for production.

Prerequisites

- Obtain the installation media for the Enterprise, Standard, or Datacenter edition of SQL Server 2008 R2, 2012, or 2014, or verify access to a file share where the installer resides.

Procedure

1. Start the SQL Server installation.
2. Perform the following actions to install SQL Server.

For SQL Server 2008 R2

Wizard Page	Action
SQL Server Installation Center	Click **New installation or add features to an existing installation**.
Setup Support Rules	Click **Install** and verify that all of the rules pass. To view the detailed system configuration check report, click the link.
Setup Support Files	Click **Install** to install the setup support files.
Setup Support Rules – for SQL Server Setup support files	Verify that all of the rules passed.
Installation Type	Select **New installation or add shared features**.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: ■ Database Engine Services Shared Features: ■ Client Tools Connectivity ■ SQL Server Books online ■ Management Tools - Basic and Management Tools - Complete
Installation Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Disk Space Requirements	Review the disk usage summary.

Wizard Page	Action
Server Configuration	Click **Use the same account for all SQL Server services** and enter the NT AUTHORITY\SYSTEM account and password. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Database Engine Configuration	Select **Windows authentication** and click **Add Current User** to add the account to the SQL Server administrators.
Error Reporting	Review the summary information.
Installation Configuration Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

For SQL Server 2012

Wizard Page	Action
SQL Server Installation Center	Click **New SQL Server stand-alone installation or add features to an existing installation**.
Setup Support Rules	Click **Install** and verify that all of the rules pass. To view the detailed system configuration check report, click the link.
Product Updates	Check for SQL Server updates.
Install Setup Files	Verify that all rules are passed.
Setup Support Rules – for SQL Server Setup support files	Verify that all of the rules passed.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Setup Role	Select **SQL Server Feature Installation**.

Wizard Page	Action
Feature Selection	Select the following features. Instance Features: - Database Engine Services Shared Features: - Client Tools Connectivity - Management Tools - Basic and Management Tools - Complete
Installation Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Disk Space Requirements	Review the disk usage summary.
Server Configuration	Browse the accounts for all SQL services and enter the NT AUTHORITY\SYSTEM account. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Database Engine Configuration	Select **Windows authentication** and click **Add Current User** to add the account to the SQL Server administrators.
Error Reporting	Review the summary information.
Installation Configuration Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

For SQL Server 2014

Wizard Page	Action
SQL Server Installation Center	Click **New SQL Server stand-alone installation or add features to an existing installation**.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Microsoft Update	Use this option to check for Microsoft updates.

Wizard Page	Action
Install Setup Files	Verify that all rules are passed.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: ■ Database Engine Services Shared Features: ■ Client Tools Connectivity ■ Management Tools - Basic and Management Tools - Complete
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Server Configuration	Browse the accounts for all SQL services and enter the NT AUTHORITY\SYSTEM account. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Database Engine Configuration	Select **Windows authentication** and click **Add Current User** to add the account to the SQL Server administrators.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

What to do next

- Reboot the database server machine.

Verify and Configure the SQL Server Properties

To ensure that SQL Server will operate with VCM, 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 Administration Guide*.

Procedure

1. Launch **SQL Server Management Studio**.
2. Right-click the SQL instance and select **Properties**.
3. Confirm the General page server property of Version as 10.50.1600.1 or some later build of version 10.50.
4. Select and confirm the Security page server properties.

   a. Select Windows Authentication mode, which is recommended.
   b. Although SQL Server and Windows Authentication mode is acceptable for VCM, select Windows Authentication mode, which is recommended.
5. Select and confirm the Database Settings page server properties.
   a. For 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 keep 20% free space available in each index page.
   b. For Recovery interval (minutes), type or select 5.
6. Click **OK** to save your changes.

What to do next

To ensure that SQL Server and VCM operate correctly together, verify that the SQL Server name matches the Windows machine name. See "Verify Matching SQL Server and Computer Names" below.

Verify Matching SQL Server and Computer Names

To ensure that SQL Server and VCM operate correctly together, you must verify that the SQL Server name matches the Windows machine name. If you recently installed SQL Server, you do not need to verify that the names match. If you obtained a machine that was renamed after the operating system and SQL Server were installed, verify and reset the SQL Server server name.

Procedure

1. Launch **SQL Server Management Studio**.
2. Click **Database Engine Query**.
3. In the **SQL Query** pane, type `SELECT @@Servername` and click **Execute**.
4. Verify that the resulting SQL Server name matches the Windows machine name.
5. If the SQL Server name does not match the Windows machine name, reset the SQL Server name.
   a. In the SQL Query pane, type the following command and replace `NewServerName` with the server name.

      ```
      exec sp_dropserver @@SERVERNAME
      exec sp_addserver 'NewServerName', 'local'
      ```
   b. Click **Execute**.
   c. To restart the SQL Server services, click **Start** and select **Programs > Microsoft SQL Server {version} > Configuration Tools > SQL Server Configuration Manager > SQL Server {version} Services**.
   d. Right-click **SQL Server** and click **Restart**.
6. Reboot the database server machine.

What to do next

- Reboot the database server machine.
- Verify that the SQL Server Agent service account has the SQL Server `sysadmin` role. See "Verify the SQL Server Agent Service Account is a sysadmin" on the next page.

Verify the SQL Server Agent Service Account is a sysadmin

The SQL Server Agent service account that runs scheduled jobs in SQL Server must be a sysadmin.

Open SQL Server Management Studio and verify that the account you will use for the SQL Server Agent service account has the `sysadmin` privilege.

Procedure

1. Launch **SQL Server Management Studio**.
2. Expand the server, expand **Security**, expand **Server Roles**.
3. Double-click `sysadmin` and view the members of the sysadmin role.
4. Verify that the account to use for the SQL Server Agent service is a member of the `sysadmin` fixed role.
5. If the account is not a member of the `sysadmin` fixed role, add this role to the account.

What to do next

Verify that the SQL Server Agent service is configured to start automatically. See "Verify that the SQL Server Agent Service Starts Automatically" below.

Verify that the SQL Server Agent Service Starts Automatically

VCM uses the SQL Server Agent service to run all scheduled jobs and SSRS reports, including dashboards. Set the service to automatically start on the VCM server where SQL Server is installed.

Procedure

1. On the VCM database server, click **Start** and select **Administrative Tools** > **Services**.
2. Right-click **SQL Server Agent**, and select **Properties**.
3. From the **Startup type** menu, select **Automatic**.
4. Click **OK**, and close the Services window.

What to do next

Select the SQL Server Agent service account See "Select the SQL Server Agent Service Account" below.

Select the SQL Server Agent Service Account

SQL Server Agent is a service that runs scheduled jobs in SQL Server and runs as a specific user account. Verify that the SQL Server Agent service account that you provided during the SQL Server installation is a SQL Server sysadmin. The SQL Server Agent runs as a user account.

Prerequisites

- Verify that the account you provide for the SQL Server Agent service has permission to log in as a service and the required additional permissions. See the online Microsoft Developer Network for more information.
- Understand the supported service account types for non-clustered and clustered servers. VCM 5.8 supports Active/Active SQL clusters. See the online Microsoft Developer Network for more information.
- Verify that the account you will use for the SQL Server Agent service account has the `sysadmin` privilege. See "Verify the SQL Server Agent Service Account is a sysadmin" on page 72.

Procedure

1. On the VCM database server machine, click **Start** and select **All Programs**.
2. Click **Microsoft SQL Server {version}** > **Configuration Tools > SQL Server Configuration Manager**.
3. Click **SQL Server Services**.
4. Right-click **SQL Server Agent (MSSQLSERVER)** and click **Properties**.
5. On the Log On tab, select a log in option and provide the account information.

Option	Description
Built-in account	In a single-tier installation, you can select the Local System account, which has unrestricted access to all system resources. In a split installation environment, do not select the built-in Local System account. This account is a member of the Windows Administrators group on the local machine.
This account	In a split installation, the SQL Server Agent must be running as a user account. Select a Windows domain account for the SQL Server Agent service account. This option provides increased security. Select this option for jobs that require application resources across a network, to forward events to other Windows application logs, or to notify administrators through email or pagers.

6. Type or select an account name that has the `sysadmin` privilege.
7. Click **OK**.

What to do next

Establish SQL Server administration rights. See "Establish SQL Server Administration Rights" below.

Establish SQL Server Administration Rights

Members of the SQL Server `sysadmin` fixed server role can perform any activity in the server. The user who installs VCM must have SQL Server `sysadmin` rights.

Procedure

1. Launch **SQL Server Management Studio**.
2. Expand the server instance, select **Security** and select **Logins**.
3. Right-click the login ID 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, select the **sysadmin** check box.
6. Click **OK** to save the settings and close the window.

What to do next

Configure the combined VCM Collector and Web server. See "Configure the Combined VCM Collector and Web Server" on the next page.

Configure the Combined VCM Collector and Web Server

In a two-tier split installation configuration, the VCM Collector and the Web server components reside together on a dedicated Windows Server 2008 R2, 2012, or 2012 R2 machine, and the VCM database server resides on a separate Windows Server 2008 R2, 2012, or 2012 R2 machine.

To configure the combined VCM Collector and Web server for a two-tier installation, verify the SQLXML version, configure IIS, install and configure SSRS, then configure the VCM Collector components.

Install the .NET Framework

To support library and language interoperability, the VCM Collector must have the required versions of the .NET Framework installed.

VCM 5.8 requires the .NET 3.5.1 Framework. If you use Package Studio, the VCM Collector must have .NET 3.5.1 installed. If you use Package Manager, the VCM Collector must have .NET 3.5.1 or .NET 4.0 installed.

Determine the installed version of the .NET Framework. If one of the .NET Framework versions is missing, install the version from the Microsoft download Web site.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Server Manager**.
2. Click **Features**.
3. Verify that .NET Framework 3.5.1 appears in the feature summary.
4. If .NET Framework 3.5.1 does not appear, under Features select **Add Features** and select **.NET 3.5.1**.

Verify the ASP.NET Client System Web Version

To support client programming, verify the ASP.NET Client System Web version to confirm that the .NET framework is installed correctly, and install it if the version is not correct.

1. Click **Start** and select **All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand **<server name>** and click **Sites**.
3. Expand **Default Web Site**, expand **aspnet_client**, and expand **system_web**.
4. Verify that the version is **2_0_50727**.

Verify the ASP Role Service

To support client programming, verify the status of the ASP Role Service to confirm that the .NET framework is installed correctly.

Procedure

1. Click **Start** and select **All Programs > 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 whether the role service is installed.
6. If the role service is not installed, click **Add Role Services** and add the ASP role service.

Verify ASP.NET Role Service

To support client programming, verify the status of the ASP.NET Role Service to confirm that the .NET framework is installed correctly.

Procedure

1. Click **Start** and select **All Programs > 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 role service is installed.
6. If the role service is not installed, click **Add Role Services** and add the ASP.NET role service.

What to do next

Configure the Web components for the combined VCM Collector and Web server. See "Configure the Web Components" below.

Configure the Web Components

The combined VCM Collector and Web server contains Web applications such as IIS and SQL Server Reporting Services (SSRS), other services, and VCM software components. Before you install VCM, you must configure the combined VCM Collector and Web server.

The Windows machine that hosts the Web components must be running Internet Information Services (IIS) 7.5. IIS is installed when you install Windows Server 2008 R2, 2012, or 2012 R2.

For a two-tier installation, the Web server components reside on the same machine as the VCM Collector.

The SQL Server license includes SQL Server Reporting Services (SSRS). In your two-tier split installation configuration, when you run SSRS and SQL Server on the same machine, the SQL Server database machine can take on the role of the Report Server (SSRS).

VCM 5.8 supports running SSRS on the Web server or on the database server in a split installation. Depending on the separation of services in your environment, you might want to install SSRS on the Web server machine in a split installation, because SSRS has its own Web server.

If you install SSRS on the Web server, it requires an additional SQL Server license, because you are installing SSRS on a Windows Server 2008 R2, 2012, or 2012 R2 machine that is separate from the SQL Server database services. If you run SQL Server Enterprise Edition, all SQL Server services running in guests on a single virtual machine host are covered by the Enterprise Edition license.

Prerequisites

- Perform the prerequisite tasks for your two-tier split installation configuration. See "Two-Tier Split Installation" on page 61.
- Place the Web server in the Internet Explorer Trusted Zone so that Internet Explorer can delegate the VCM user's credentials to the Web service for use with SQL Server. See "Place the Web Server in the Internet Explorer Trusted Zone" on page 107.
- If the domain firewall is turned on, verify that any required ports are open. If the database server is blocked from communicating with the Collector, problems can occur when you submit jobs. VCM displays an error about the SAS service, and the VCM Debug Event Log displays failures when calling `ecm_sp_collector_control`.

- Verify that .NET Framework 3.5.1 is installed on Windows Server 2008 R2, 2012, or 2012 R2 machines where Package Studio will be installed.
- Verify that you have an Internet connection to check for patch bulletin updates.
- On the Windows Server 2008 R2, 2012, or 2012 R2 Web server machine, verify that the following .NET Framework components are installed.
  - Windows Process Activation Service
  - Process Model
  - .NET Environment
  - Configuration APIs

Procedure

1. Restart the Web server machine.
2. Click **Start** and select **All Programs > Administrative Tools > Server Manager**.
3. Click **Roles** and verify that the Web Server (IIS) role appears.
4. If the Web Server (IIS) role does not appear, in the Roles Summary area, click **Add Roles** and add the Web Server (IIS) role.
5. On the Select Server Roles page, select **Web Server (IIS)** and select the Web Server components to add.

Option	Action
Common HTTP Features	Select these options: ■ Static Content ■ Default Document ■ Directory Browsing ■ HTTP Errors
Application Development	Select these options: ■ ASP .NET ■ .Net Extensibility ■ ASP ■ ISAPI Extensions ■ ISAPI Filters ■ Server Side Includes
Health and Diagnostics	Select these options: ■ HTTP Logging ■ Request Monitor
Security	Select these options: ■ Basic Authentication ■ Request Filtering

Option	Action
Performance	Select: - Static Content Compression

Configuring IIS

To ensure that the Web components are correctly configured, verify that the correct role services are enabled, the bindings are set correctly, and the default Web site is correct.

Verify the IIS 7.5 Role Services are Enabled

Verify that the correct IIS 7.5 Role Services are enabled on the combined VCM Collector and Web server .

Procedure

1. On the Collector, click **Start** and select **All Programs > Administrative Tools > Server Manager**.
2. Expand **Roles** and click **Web Server (IIS)**.
3. If the Web Server (IIS) role does not appear in the list of Roles, scroll to Role Services, click Add Role Services and add the Web Server (IIS) Role.

   When you installed IIS, the ASP Role Service, ASP.NET Role Service, and IIS ServerSideIncludes Role Service were installed.
4. In the Web Server (IIS) pane, scroll to **Role Services** and verify that the status is set to **Installed** for the following Role Services.

Role Service Category	Role Service
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 Request Monitor
Security	Basic Authentication Windows Authentication Digest Authentication URL Authorization Request Filtering IP and Domain Restrictions

Role Service Category	Role Service
Performance	Static Content Compression Dynamic Content Compression
Management Tools	IIS Management Console IIS Management Scripts and Tools Management Service

5. If any of the Role Services are not installed, click **Add Role Services**, select the check boxes of the services to install, and click **Install**.

Configure the IIS 7.5 Settings

IIS settings configure the information required for requests to communicate with a Web site. To support VCM interaction with IIS, configure the settings for the IIS 7.5 bindings on the combined VCM Collector and Web server to ensure that the settings are correct.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand **<server name>**, expand **Sites**, and click **Default Web Site**.
3. In the Actions pane, under Edit Site, click **Bindings**.
4. Click **Add** to open the Site Bindings dialog box.
   a. In the Type menu, select **http**.
   b. In the IP address menu, select **All Unassigned**.
   c. In the Port text box, type **80**.
5. In the Site Bindings dialog box, click **Close**.
6. In the Actions pane, under Manage Web Site and Browse Web Site, click **Advanced Settings**.
7. Expand **Connection Limits** and set Connection Time-out (seconds) to `3600`.
8. Click **OK**.

Verify the IIS 7.5 Default Web Site

IIS 7.5 provides a default Web site that defines the default authentication settings for applications and virtual directories. Verify that the IIS 7.5 default Web site has the correct settings.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand **<server name>**, expand **Sites**, and click **Default Web Site**.
3. In the Default Web Site Home pane, locate the IIS options.
4. Double-click **Authentication** and set the authentication.

Option	Action
Anonymous Authentication	Set to **Disabled**.

Option	Action
ASP.NET Impersonation	Set to **Disabled**.
Basic Authentication	Set to **Enabled**.
Forms Authentication	Set to **Disabled**.

Verify the ISAPI Extensions

The ISAPI Extensions role provides support for dynamic Web content development. You must verify that the role service is installed, and install it if needed.

Procedure

1. Click **Start** and select **All Programs** > **Administrative Tools** > **Server Manager**.
2. Expand **Server Manager (<server name>)** and expand **Roles**.
3. Click **Web Server (IIS)**.
4. Scroll to Role Services.
5. Locate ISAPI Extensions and verify that the role service is installed.
6. If the role service is not installed, click **Add Role Services** and add the ISAPI Extensions role service.

What to do next

Prepare SQL Server Reporting Services (SSRS) to generate VCM reports. See "Installing and Configuring SSRS on the Combined VCM Collector and Web Server" below.

Installing and Configuring SSRS on the Combined VCM Collector and Web Server

SQL Server Reporting Services (SSRS) is a server-based report generation software system that is administered using a web interface and used to deliver VCM reports.

Back Up Your SSRS Key

The `rskeymgmt` utility manages the symmetric keys used by a report server. This utility provides a way to delete encrypted content that can no longer be used if you cannot recover or apply the key.

Use the Microsoft command-line utility to back up the symmetric key to an encrypted file.

Prerequisites

- See the online Microsoft Support center for details about how to use the `rskeymgmt` utility.

Procedure

1. On the Collector file system, locate the `rskeymgmt.exe` utility at `c:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn` or the directory where you installed SQL Server.
2. To copy your SSRS key set to a removable media device and store it in a secure location, open a command line prompt and run the `rskeymgmt.exe` utility with the appropriate options.

Install SQL Server Reporting Services

In a two-tier installation configuration, for the Web server to generate VCM reports, install SQL Server Reporting Services (SSRS).

Prerequisites

- Back up your SSRS key. See "Back Up Your SSRS Key" on the previous page.
- Obtain the installation media for the Enterprise, Standard, or Datacenter edition of SQL Server 2008 R2, 2012, or 2014, or verify access to a file share where the installer resides.

Procedure

1. Start the SQL Server 2008 R2, 2012, or 2014 installation.
2. Perform the actions to install SQL Server Reporting Services.

For SSRS 2008 R2

Wizard Page	Action
SQL Server Installation Center	Click **New installation or add features to an existing installation**.
Setup Support Rules	Click **Install** and verify that all of the rules pass. To view the detailed system configuration check report, click the link.
Setup Support Files	Click **Install** to install the setup support files.
Setup Support Rules – for SQL Server Setup support files	Verify that all of the rules passed.
Installation Type	Select **New installation or add shared features**.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: - Reporting Services Shared Features: - Client Tools Connectivity - Management Tools - Basic and Management Tools - Complete
Installation Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is installed, select **Named Instance** and assign a name.

Wizard Page	Action
Disk Space Requirements	Review the disk usage summary.
Server Configuration	Click **Use the same account for all SQL Server services**. ■ If you will not install SSRS on the combined VCM Collector and Web Server machine, enter the NT AUTHORITY\SYSTEM account and password. ■ If you will install SSRS on the combined VCM Collector and Web Server, use the Network Service account instead of NT AUTHORITY\SYSTEM. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices, otherwise you must grant manual permissions.
Reporting Services Configuration	Specify the reporting services configuration mode. Select **Install, but do not configure the report server**.
Error Reporting	Review the summary information.
Installation Configuration Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Ready to Install	Review the summary of features and click **Install** to install SQL Server Reporting Services. When the installation is finished, click the link to view the log file.

For SSRS 2012

Wizard Page	Action
SQL Server Installation Center	Click **New SQL Server stand-alone installation or add features to an existing installation**.
Setup Support Rules	Click **Install** and verify that all of the rules pass. To view the detailed system configuration check report, click the link.
Product Updates	Check for SQL Server updates.
Install Setup Files	Verify that all rules are passed.
Setup Support Rules – for SQL Server Setup support files	Verify that all of the rules passed.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.

Wizard Page	Action
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: - Reporting Services Shared Features: - Client Tools Connectivity - Management Tools - Basic and Management Tools - Complete
Installation Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Disk Space Requirements	Review the disk usage summary.
Server Configuration	Browse the accounts for all SQL services and enter the NT AUTHORITY\SYSTEM account. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Reporting Services Configuration	Specify the reporting services configuration mode.
Error Reporting	Review the summary information.
Installation Configuration Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

For SSRS 2014

Wizard Page	Action
SQL Server Installation Center	Click **New SQL Server stand-alone installation or add features to an existing installation**.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.

Wizard Page	Action
Microsoft Update	Use this option to check for Microsoft updates.
Install Setup Files	Verify that all rules are passed.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: ■ Reporting Services Shared Features: ■ Client Tools Connectivity ■ Management Tools - Basic and Management Tools - Complete
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Server Configuration	Browse the accounts for all SQL services and enter the NT AUTHORITY\SYSTEM account. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Reporting Services Configuration	Specify the reporting services configuration mode.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

Configure SSRS

Configure SSRS manually in your installation configuration, because the SSRS command-line configuration tool does not perform these steps.

SSRS might require HTTPS during installation. If HTTPS is required, you manually export a self-signed certificate and import it to the VCM Collector machine's root certificate store. If you do not manually export the certificate, a manual import of a VCM report might fail. If the manual import fails, run the import from the VCM Collector machine. For more information, see the Microsoft IIS Resource Kit Tools.

Prerequisites

- Back up your SSRS key. See "Back Up Your SSRS Key" on page 79.

Procedure

1. On your combined VCM Collector and Web server, start SQL Server 2008 R2, 2012, or 2014 Reporting Services Configuration Manager.

   a. Click **Start**, select **Run**, and type `rsconfigtool.exe`.

   b. In the Reporting Services Configuration Connection dialog box, click **Connect** to connect and log in to SQL Server Reporting Services.

2. Update the SQL Server database.

   a. In the navigation pane, click **Database** and click **Change Database**.

   b. In the Report Server Database Configuration pane, verify that **Action** is selected.

   c. On the Change Database page, select **Create a new report server database** and click **Next**.

   d. Change the server name of your database server to the database machine and database instance where SSRS will connect.

   e. Verify that the authentication type is set to **Current User – Integrated Security** and click **Test Connection**.

   f. When the test message is successful, close the Test Connection dialog box and click **Next**.

   g. On the Database pane, enter a name for the Database.

   h. Set the Report Server Mode to **Native Mode** and click **Next**.

   i. In the Credentials pane, change the Authentication Type to **Windows Credentials**, specify an account, and click **Next**.

   Specify an account that has permission to connect from the combined VCM Collector and Web server to the database server, and specify the password for the account.

   j. In the Summary pane, review the selections and click **Next**.

   k. In the Progress and Finish pane, resolve any errors, and click **Finish**.

3. Update the encryption keys.

   a. In the navigation pane, click **Encryption Keys**.

   b. In the Delete Encrypted Content area, click **Delete** and accept the prompt to delete all encrypted data.

   c. In the Change area, click **Change** to replace the encryption key, and click **OK**.

4. Configure the Web Service URL.

   a. In the navigation pane, click **Web Service URL**.

   b. Verify or configure the settings and click **Apply** to activate the Report Server Web Service URL.

Option	Action
Virtual Directory	Set to **ReportServer**.
IP Address	Set to **All Assigned (Recommended)**.
TCP Port	Set to `80` if you are not using HTTPS.
SSL Certificate	Not Selected

   c. In the Results area, confirm that the virtual directory is created and that the URL is reserved.

5. Confirm the Report Manager URL.
   a. In the navigation pane, click **Report Manager URL** and click **Apply** to activate the Report Manager URL.
   b. Verify that the virtual directory was created and that the URL was reserved in the Results area.
   c. Click the default URL and verify that it opens SQL Server Reporting Services.
6. Click **Exit** to close SQL Server 2008 R2, 2012, or 2014 Reporting Services Configuration Manager.

What to do next

To authenticate users and client applications against the report server, configure Basic Authentication on the report server. See "Configure Basic Authentication on the Report Server for Multi-Tier Installations" on page 85.

Configure Basic Authentication on the Report Server for Multi-Tier Installations

SQL Server Reporting Services (SSRS) provides several options to authenticate users and client applications against the report server. When you install VCM in a two-tier split installation and use Basic authentication, you must allow direct access to the Reports virtual directory.

Update the `rsreportserver.config` file so that VCM can authenticate users who use the VCM Web console, and users can launch SSRS reports. To configure Basic authentication on the report server, edit the XML elements and values in the RSReportServer.config file.

Procedure

1. On the Windows machine where you installed SSRS, stop the SSRS service.
2. Navigate to the `rsreportserver.config` file.

   By default: `C:\Program Files\Microsoft SQL Server\{`*`reporting-services-instance`*`}`
   `\Reporting Services\ReportServer\rsreportserver.config`
3. Open `rsreportserver.config` in a text editor.
4. Locate the `<AuthenticationTypes>` XML code.

   ```
   <Authentication>
      <AuthenticationTypes>
         <RSWindowsNegotiate/>
         <RSWindowsNTLM/>
      </AuthenticationTypes>
      . . .
   </Authentication>
   ```
5. Replace any existing `<AuthenticationTypes>` parameters with one `<RSWindowsBasic/>` parameter.

   ```
   <Authentication>
      <AuthenticationTypes>
         <RSWindowsBasic/>
      </AuthenticationTypes>
      . . .
   </Authentication>
   ```
6. Save and close `rsreportserver.config`.
7. Start the SSRS service.

What to do next

To authenticate VCM reports with Kerberos, see "Configure Kerberos Authentication" below.

Configure Kerberos Authentication

The Kerberos network protocol uses secret-key cryptography to ensure security in your VCM applications. To authenticate VCM Reports, you must use Basic Authentication with HTTPS or Kerberos Authentication.

When you configure Kerberos Authentication in your two-tier split installation, configure it on the database server and the combined VCM Collector and Web server.

Prerequisites

- Verify that your Windows Server 2008 R2, 2012, or 2012 R2 machine has Active Directory management tools installed. If the tools are not installed, install them. See Microsoft TechNet online. This configuration requires an Active Directory domain running at Windows Server 2003 or later domain functional level.
- If SQL Server Reporting Services is running on a different Windows machine than the VCM Collector in a two-tier installation, verify that the Application Pool account is a local administrator.

Procedure

1. Log in to your Windows Server 2008 R2, 2012, or 2012 R2 machine as a user who has domain administrator privileges.
2. Start **Active Directory Domain Services** and select **Active Directory Users and Computers**.
3. Verify whether AD accounts exist in your domain for the SQL Server service and the VCM IIS Application Pool.
4. If the accounts do not exist, create them.
   a. Set the database account to be a local administrator on the database server.
   b. Make the Application Pool account a local administrator on the VCM Collector in a two-tier installation.
5. Select the Computers container and locate the Web system.
   a. Open the properties for Web system.
   b. Click the **Delegation** tab.
   c. Select **Trust this computer for delegation to any service**.
6. Open IIS manager and set the identity of the `CMAppPool` application pool to the IIS account.
7. In Reporting Services Configuration Manager, configure the SQL Server Reporting Services service to run as the IIS Application Pool account.
8. Change SQL Server to run as the SQL Server Domain account.
   a. In Reporting Services Configuration Manager, click **Encryption Keys** and click **Delete** to delete encrypted content.
   b. In the navigation pane, click **Service Account** and enter the `app_pool_account` account for the database connection.
9. Open a command prompt to set the service principal names directory property for the Active Directory service accounts.

a. Click **Start**, select **All Programs > Accessories**, right-click **Command Prompt**, and select **Run as administrator**.

b. Type: `Setspn -a MSSQLSvc/db_server_name domain\sql_server_account_name` and press **Enter**.

c. Type: `Setspn -a MSSQLSvc/db_server_name:1433 domain\sql_server_account_name` and press **Enter**.

d. Type: `Setspn -a MSSQLSvc/db_server_fqdn domain\sql_server_account_name` and press **Enter**.

e. Type: `Setspn -a MSSQLSvc/db_server_fqdn:1433 domain\sql_server_account_name` and press **Enter**.

10. Verify whether SSRS is running on the SQL Server and if it is not running, locate and update the Report Server configuration file named `rsreportserver.config`.

    a. Locate the `AuthenticationTypes` XML element.

    b. Remove `<RSWindowsNTLM/>` and `<RSWindowsBasic/>`.

    c. Add `<RSWindowsNegotiate/>` and `<RSWindowsKerberos/>`.

    The default location for the configuration file is `C:\Program Files\Microsoft SQL Server\{`*`reporting-services-instance`*`}\Reporting Services\ReportServer\rsreportserver.config`.

11. In SQL Server Management Studio, grant the Application Pool user access to the VCM and VCM_Unix databases, with membership in the VCM__SelectRole_General role in each database.

12. (Optional) If you did not configure the SQL Server Reporting Services service to run as the IIS Application Pool account before installing VCM, start Internet Explorer as administrator and set the report settings.

    a. Click **Start**, select **All Programs**, right-click **Internet Explorer** and select **Run as administrator**.

    b. Connect to `http://localhost/Reports/Pages/Folder.aspx`.

    c. Click **ECM Reports** and click the **ECM** data source to display the properties menu.

    d. To use integrated authentication, type the following text into the Connection string text box and click **Apply**.

    ```
    Integrated Security=SSPI;Data Source=db_server_name;Initial
    Catalog=VCM;LANGUAGE=us_english;
    ```

    e. Click the back button to return to the ECM Reports view.

13. Select **Folder Settings**, select **Security**, select the new SSRS user or group, and click **New Role Assignment**.

14. Click **Browser** to allow the VCM SSRS user or group to view folders and reports and subscribe to reports, and click **OK**.

15. In Server Manager, set the authentication mode.

    a. In the navigation pane, select **Roles > Web Server (IIS)** and click **Add Role Services** in the Role Services area.

    b. In the Select Role Services wizard, locate the Security (Installed) section, click **Windows Authentication**, and follow the prompts to install the service.

    c. In the navigation pane, select **Roles > Web Server (IIS)**.

    d. Under `server_name`, select `Sites\Default Web Site\VCM`, double-click **Authentication**, and verify that Windows Authentication is the only option enabled.

e. Under `server_name\Sites\Default Web Site`, double-click **Authentication**, click **Windows Authentication**, verify that Windows Authentication is enabled, and click **Advanced Settings**.

f. Verify that Kernel Mode Authentication is disabled and click **OK**.

16. In Windows Explorer, update the configuration files.

    a. Open the configuration file at `Windows\System32\inetsrv\config\applicationhost.config` and locate the `<authentication>` section.

    b. Verify that Windows authentication is enabled, and if it is not enabled, enable it.

    c. Save any changes and close the file.

17. Open a command prompt to set the property for the Active Directory service accounts for the service principal names directory.

    a. Click **Start** and select **All Programs** > **Accessories**.

    b. Right-click **Command Prompt** and select **Run as administrator**.

    c. Type **`Setspn -a http/web_server_name domain\Application Pool Account Name`** and press **Enter**.

    d. Type **`Setspn -a http/web_server_fqdn domain\Application Pool Account Name`** and press **Enter**.

18. Open the properties for the SQL Server and Application Pool accounts, click the **Delegation** tab, and select **Trust this user for delegation to any service**.

What to do next

Configure the VCM Collector components of the combined VCM Collector and Web server before you install VCM. See "Configure the VCM Collector Components" on page 88.

Configure the VCM Collector Components

The combined VCM Collector and Web server contains the VCM software application and VCM services. To prepare the VCM Collector components of the combined VCM Collector and Web server for VCM installation, configure the required utilities.

In your two-tier split installation configuration, configure the Web server and VCM Collector components on the same machine.

NOTE This procedure is required only if you did not install the complete set of Management Tools and support components earlier.

Prerequisites

- Perform the prerequisite tasks for your two-tier split installation configuration. See "Two-Tier Split Installation" on page 61.

- From the VCM Collector, verify that you can access the Microsoft Download Center, Microsoft SQL Server Feature Pack to download SQLXML 4.0 SP1 in the following procedure. See the online Microsoft Download Center.

- Verify that you can access the Microsoft Download Center, Microsoft SQL Server Feature Pack to download and install the Native Client (`sqlncli.msi`) in the following procedure. See the online Microsoft Download Center. The SQL Command Line Tools in the SQL Server Feature Pack are required on the combined VCM Collector and Web server.

- Install .NET Framework 3.5.1 on the Windows Server 2008 R2, 2012, or 2012 R2 machines where Package Studio will be installed.

Procedure

1. Download and install SQLXML 4.0 SP1, x64 Package.
2. Download and install SQL Server Command Line Utilities, which includes the `SQLCMD` utility, x64 Package (`SqlCmdLnUtils.msi`).

   The SQL Command Line Tools in the SQL Server 2008 R2, 2012, or 2014 Feature Pack are required on the combined VCM Collector and Web server.
3. Download and install the SQL Server Native Client, x64 Package (`sqlncli.msi`).

   The Native Client from the SQL Server Feature Pack is required on the combined VCM Collector and Web server.
4. Reboot the combined VCM Collector and Web server.

What to do next

Review the DCOM and port requirements, and use VCM Installation Manager to install the VCM components. See "Installing VCM" on page 125.

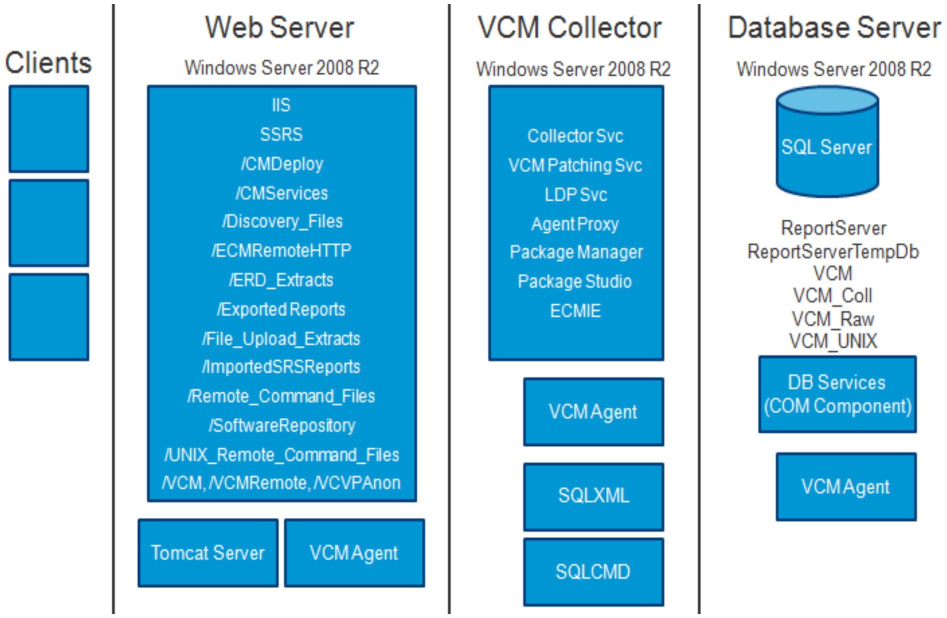
Three-Tier Split Installation 10

In a three-tier split installation, the VCM databases, the Web applications, and the VCM Collector components reside on three different Windows Server 2008 R2, 2012, or 2012 R2 machines.

CAUTION A three-tier installation configuration uses basic authentication with HTTPS by default. Be aware of the risks to exposure of sensitive data if you use basic security without HTTPS. Optionally, you can use Kerberos Authentication.

VCM 5.8 supports 64-bit environments that include 64-bit hardware, the 64-bit Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system, and SQL Server 2008 R2, or 2012, or 2014.

Figure 10–1. Three-Tier Split Installation



VCM 5.8 supports running SSRS on the Web server or on the database server in a split installation. Depending on the separation of services in your environment, you might want to install SSRS on the Web server machine in a split installation, because SSRS has its own Web server.

The VMware Knowledge Base includes information about sizing your hardware environment for a three-tier installation of VCM. See http://kb.vmware.com/kb/2033894.

Configuring a Three-Tier Split Installation Environment

In a three-tier installation environment, you configure the database server first, configure the Web server next, then configure the VCM Collector. All machines are physical or virtual Windows machines.

Prerequisites

- Perform the general system prerequisite tasks. See "System Prerequisites to Install VCM" on page 21.
- Connect the database server machine, Web server machine, and VCM Collector machine to the domain.
- Obtain the installation media for the Enterprise, Standard, or Datacenter edition of SQL Server 2008 R2, 2012, or 2014, or verify access to a file share where the installer resides.

Procedure

1. "Verify that the Installing User is an Administrator" below

   The user who installs Windows Server 2008 R2, 2012, or 2012 R2 operating system must be an Administrator and a domain account.

2. "Install and Configure Windows Server Operating System" on the facing page

   Install the Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system on each Windows machine that serves as a tier in your configuration.

3. "Configure the VCM Database Server" on page 95

   To ensure that the installation creates the VCM databases, you must configure the VCM database server before you install VCM. In a three-tier split installation configuration, the VCM database server resides on a separate machine. The databases include VCM, VCM_Coll, VCM_Raw, and VCM_UNIX.

4. "Configure the Web Server" on page 103

   The Web server contains Web applications such as IIS and SQL Server Reporting Services (SSRS), other services, and VCM software components. Before you install VCM, you must configure the Web server.

5. "Configure the VCM Collector" on page 119

   The VCM Collector contains the VCM software application and VCM services. To prepare the VCM Collector for VCM installation, configure the required utilities.

What to do next

Review the DCOM and port requirements, and use VCM Installation Manager to install the VCM components. See "Installing VCM" on page 125.

Verify that the Installing User is an Administrator

The user who installs Windows Server 2008 R2, 2012, or 2012 R2 operating system must be an Administrator and a domain account.

Procedure

1. Verify that the user is an Administrator.
   a. Click **Start** and select **All Programs** > **Administrative Tools** > **Computer Management**.
   b. Expand **System Tools**, expand **Local Users and Groups**, and click **Users**.
   c. Right-click the user and click **Properties**.
   d. Click the **Member Of** tab and verify that **Administrators** is listed.
   e. If **Administrators** is not listed, add the user to the Administrators group.
   f. Click **Check Names** and click **OK**.
2. Verify that the user is a domain account.
   a. Click **Groups**.
   b. Right-click **Administrators** and click **Properties**.
   c. Verify that the Domain User is listed in the Members area.

What to do next

Prepare your Windows machine for VCM installation. See "Install and Configure Windows Server Operating System" below.

Install and Configure Windows Server Operating System

Install the Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system on each Windows machine that serves as a tier in your configuration.

Prerequisites

- Determine whether you require Windows Server 2008 R2, 2012, or 2012 R2 operating system. See "Sizing Impact on Software Edition Requirements" on page 17.
- The user who installs Windows Server 2008 R2, 2012, or 2012 R2 operating system must be an Administrator and a domain account. See "Verify that the Installing User is an Administrator" on page 92.
- Decide on a valid DNS computer name with no underscores for use when the Windows installation prompts for a machine name. If you attempt to change the machine name after a machine is identified as a Collector, problems might occur with VCM, SQL Server, and SQL Server Reporting Services.

Procedure

1. Install Microsoft Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 on your Windows machine.
2. During the installation, you can configure several options.

Option	Description
Regional and Language Options	Determines how numbers, dates, currencies, and time settings appear. ■ Language: Setting for your language. The default is English. ■ Time and currency format: Determines how numbers, dates, currencies, and time settings appear. The default is English (United States). ■ Keyboard or input method: Allows text entry for multiple languages. The default is US.
Disk Configuration	Allows you to separate the machine disk drive into partitions to store data in different partitions. You can create new disk partitions and delete existing partitions. After you configure the disk, select a partition on which to install Windows Server 2008 R2, 2012, or 2012 R2 Edition.
Product Key	When the installation prompts, enter your product key.
Licensing Modes	Windows Server 2008 R2, 2012, or 2012 R2 supports a single license that is included with the product key.
Administrator Password	The installation setup creates an account called administrator. To log in, you must create a password that complies with the criteria. The password must have the following attributes. ■ Minimum of six characters ■ Does not contain “administrator” or “admin” ■ Contains uppercase letters ■ Contains lower case letters ■ Contains numbers ■ Contains at least one non-alphanumeric character

3. Perform the initial configuration tasks to set the time zone and the computer name.

Disable the Remote Desktop Session Host

A Remote Desktop Session Host server hosts Windows-based programs for Remote Desktop Services clients.

If the Remote Desktop Session Host role service is enabled, you must disable it to avoid changes to settings for new connections, modifications of existing connections, or removal of connections.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Server Manager**.
2. In the navigation pane, expand **Roles** and click **Remote Desktop Services**.
3. In the Remote Desktop Services pane, scroll down to Role Services.
4. Click the **Remote Desktop Session Host** role service to highlight it.
5. Click **Remove Role Services**.
6. Deselect the Remote Desktop Session Host role service and follow the prompts to finish disabling the Remote Desktop Session host role.

Enable DCOM

The Distributed Component Object Model (DCOM) protocol allows application components to interact across Windows machines. DCOM must be enabled on the Windows machine to install and run VCM.

Although DCOM is enabled by default when Windows Server 2008 R2, 2012, or 2012 R2 is installed, DCOM might have been disabled by a custom installation or a lock-down script.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Component Services** to open Component Services.
2. In the Component Services navigation pane, expand **Component Services** and expand **Computers**.
3. Right-click the computer and click **Properties**.
4. Click the **Default Properties** tab.
5. Select **Enable Distributed COM on this computer** and click **OK**.

What to do next

Configure the database server. See "Configure the VCM Database Server" below.

Configure the VCM Database Server

To ensure that the installation creates the VCM databases, you must configure the VCM database server before you install VCM. In a three-tier split installation configuration, the VCM database server resides on a separate machine. The databases include VCM, VCM_Coll, VCM_Raw, and VCM_UNIX.

Use of a shared SQL Server is supported for VCM. However, VCM makes heavy use of SQL Server for query and transaction processing. You must ensure that you have or can add enough capacity to a shared SQL Server so that VCM and any other databases on the shared server do not experience poor performance.

The SQL Server license includes SQL Server Reporting Services (SSRS). In your three-tier split installation configuration, when you run SSRS and SQL Server on the same machine, the SQL Server database machine can take on the role of the Report Server (SSRS).

VCM 5.8 supports running SSRS on the Web server or on the database server in a split installation. Depending on the separation of services in your environment, you might want to install SSRS on the Web server machine in a split installation, because SSRS has its own Web server.

If you install SSRS on the Web server, it requires an additional SQL Server license, because you are installing SSRS on a Windows Server 2008 R2, 2012, or 2012 R2 machine that is separate from the SQL Server database services. If you run SQL Server Enterprise Edition, all SQL Server services running in guests on a single virtual machine host are covered by the Enterprise Edition license.

VCM operates with a Standard, Enterprise, or Datacenter edition of SQL Server. You must install the 64-bit SQL Server 2008 R2, or 2012, or 2014 version on your designated database server machine and verify that the settings are configured correctly for a VCM installation.

If you plan to change the communication port that SQL Server uses 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 change the port after installation, you must configure additional SSRS settings to repair the configuration.

Install SQL Server on the Database Server

In a three-tier split installation configuration, the VCM database server resides on a separate machine. The database server contains the VCM, VCM_Coll, VCM_Raw, and VCM_UNIX databases. You must configure the VCM database server before you install VCM in a three-tier split installation configuration.

NOTE Do not run VCM in a production environment when using only an evaluation version of SQL Server. Evaluation versions are not supported for production.

Prerequisites

- Obtain the installation media for the Enterprise, Standard, or Datacenter edition of SQL Server 2008 R2, 2012, or 2014, or verify access to a file share where the installer resides.

Procedure

1. Start the SQL Server installation.
2. Perform the following actions to install SQL Server.

For SQL Server 2008 R2

Wizard Page	Action
SQL Server Installation Center	Click **New installation or add features to an existing installation**.
Setup Support Rules	Click **Install** and verify that all of the rules pass. To view the detailed system configuration check report, click the link.
Setup Support Files	Click **Install** to install the setup support files.
Setup Support Rules – for SQL Server Setup support files	Verify that all of the rules passed.
Installation Type	Select **New installation or add shared features**.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Setup Role	Select **SQL Server Feature Installation**.

Wizard Page	Action
Feature Selection	Select the following features. Instance Features: ■ Database Engine Services Shared Features: ■ Client Tools Connectivity ■ SQL Server Books online ■ Management Tools - Basic and Management Tools - Complete
Installation Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Disk Space Requirements	Review the disk usage summary.
Server Configuration	Click **Use the same account for all SQL Server services** and enter the NT AUTHORITY\SYSTEM account and password. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Database Engine Configuration	Select **Windows authentication** and click **Add Current User** to add the account to the SQL Server administrators.
Error Reporting	Review the summary information.
Installation Configuration Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

For SQL Server 2012

Wizard Page	Action
SQL Server Installation Center	Click **New SQL Server stand-alone installation or add features to an existing installation**.

Wizard Page	Action
Setup Support Rules	Click **Install** and verify that all of the rules pass. To view the detailed system configuration check report, click the link.
Product Updates	Check for SQL Server updates.
Install Setup Files	Verify that all rules are passed.
Setup Support Rules – for SQL Server Setup support files	Verify that all of the rules passed.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: ▪ Database Engine Services Shared Features: ▪ Client Tools Connectivity ▪ Management Tools - Basic and Management Tools - Complete
Installation Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Disk Space Requirements	Review the disk usage summary.
Server Configuration	Browse the accounts for all SQL services and enter the NT AUTHORITY\SYSTEM account. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Database Engine Configuration	Select **Windows authentication** and click **Add Current User** to add the account to the SQL Server administrators.

Wizard Page	Action
Error Reporting	Review the summary information.
Installation Configuration Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

For SQL Server 2014

Wizard Page	Action
SQL Server Installation Center	Click **New SQL Server stand-alone installation or add features to an existing installation**.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Microsoft Update	Use this option to check for Microsoft updates.
Install Setup Files	Verify that all rules are passed.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: ■ Database Engine Services Shared Features: ■ Client Tools Connectivity ■ Management Tools - Basic and Management Tools - Complete
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Server Configuration	Browse the accounts for all SQL services and enter the NT AUTHORITY\SYSTEM account. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Database Engine Configuration	Select **Windows authentication** and click **Add Current User** to add the account to the SQL Server administrators.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

What to do next

- Reboot the database server machine.

Verify and Configure the SQL Server Properties

To ensure that SQL Server will operate with VCM, 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 Administration Guide*.

Procedure

1. Launch **SQL Server Management Studio**.
2. Right-click the SQL instance and select **Properties**.
3. Confirm the General page server property of Version as 10.50.1600.1 or some later build of version 10.50.
4. Select and confirm the Security page server properties.
   a. Select Windows Authentication mode, which is recommended.
   b. Although SQL Server and Windows Authentication mode is acceptable for VCM, select Windows Authentication mode, which is recommended.
5. Select and confirm the Database Settings page server properties.
   a. For 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 keep 20% free space available in each index page.
   b. For Recovery interval (minutes), type or select 5.
6. Click **OK** to save your changes.

What to do next

- Restart the database machine.
- To ensure that SQL Server and VCM operate correctly together, verify that the SQL Server name matches the Windows machine name. See "Verify Matching SQL Server and Computer Names" below.

Verify Matching SQL Server and Computer Names

To ensure that SQL Server and VCM operate correctly together, you must verify that the SQL Server name matches the Windows machine name. If you recently installed SQL Server, you do not need to verify that the names match. If you obtained a machine that was renamed after the operating system and SQL Server were installed, verify and reset the SQL Server server name.

Procedure

1. Launch **SQL Server Management Studio**.
2. Click **Database Engine Query**.
3. In the **SQL Query** pane, type `SELECT @@Servername` and click **Execute**.
4. Verify that the resulting SQL Server name matches the Windows machine name.
5. If the SQL Server name does not match the Windows machine name, reset the SQL Server name.

a. In the SQL Query pane, type the following command and replace `NewServerName` with the server name.

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

b. Click **Execute**.

c. To restart the SQL Server services, click **Start** and select **Programs > Microsoft SQL Server {version} > Configuration Tools > SQL Server Configuration Manager > SQL Server {version} Services**.

d. Right-click **SQL Server** and click **Restart**.

6. Reboot the database server machine.

What to do next

- Reboot the database server machine.
- Verify that the SQL Server Agent service account has the SQL Server `sysadmin` role. See "Verify the SQL Server Agent Service Account is a sysadmin" below.

Verify the SQL Server Agent Service Account is a sysadmin

The SQL Server Agent service account that runs scheduled jobs in SQL Server must be a sysadmin.

Open SQL Server Management Studio and verify that the account you will use for the SQL Server Agent service account has the `sysadmin` privilege.

Procedure

1. Launch **SQL Server Management Studio**.
2. Expand the server, expand **Security**, expand **Server Roles**.
3. Double-click `sysadmin` and view the members of the sysadmin role.
4. Verify that the account to use for the SQL Server Agent service is a member of the `sysadmin` fixed role.
5. If the account is not a member of the `sysadmin` fixed role, add this role to the account.

What to do next

Verify that the SQL Server Agent service is configured to start automatically. See "Verify that the SQL Server Agent Service Starts Automatically" below.

Verify that the SQL Server Agent Service Starts Automatically

VCM uses the SQL Server Agent service to run all scheduled jobs and SSRS reports, including dashboards. Set the service to automatically start on the VCM server where SQL Server is installed.

Procedure

1. On the VCM database server, click **Start** and select **Administrative Tools** > **Services**.
2. Right-click **SQL Server Agent**, and select **Properties**.
3. From the **Startup type** menu, select **Automatic**.
4. Click **OK**, and close the Services window.

What to do next

Select the SQL Server Agent service account See "Select the SQL Server Agent Service Account" below.

Select the SQL Server Agent Service Account

SQL Server Agent is a service that runs scheduled jobs in SQL Server and runs as a specific user account. Verify that the SQL Server Agent service account that you provided during the SQL Server installation is a SQL Server sysadmin. The SQL Server Agent runs as a user account.

Prerequisites

- Verify that the account you provide for the SQL Server Agent service has permission to log in as a service and the required additional permissions. See the online Microsoft Developer Network for more information.
- Understand the supported service account types for non-clustered and clustered servers. VCM 5.8 supports Active/Active SQL clusters. See the online Microsoft Developer Network for more information.
- Verify that the account you will use for the SQL Server Agent service account has the `sysadmin` privilege. See "Verify the SQL Server Agent Service Account is a sysadmin" on page 101.

Procedure

1. On the VCM database server machine, click **Start** and select **All Programs**.
2. Click **Microsoft SQL Server {version}** > **Configuration Tools > SQL Server Configuration Manager**.
3. Click **SQL Server Services**.
4. Right-click **SQL Server Agent (MSSQLSERVER)** and click **Properties**.
5. On the Log On tab, select a log in option and provide the account information.

Option	Description
Built-in account	In a single-tier installation, you can select the Local System account, which has unrestricted access to all system resources. In a split installation environment, do not select the built-in Local System account. This account is a member of the Windows Administrators group on the local machine.
This account	In a split installation, the SQL Server Agent must be running as a user account. Select a Windows domain account for the SQL Server Agent service account. This option provides increased security. Select this option for jobs that require application resources across a network, to forward events to other Windows application logs, or to notify administrators through email or pagers.

6. Type or select an account name that has the `sysadmin` privilege.
7. Click **OK**.

What to do next

Establish SQL Server administration rights. See "Establish SQL Server Administration Rights" on the facing page.

Establish SQL Server Administration Rights

Members of the SQL Server `sysadmin` fixed server role can perform any activity in the server. The user who installs VCM must have SQL Server `sysadmin` rights.

Procedure

1. Launch **SQL Server Management Studio**.
2. Expand the server instance, select **Security** and select **Logins**.
3. Right-click the login ID 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, select the **sysadmin** check box.
6. Click **OK** to save the settings and close the window.

What to do next

Configure the separate Web server. See "Configure the Web Server" below.

Configure the Web Server

The Web server contains Web applications such as IIS and SQL Server Reporting Services (SSRS), other services, and VCM software components. Before you install VCM, you must configure the Web server.

The Windows machine that hosts the Web components must be running Internet Information Services (IIS) 7.5. IIS is installed when you install Windows Server 2008 R2, 2012, or 2012 R2.

The SQL Server license includes SQL Server Reporting Services (SSRS). In your three-tier split installation configuration, when you run SSRS and SQL Server on the same machine, the SQL Server database machine can take on the role of the Report Server (SSRS).

VCM 5.8 supports running SSRS on the Web server or on the database server in a split installation. Depending on the separation of services in your environment, you might want to install SSRS on the Web server machine in a split installation, because SSRS has its own Web server.

If you install SSRS on the Web server, it requires an additional SQL Server license, because you are installing SSRS on a Windows Server 2008 R2, 2012, or 2012 R2 machine that is separate from the SQL Server database services. If you run SQL Server Enterprise Edition, all SQL Server services running in guests on a single virtual machine host are covered by the Enterprise Edition license.

Prerequisites

- Perform the prerequisite tasks for your three-tier split installation configuration. See "Three-Tier Split Installation" on page 91.
- Place the Web server in the Internet Explorer Trusted Zone so that Internet Explorer can delegate the VCM user's credentials to the Web service for use with SQL Server. See "Place the Web Server in the Internet Explorer Trusted Zone" on page 107.
- If the domain firewall is turned on, verify that any required ports are open. If the database server is blocked from communicating with the Collector, problems can occur when you submit jobs. VCM displays an error about the SAS service, and the VCM Debug Event Log displays failures when calling `ecm_sp_collector_control`.
- Verify that .NET Framework 3.5.1 is installed on Windows Server 2008 R2, 2012, or 2012 R2 machines where Package Studio will be installed.
- Verify that you have an Internet connection to check for patch bulletin updates.

- On the Windows Server 2008 R2, 2012, or 2012 R2 Web server machine, verify that the following .NET Framework components are installed.
  - Windows Process Activation Service
  - Process Model
  - .NET Environment
  - Configuration APIs

Procedure

1. Restart the Web server machine.
2. Click **Start** and select **All Programs > Administrative Tools > Server Manager**.
3. Click **Roles** and verify that the Web Server (IIS) role appears.
4. If the Web Server (IIS) role does not appear, in the Roles Summary area, click **Add Roles** and add the Web Server (IIS) role.
5. On the Select Server Roles page, select **Web Server (IIS)** and select the Web Server components to add.

Option	Action
Common HTTP Features	Select these options: ■ Static Content ■ Default Document ■ Directory Browsing ■ HTTP Errors
Application Development	Select these options: ■ ASP .NET ■ .Net Extensibility ■ ASP ■ ISAPI Extensions ■ ISAPI Filters ■ Server Side Includes
Health and Diagnostics	Select these options: ■ HTTP Logging ■ Request Monitor
Security	Select these options: ■ Basic Authentication ■ Request Filtering
Performance	Select: ■ Static Content Compression

Configuring IIS

To ensure that the Web components are correctly configured, verify that the correct role services are enabled, the bindings are set correctly, and the default Web site is correct.

Verify the IIS 7.5 Role Services are Enabled

Verify that the correct IIS 7.5 Role Services are enabled on the Web server.

Procedure

1. On the Collector, click **Start** and select **All Programs > Administrative Tools > Server Manager**.
2. Expand **Roles** and click **Web Server (IIS)**.
3. If the Web Server (IIS) role does not appear in the list of Roles, scroll to Role Services, click Add Role Services and add the Web Server (IIS) Role.

   When you installed IIS, the ASP Role Service, ASP.NET Role Service, and IIS ServerSideIncludes Role Service were installed.
4. In the Web Server (IIS) pane, scroll to **Role Services** and verify that the status is set to **Installed** for the following Role Services.

Role Service Category	Role Service
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	Logging Tools Request Monitor Tracing
Security	Basic Authentication Windows Authentication Digest Authentication URL Authorization Request Filtering IP and Domain Restrictions
Performance	Static Content Compression Dynamic Content Compression

Role Service Category	Role Service
Management Tools	IIS Management Console IIS Management Scripts and Tools Management Service

5. If any of the Role Services are not installed, click **Add Role Services**, select the check boxes of the services to install, and click **Install**.

Configure the IIS 7.5 Settings

IIS settings configure the information required for requests to communicate with a Web site. To support VCM interaction with IIS, configure the settings for the IIS 7.5 bindings on the Web server to ensure that the settings are correct.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand **<server name>**, expand **Sites**, and click **Default Web Site**.
3. In the Actions pane, under Edit Site, click **Bindings**.
4. Click **Add** to open the Site Bindings dialog box.
   a. In the Type menu, select **http**.
   b. In the IP address menu, select **All Unassigned**.
   c. In the Port text box, type **80**.
5. In the Site Bindings dialog box, click **Close**.
6. In the Actions pane, under Manage Web Site and Browse Web Site, click **Advanced Settings**.
7. Expand **Connection Limits** and set Connection Time-out (seconds) to `3600`.
8. Click **OK**.

Verify the IIS 7.5 Default Web Site

IIS 7.5 provides a default Web site that defines the default authentication settings for applications and virtual directories. Verify that the IIS 7.5 default Web site has the correct settings.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand **<server name>**, expand **Sites**, and click **Default Web Site**.
3. In the Default Web Site Home pane, locate the IIS options.
4. Double-click **Authentication** and set the authentication.

Option	Action
Anonymous Authentication	Set to **Disabled**.
ASP.NET Impersonation	Set to **Disabled**.
Basic Authentication	Set to **Enabled**.
Forms Authentication	Set to **Disabled**.

Verify the ISAPI Extensions

The ISAPI Extensions role provides support for dynamic Web content development. You must verify that the role service is installed, and install it if needed.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Server Manager**.
2. Expand **Server Manager (<server name>)** and expand **Roles**.
3. Click **Web Server (IIS)**.
4. Scroll to Role Services.
5. Locate ISAPI Extensions and verify that the role service is installed.
6. If the role service is not installed, click **Add Role Services** and add the ISAPI Extensions role service.

What to do next

Place the Web server in the Internet Explorer trusted zone so that Internet Explorer can delegate the VCM user's credentials to the Web service for use with SQL Server. See "Place the Web Server in the Internet Explorer Trusted Zone" below.

Place the Web Server in the Internet Explorer Trusted Zone

To ensure that Internet Explorer can delegate the VCM user's credentials to the Web service for use with SQL Server, you must place the VCM Web server in the Internet Explorer Trusted Zone.

When the VCM Web server is in the trusted zone, users can disable navigation into the trusted zone from less privileged zones, which reduces the potential of cross-site scripting. When the Web server is not in a trusted zone, the browser cannot authenticate the Web server.

Procedure

1. Open Internet Explorer.
2. Click **Tools** and select **Internet Options**.
3. Click the **Security** tab.
4. In the Select a zone to view or change security settings area, click **Local intranet**.
5. Click **Sites**.
6. In the Local intranet dialog box, click **Advanced**.
7. In the Add this website to the zone area, type the host name and click **Add**.
8. Click **Close**.
9. Click **OK** and click **OK** again.

What to do next

Grant the Collector service access to the patch download folder to download patches during Windows patch deployment. See "Access to Patch Download Folder for Windows Patch Deployment" below.

Access to Patch Download Folder for Windows Patch Deployment

Grant the Collector service access to the patch download folder to download patches during Windows patch deployment.

During Windows patch deployment in a three-tier split installation, you must download the Windows patches immediately. If you download the patches during the patch deployment, the patches are not downloaded to the Web server. The patch job history shows a status of `Completed - Error` and indicates that the job could not download all patch files to `the C:\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\SUM Downloads` folder.

In a three-tier split installation, use one of the following methods to ensure that VCM downloads the Windows patches to the `SUM Downloads` folder.

- When you run a VCM patch deployment, select the option to download the patches immediately instead of downloading them during patch deployment runtime.
- Give write permission to the Collector service account on the `L1033\files\SUM Downloads` folder.
- (Optional) Verify that the Collector service account is a local admin on the Web server.

Procedure

1. In VCM on the Web server in a three-tier installation, select **Patching**.
2. Click **Check for Update** and download all Windows patch bulletins.
3. Select **Windows** and click **Assessment Templates**.
4. Select your template or create an assessment template and click **Assess**.
5. After the assessment is finished, under Assessment Templates, click your assessment template to display the list of patches to deploy to the managed machines.
6. Select the patch to deploy and click **Deploy**.
7. In the Deploy Patches wizard, on the Patch Status page, click **Download now** to download the patches immediately from the Internet, and finish the wizard.
8. (Optional) Assign write permission to the Collector service named `scm.service` to access the `SUM Downloads` folder.

   a. On the Web server, navigate to `C:\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files`.

   b. Right-click the **SUM Downloads** folder and click **Properties**.

   c. On the Security tab, click **Edit (To change Permissions)**.

   d. In the Permissions for Sum Downloads dialog box, click **Add**.

   e. In the Select Users, Computers, Service Accounts or Groups dialog box, click **Advanced**.

   f. In the Common Queries area, select **Is exactly** for Name, type the collector service account name in the text box, and click **Find Now**.

      The collector service account name is `scm.service` by default. The search results displays the Collector service account name.

   g. Select the added account, and in the Select Users, Computers,Service Accounts or Groups dialog box click **OK**.

   h. In the Permissions for Sum Downloads dialog box, select the service user, and select the **write** check box in the panel below.

   i. Click **OK** and click **OK** in the properties window.

What to do next

Prepare SQL Server Reporting Services (SSRS) to generate VCM reports. See "Installing and Configuring SSRS on the Web Server" on the facing page.

Installing and Configuring SSRS on the Web Server

SQL Server Reporting Services (SSRS) is a server-based report generation software system that is administered using a web interface and used to deliver VCM reports.

Back Up Your SSRS Key

The `rskeymgmt` utility manages the symmetric keys used by a report server. This utility provides a way to delete encrypted content that can no longer be used if you cannot recover or apply the key.

Use the Microsoft command-line utility to back up the symmetric key to an encrypted file.

Prerequisites

- See the online Microsoft Support center for details about how to use the `rskeymgmt` utility.

Procedure

1. On the Collector file system, locate the `rskeymgmt.exe` utility at `c:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn` or the directory where you installed SQL Server.
2. To copy your SSRS key set to a removable media device and store it in a secure location, open a command line prompt and run the `rskeymgmt.exe` utility with the appropriate options.

Disable IE Protected Mode for SSRS

On the VCM Collector, when User Account Control (UAC) is turned on and Internet Explorer Protected Mode is enabled, SSRS user permissions errors and Web service errors on dashboards and node summaries can occur. UAC and Internet Explorer Protected Mode also block access to the http://localhost/reports SSRS administration interfaces. If you use another machine to access the VCM Web console interface, this problem does not occur.

CAUTION Do not use the VCM Collector Web console interface for general Internet access, because doing so causes VCM SSRS dashboard errors. If you access the Internet through the VCM Collector Web console interface, to enable the SSRS dashboards you must either disable Internet Explorer Protected Mode for the zone of the Collector or run Internet Explorer as administrator.

Do not modify the Internet Explorer Protected Mode setting in other circumstances, because doing so reduces the protection on the Collector and can increase the exposure of the Collector to attacks through Internet Explorer.

Procedure

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

Install SQL Server Reporting Services

In a three-tier installation configuration, for the Web server to generate VCM reports, install SQL Server Reporting Services (SSRS).

Prerequisites

- Back up your SSRS key. See "Back Up Your SSRS Key" on the previous page.
- Disable the Internet Explorer Protected Mode. See "Disable IE Protected Mode for SSRS" on the previous page.
- Obtain the installation media for the Enterprise, Standard, or Datacenter edition of SQL Server 2008 R2, 2012, or 2014, or verify access to a file share where the installer resides.

Procedure

1. Start the SQL Server 2008 R2, 2012, or 2014 installation.
2. Perform the actions to install SQL Server Reporting Services.

For SSRS 2008 R2

Wizard Page	Action
SQL Server Installation Center	Click **New installation or add features to an existing installation**.
Setup Support Rules	Click **Install** and verify that all of the rules pass. To view the detailed system configuration check report, click the link.
Setup Support Files	Click **Install** to install the setup support files.
Setup Support Rules – for SQL Server Setup support files	Verify that all of the rules passed.
Installation Type	Select **New installation or add shared features**.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: ■ Reporting Services Shared Features: ■ Client Tools Connectivity ■ Management Tools - Basic and Management Tools - Complete
Installation Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.

Wizard Page	Action
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is installed, select **Named Instance** and assign a name.
Disk Space Requirements	Review the disk usage summary.
Server Configuration	Click **Use the same account for all SQL Server services**. ■ If you will not install SSRS on the combined VCM Collector and Web Server machine, enter the NT AUTHORITY\SYSTEM account and password. ■ If you will install SSRS on the combined VCM Collector and Web Server, use the Network Service account instead of NT AUTHORITY\SYSTEM. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices, otherwise you must grant manual permissions.
Reporting Services Configuration	Specify the reporting services configuration mode. Select **Install, but do not configure the report server**.
Error Reporting	Review the summary information.
Installation Configuration Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Ready to Install	Review the summary of features and click **Install** to install SQL Server Reporting Services. When the installation is finished, click the link to view the log file.

For SSRS 2012

Wizard Page	Action
SQL Server Installation Center	Click **New SQL Server stand-alone installation or add features to an existing installation**.
Setup Support Rules	Click **Install** and verify that all of the rules pass. To view the detailed system configuration check report, click the link.
Product Updates	Check for SQL Server updates.
Install Setup Files	Verify that all rules are passed.

Wizard Page	Action
Setup Support Rules – for SQL Server Setup support files	Verify that all of the rules passed.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: - Reporting Services Shared Features: - Client Tools Connectivity - Management Tools - Basic and Management Tools - Complete
Installation Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Disk Space Requirements	Review the disk usage summary.
Server Configuration	Browse the accounts for all SQL services and enter the NT AUTHORITY\SYSTEM account. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Reporting Services Configuration	Specify the reporting services configuration mode.
Error Reporting	Review the summary information.
Installation Configuration Rules	Verify that the rules passed. To view the detailed system configuration check report, click the link.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

For SSRS 2014

Wizard Page	Action
SQL Server Installation Center	Click **New SQL Server stand-alone installation or add features to an existing installation**.
Product Key	Verify that the product key is entered.
License Terms	Accept the license terms.
Microsoft Update	Use this option to check for Microsoft updates.
Install Setup Files	Verify that all rules are passed.
Setup Role	Select **SQL Server Feature Installation**.
Feature Selection	Select the following features. Instance Features: ■ Reporting Services Shared Features: ■ Client Tools Connectivity ■ Management Tools - Basic and Management Tools - Complete
Instance Configuration	Select **Default Instance**. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is already installed, select **Named Instance** and assign a name.
Server Configuration	Browse the accounts for all SQL services and enter the NT AUTHORITY\SYSTEM account. It is possible to use a domain account for SQL Server services. A domain account might be required for split installations, because the SQL Server Agent might need access to the Collector for some activities. If you use a domain account, you should use a local administrator on the SQL Server machine to access DBServices. Otherwise, you must grant manual permissions.
Reporting Services Configuration	Specify the reporting services configuration mode.
Ready to Install	Review the summary of features and click **Install** to install SQL Server. When the installation is finished, click the link to view the log file.

Configure SSRS

Configure SSRS manually in your installation configuration, because the SSRS command-line configuration tool does not perform these steps.

SSRS might require HTTPS during installation. If HTTPS is required, you manually export a self-signed certificate and import it to the VCM Collector machine’s root certificate store. If you do not manually export the certificate, a manual import of a VCM report might fail. If the manual import fails, run the import from the VCM Collector machine. For more information, see the Microsoft IIS Resource Kit Tools.

Prerequisites

- Back up your SSRS key. See "Back Up Your SSRS Key" on page 109.
- Disable the Internet Explorer Protected Mode. See "Disable IE Protected Mode for SSRS" on page 109.

Procedure

1. On your Web server, start SQL Server 2008 R2, 2012, or 2014 Reporting Services Configuration Manager.
   a. Click **Start**, select **Run**, and type `rsconfigtool.exe`.
   b. In the Reporting Services Configuration Connection dialog box, click **Connect** to connect and log in to SQL Server Reporting Services.
2. Update the SQL Server database.
   a. In the navigation pane, click **Database** and click **Change Database**.
   b. In the Report Server Database Configuration pane, verify that **Action** is selected.
   c. On the Change Database page, select **Create a new report server database** and click **Next**.
   d. Change the server name of your database server to the database machine and database instance where SSRS will connect.
   e. Verify that the authentication type is set to **Current User – Integrated Security** and click **Test Connection**.
   f. When the test message is successful, close the Test Connection dialog box and click **Next**.
   g. On the Database pane, enter a name for the Database.
   h. Set the Report Server Mode to **Native Mode** and click **Next**.
   i. In the Credentials pane, change the Authentication Type to **Windows Credentials**, specify an account, and click **Next**.

      Specify an account that has permission to connect from the Web server to the database server, and specify the password for the account.
   j. In the Summary pane, review the selections and click **Next**.
   k. In the Progress and Finish pane, resolve any errors, and click **Finish**.
3. Update the encryption keys.
   a. In the navigation pane, click **Encryption Keys**.
   b. In the Delete Encrypted Content area, click **Delete** and accept the prompt to delete all encrypted data.
   c. In the Change area, click **Change** to replace the encryption key, and click **OK**.
4. Configure the Web Service URL.

a. In the navigation pane, click **Web Service URL**.

b. Verify or configure the settings and click **Apply** to activate the Report Server Web Service URL.

Option	Action
Virtual Directory	Set to **ReportServer**.
IP Address	Set to **All Assigned (Recommended)**.
TCP Port	Set to `80` if you are not using HTTPS.
SSL Certificate	Not Selected

c. In the Results area, confirm that the virtual directory is created and that the URL is reserved.

5. Confirm the Report Manager URL.

   a. In the navigation pane, click **Report Manager URL** and click **Apply** to activate the Report Manager URL.

   b. Verify that the virtual directory was created and that the URL was reserved in the Results area.

   c. Click the default URL and verify that it opens SQL Server Reporting Services.

6. Click **Exit** to close SQL Server 2008 R2, 2012, or 2014 Reporting Services Configuration Manager.

7. Reboot the Web server.

What to do next

To authenticate users and client applications against the report server, configure Basic Authentication on the report server. See "Configure Basic Authentication on the Report Server for Multi-Tier Installations" on page 115.

Configure Basic Authentication on the Report Server for Multi-Tier Installations

SQL Server Reporting Services (SSRS) provides several options to authenticate users and client applications against the report server. When you install VCM in a three-tier split installation and use Basic authentication, you must allow direct access to the Reports virtual directory.

Update the `rsreportserver.config` file so that VCM can authenticate users who use the VCM Web console, and users can launch SSRS reports. To configure Basic authentication on the report server, edit the XML elements and values in the RSReportServer.config file.

Procedure

1. On the Windows machine where you installed SSRS, stop the SSRS service.

2. Navigate to the `rsreportserver.config` file.

   By default: `C:\Program Files\Microsoft SQL Server\{`*`reporting-services-instance`*`}\Reporting Services\ReportServer\rsreportserver.config`

3. Open `rsreportserver.config` in a text editor.

4. Locate the `<AuthenticationTypes>` XML code.

```
<Authentication>
   <AuthenticationTypes>
      <RSWindowsNegotiate/>
      <RSWindowsNTLM/>
   </AuthenticationTypes>
   ...
</Authentication>
```

5. Replace any existing `<AuthenticationTypes>` parameters with one `<RSWindowsBasic/>` parameter.

```
<Authentication>
   <AuthenticationTypes>
      <RSWindowsBasic/>
   </AuthenticationTypes>
   ...
</Authentication>
```

6. Save and close `rsreportserver.config`.
7. Start the SSRS service.

What to do next

To authenticate VCM reports with Kerberos, see "Configure Kerberos Authentication" below.

Configure Kerberos Authentication

The Kerberos network protocol uses secret-key cryptography to ensure security in your VCM applications. To authenticate VCM Reports, you must use Basic Authentication with HTTPS or Kerberos Authentication.

When you configure Kerberos Authentication in your three-tier split installation, configure it on the database server and the Web server.

Prerequisites

- Verify that your Windows Server 2008 R2, 2012, or 2012 R2 machine has Active Directory management tools installed. If the tools are not installed, install them. See Microsoft TechNet online. This configuration requires an Active Directory domain running at Windows Server 2003 or later domain functional level.
- If SQL Server Reporting Services is running on a different Windows machine than the Web server in a three-tier installation, verify that the Application Pool account is a local administrator.

Procedure

1. Log in to your Windows Server 2008 R2, 2012, or 2012 R2 machine as a user who has domain administrator privileges.
2. Start **Active Directory Domain Services** and select **Active Directory Users and Computers**.
3. Verify whether AD accounts exist in your domain for the SQL Server service and the VCM IIS Application Pool.
4. If the accounts do not exist, create them.

   a. Set the database account to be a local administrator on the database server.
   b. Make the Application Pool account a local administrator on the Web server in a three-tier installation.
5. Select the Computers container and locate the Web system.
   a. Open the properties for Web system.
   b. Click the **Delegation** tab.
   c. Select **Trust this computer for delegation to any service**.
6. Open IIS manager and set the identity of the `CMAppPool` application pool to the IIS account.
7. In Reporting Services Configuration Manager, configure the SQL Server Reporting Services service to run as the IIS Application Pool account.
8. Change SQL Server to run as the SQL Server Domain account.
   a. In Reporting Services Configuration Manager, click **Encryption Keys** and click **Delete** to delete encrypted content.
   b. In the navigation pane, click **Service Account** and enter the `app_pool_account` account for the database connection.
9. Open a command prompt to set the service principal names directory property for the Active Directory service accounts.
   a. Click **Start**, select **All Programs > Accessories**, right-click **Command Prompt**, and select **Run as administrator**.
   b. Type: **`Setspn -a MSSQLSvc/db_server_name domain\sql_server_account_name`** and press **Enter**.
   c. Type: **`Setspn -a MSSQLSvc/db_server_name:1433 domain\sql_server_account_name`** and press **Enter**.
   d. Type: **`Setspn -a MSSQLSvc/db_server_fqdn domain\sql_server_account_name`** and press **Enter**.
   e. Type: **`Setspn -a MSSQLSvc/db_server_fqdn:1433 domain\sql_server_account_name`** and press **Enter**.
10. Verify whether SSRS is running on the SQL Server and if it is not running, locate and update the Report Server configuration file named `rsreportserver.config`.
    a. Locate the `AuthenticationTypes` XML element.
    b. Remove `<RSWindowsNTLM/>` and `<RSWindowsBasic/>`.
    c. Add `<RSWindowsNegotiate/>` and `<RSWindowsKerberos/>`.

    The default location for the configuration file is `C:\Program Files\Microsoft SQL Server\{`*`reporting-services-instance`*`}\Reporting Services\ReportServer\rsreportserver.config`.
11. In SQL Server Management Studio, grant the Application Pool user access to the VCM and VCM_Unix databases, with membership in the VCM__SelectRole_General role in each database.

12. (Optional) If you did not configure the SQL Server Reporting Services service to run as the IIS Application Pool account before installing VCM, start Internet Explorer as administrator and set the report settings.

    a. Click **Start**, select **All Programs**, right-click **Internet Explorer** and select **Run as administrator**.

    b. Connect to `http://localhost/Reports/Pages/Folder.aspx`.

    c. Click **ECM Reports** and click the **ECM** data source to display the properties menu.

    d. To use integrated authentication, type the following text into the Connection string text box and click **Apply**.

    ```
    Integrated Security=SSPI;Data Source=db_server_name;Initial
    Catalog=VCM;LANGUAGE=us_english;
    ```

    e. Click the back button to return to the ECM Reports view.

13. Select **Folder Settings**, select **Security**, select the new SSRS user or group, and click **New Role Assignment**.

14. Click **Browser** to allow the VCM SSRS user or group to view folders and reports and subscribe to reports, and click **OK**.

15. In Server Manager, set the authentication mode.

    a. In the navigation pane, select **Roles > Web Server (IIS)** and click **Add Role Services** in the Role Services area.

    b. In the Select Role Services wizard, locate the Security (Installed) section, click **Windows Authentication**, and follow the prompts to install the service.

    c. In the navigation pane, select **Roles > Web Server (IIS)**.

    d. Under `server_name`, select `Sites\Default Web Site\VCM`, double-click **Authentication**, and verify that Windows Authentication is the only option enabled.

    e. Under `server_name\Sites\Default Web Site`, double-click **Authentication**, click **Windows Authentication**, verify that Windows Authentication is enabled, and click **Advanced Settings**.

    f. Verify that Kernel Mode Authentication is disabled and click **OK**.

16. In Windows Explorer, update the configuration files.

    a. Open the configuration file at `Windows\System32\inetsrv\config\applicationhost.config` and locate the `<authentication>` section.

    b. Verify that Windows authentication is enabled, and if it is not enabled, enable it.

    c. Save any changes and close the file.

17. Open a command prompt to set the property for the Active Directory service accounts for the service principal names directory.

    a. Click **Start** and select **All Programs > Accessories**.

    b. Right-click **Command Prompt** and select **Run as administrator**.

    c. Type **`Setspn -a http/web_server_name domain\Application Pool Account Name`** and press **Enter**.

    d. Type **`Setspn -a http/web_server_fqdn domain\Application Pool Account Name`** and press **Enter**.

18. Open the properties for the SQL Server and Application Pool accounts, click the **Delegation** tab, and select **Trust this user for delegation to any service**.

What to do next

Modify the SQLCMD path variable to ensure that VCM Patching recognizes the SQLCMD path. See "Modify the SQLCMD Path Variable" on page 119.

Modify the SQLCMD Path Variable

SQLCMD is a command-line utility that allows you to use Transact-SQL statements, system procedures, and script files at the command prompt. To ensure that VCM Patching recognizes the SQLCMD path in a three-tier installation, you must modify the environment variable to point to the path where SQLCMD is installed.

In a three-tier split installation, SQLCMD is installed on the Web server, VCM Collector, and VCM database server when you install Client Connectivity Tools or Management Tools - Basic.

Procedure

1. On the Web server, in the Control Panel click **System and Security**.
2. Click **System**.
3. Click **Change settings**.
4. Select the **Advanced** tab.
5. Click **Environment Variables**.
6. In the User variables area, click **New**.
7. Type a name for the environment variable and enter the following value:

   ```
   C:\Program Files\Microsoft SQL Server\100\Tools\Binn
   ```
8. Click **OK** to close the New User Variable dialog box.
9. Click **OK** and **OK** to close the Environment Variables and System Properties dialog boxes.

What to do next

Configure the VCM Collector. See "Configure the VCM Collector" below.

Configure the VCM Collector

The VCM Collector contains the VCM software application and VCM services. To prepare the VCM Collector for VCM installation, configure the required utilities.

In a three-tier split installation configuration, configure the Web server and VCM Collector on separate machines.

NOTE This procedure is required only if you did not install the complete set of Management Tools and support components earlier.

Prerequisites

- Perform the prerequisite tasks for your three-tier split installation configuration. See "Three-Tier Split Installation" on page 91.
- From the VCM Collector, verify that you can access the Microsoft Download Center, Microsoft SQL Server Feature Pack to download SQLXML 4.0 SP1 in the following procedure. See the online Microsoft Download Center.

- Verify that you can access the Microsoft Download Center, Microsoft SQL Server Feature Pack to download and install the Native Client (`sqlncli.msi`) in the following procedure. See the online Microsoft Download Center. The SQL Command Line Tools in the SQL Server Feature Pack are required on the Web server and the VCM Collector.
- Install .NET Framework 3.5.1 on the Windows Server 2008 R2, 2012, or 2012 R2 machines where Package Studio will be installed.

Procedure

1. Download and install SQLXML 4.0 SP1, x64 Package.
2. Download and install SQL Server Command Line Utilities, which includes the `SQLCMD` utility, x64 Package (`SqlCmdLnUtils.msi`).

   The SQL Command Line Tools in the SQL Server 2008 R2, 2012, or 2014 Feature Pack are required on the Web server and the VCM Collector.
3. Download and install the SQL Server Native Client, x64 Package (`sqlncli.msi`).

   The Native Client from the SQL Server Feature Pack is required on the Web server and the VCM Collector.
4. Reboot the VCM Collector.

Install the .NET Framework

To support library and language interoperability, the VCM Collector must have the required versions of the .NET Framework installed.

VCM 5.8 requires the .NET 3.5.1 Framework. If you use Package Studio, the VCM Collector must have .NET 3.5.1 installed. If you use Package Manager, the VCM Collector must have .NET 3.5.1 or .NET 4.0 installed.

Determine the installed version of the .NET Framework. If one of the .NET Framework versions is missing, install the version from the Microsoft download Web site.

Procedure

1. Click **Start** and select **All Programs > Administrative Tools > Server Manager**.
2. Click **Features**.
3. Verify that .NET Framework 3.5.1 appears in the feature summary.
4. If .NET Framework 3.5.1 does not appear, under Features select **Add Features** and select **.NET 3.5.1**.

Verify the ASP.NET Client System Web Version

To support client programming, verify the ASP.NET Client System Web version to confirm that the .NET framework is installed correctly, and install it if the version is not correct.

1. Click **Start** and select **All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand **<server name>** and click **Sites**.
3. Expand **Default Web Site**, expand **aspnet_client**, and expand **system_web**.
4. Verify that the version is **2_0_50727**.

Verify the ASP Role Service

To support client programming, verify the status of the ASP Role Service to confirm that the .NET framework is installed correctly.

Procedure

1. Click **Start** and select **All Programs > 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 whether the role service is installed.
6. If the role service is not installed, click **Add Role Services** and add the ASP role service.

Verify the ASP.NET Role Service

To support client programming, verify the status of the ASP.NET Role Service to confirm that the .NET framework is installed correctly.

Procedure

1. Click **Start** and select **All Programs > 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 role service is installed.
6. If the role service is not installed, click **Add Role Services** and add the ASP.NET role service.

What to do next

Prepare to use VCM Remote. See "Using VCM Remote" below.

Using VCM Remote

If you will use VCM Remote in your three-tier split installation, you must manually export the VCM Collector certificate from the VCM Collector and install it on the Web server so that SSRS can authenticate communication with the remote machines.

To export the VCM Collector certificate from the VCM Collector and install it on the Web server, you must perform several tasks. You typically only need to perform these tasks once.

- Export the Collector Certificate from the VCM Collector.
- Import the Collector Certificate to the Web server.

What to do next

Export the Collector Certificate. See "Export the Collector Certificate from the VCM Collector" below.

Export the Collector Certificate from the VCM Collector

When you use VCM Remote in your three-tier split installation, you must export the VCM Collector certificate from the VCM Collector machine so that you can import it to the Web server machine.

Prerequisites

- Configure the database server, the Web server, and VCM Collector for your three-tier split installation. See "Three-Tier Split Installation" on page 91.

Procedure

1. On the VCM Collector, click **Start** > **Run**, type `mmc`, and click **OK** to open the Microsoft Management Console.
   a. Select **File** > **Add/Remove Snap-In**.
   b. Select **Certificates** and click **Add**.
   c. Select **Computer Account** and click **Next**.
   d. In the Select Computer dialog box, select **Local Computer** and click **Finish**.
   e. Click **OK** to add the snap-in to Microsoft Management Console.
2. In the navigation pane, click **Certificates** > **Personal** > **Certificates**.

   This directory contains the VMware VCM Collector Certificate.
3. In the center pane, right-click the VCM certificate with the `PFX` extension and select **All Tasks** > **Export**.
   a. Click **Next**.
   b. On the Export Private Key page, select **Yes, export the private key**.
   c. In the Personal Information Exchange area, select **Export all extended properties** and click **Next**.
4. On the Password page, type the password for the certificate, type it again to confirm it, and click **Next**.

   Remember or record the password, because you must supply it during certificate import process on the Web server machine.
5. On the File to Export page, click **Browse**, type a file name for the certificate file, and click **Save**.

   By default, the certificate is stored in your Documents directory.
6. On the File to Export page, click **Next** and **Finish** to export the Collector certificate to the machine.

What to do next

Import the VCM Collector certificate from the VCM Collector machine to the Web server machine. See "Import the Collector Certificate to the Web Server" below.

Import the Collector Certificate to the Web Server

To support the use of VCM Remote in a three-tier split installation, the VCM Collector certificate must exist on the Web Server machine.

Prerequisites

- Export the VCM Collector certificate from the VCM Collector machine. See "Export the Collector Certificate from the VCM Collector" on the previous page.

Procedure

1. Open a command prompt and use the `xcopy` command to copy and paste the VCM Collector certificate file from the VCMVCM Collector machine on the Web server machine.
2. On the Web server machine, to import the Collector certificate to the Web server machine, click **Start**, select **Run**, type `mmc`, and click **OK**.
3. In the Microsoft Management Console, add the Certificate snap-in.
   a. Select **File > Add/Remove Snap-In**.
   b. Select **Certificates** and click **Add**.
   c. Select **Computer Account** and click **Next**.
   d. In the Select Computer dialog box, select **Local Computer** and click **Finish**.
   e. Click **OK** to add the snap-in to Microsoft Management Console and close the Add or Remove Snap-ins dialog box.
4. In the navigation pane, click **Certificates > Personal > Certificates**.
5. In the center pane, right-click the VCM certificate and select **All Tasks > Import**.
   a. Click **Next**.
   b. On the File to Import page, select the certificate with a `PFX` extension and click **Next**.
   c. In the Personal Information Exchange area, select **Export all extended properties** and click **Next**.
6. On the Password page, type the password for the certificate, check **Include all extended properties**, and click **Next**.
7. On the Select Certificate Store page, confirm that the certificate store is set to personal and click **Next**.
8. Click **Finish** to complete the wizard.

What to do next

- Review the DCOM and port requirements, and use VCM Installation Manager to install the VCM components. See "Installing VCM" on page 125.
- Use the *VCM Administration Guide* to configure the VCM Remote Client.

Installing VCM 11

After you perform the system prerequisite tasks and configure your installation configuration, understand the components to select during VCM installation, enable DCOM and the required ports, then use the installation image to start Installation Manager and install the appropriate VCM components on the physical and virtual machines in your installation configuration.

Single-Tier Configuration

For a single-tier VCM installation, run Installation Manager once, on the single-tier server.

Select Typical Installer.

During the Installation Manager dialogs, select a SQL Server database instance that is installed on the local system.

Two-Tier Split Configuration

For a two-tier split VCM installation, run Installation Manager once, on the Collector-Web server. Do not run Installation Manager on the database server.

Select Typical Installer.

During the Installation Manager dialogs, select a SQL Server database instance on another system, one that the local system can connect to.

Three-Tier Split Configuration

For a three-tier split VCM installation, run Installation Manager twice, first on the Web server, then the Collector server. Do not run Installation Manager on the database server.

Only Advanced Installer is supported for Three-tier Split configuration.

Web server. When installing on the Web server, select the following check boxes.

- VMware vCenter Configuration Manager
  - VCM Web Console
- Tools
  - VMwareVCM Package Manager for Windows
  - VMwareVCM Package Studio

Collector server. When installing on the Collector server, select the following check boxes.

- VMware vCenter Configuration Manager
  - VCM Collector Components
- Tools
  - Import/Export Utility
  - Foundation Checker
  - VMwareVCM Package Manager for Windows

Both times that you run Installation Manager, during the dialogs, specify the SQL Server database instance on the remote database server that the Web and Collector servers can connect to.

DCOM and Port Requirements for VCM

SQL Server must communicate with the VCM Collector in split installations to submit jobs and control the Collector service. Before you install VCM, you must enable DCOM and the required port.

- On the VCM Collector, enable DCOM. Use the built-in DCOM rule named COM+ Network Access (DCOM-In).
- On the database server, enable port 1433. For more information, see Microsoft TechNet online.

To VCM Installation Manager to install the VCM components, see "Installing VCM" on the previous page.

Install VCM using Advanced Installation

Use the VCM Installer to access and start the Advanced Installation. The Advanced Installation option runs the classic VCM Installation Manager.

Prerequisites

- Review the list of supported platforms. See "Hardware and Operating System Requirements for VCM Managed Machines" on page 167.
- If you are migrating a version of VCM to VCM 5.8, a SQL Server version to 2008 R2, 2012, or 2014, or a 32-bit environment to a 64-bit environment, see "Upgrading or Migrating VCM" on page 137.
- Obtain the installation package from the Download VMware vRealize Configuration Manager Web site or use the VCM 5.8 installation media.
- Have your suite, server, or workstation license key available.

CAUTION When the installation requires the domain name for the database server, use the NetBIOS short form name. In two-tier and three-tier installations, if you install the Collector component using the fully qualified domain name (FQDN), the Collector service stops after installation and does not start, and collections do not run. For more information, see http://kb.vmware.com/kb/2000084.

Procedure

1. Start the VCM Installer from a network location or insert the VCM installation media into the Windows machine.

   If you started the VCM Installer from a network location or if the initial screen does not appear, navigate to the media root directory or the file share and double-click `Setup.exe`.

2. Select **Advanced Installation** and follow the prompts to finish the installation.
3. For information about the installation options, click **Help** to open the Installation Manager online help.

What to do next

- After VCM is installed, verify that a SpringSource Tomcat service is registered as a local service with the Web server or the database server. If the Tomcat service is missing, the installation encountered errors that might be because of account permissions, which affect license upgrades. Check the prerequisites, including the permissions, and reinstall VCM.
- Set permissions on Machine Keys.

File System Permissions

VCM users, administrators, and service accounts must have permission to access the VCM file system. These permissions include access to the directories on the VCM Collector at `Program Files (x86) \VMware\VCM\WebConsole\L1033\Files`. The `L1033\Files` subdirectory is shared as `CMFiles$`.

You must modify the permissions according to the requirements of your environment. For example, users must have read and write access to the Exported Reports directory to export reports.

The following directories in `L1033\Files` serve multiple purposes for users, administrators, and service accounts.

- `Discovery_Files`: Provides access to text files that are used to discover or add machines manually.
- `ERD_Extracts`: Provides access to the default directory that contains extracted emergency repair disk files. Backing up registry files requires the `SE_BACKUP_NAME` user right.
- `Exported Reports`: Allows access to the exported reports.
- `File_Upload_Extracts`: Allows access to the extracted copies of files uploaded from VCM.
- `HistoryCache`: Provides access to report history files.
- `ImportedSRSReports`: Allows access to SQL Server Reporting Service (SSRS) reports that are imported into VCM.
- `Remote_Command_Files`: Provides access to the Windows remote command files that are required to run remote commands in VCM.
- `Reports`: Provides access to VCM reports, which include AD, UNIX, Licensing, Provisioning, VCM Patching, Virtualization, and so on.
- `SCAP`: Provides access to the SCAP import and export files used to assess your managed machines against SCAP benchmarks.
- `SUM Downloads`: Provides access to patch files to patch managed machines. The service account user, or a group to which this user belongs, must have write permission to this directory, or the user must have Administrative privileges to this directory. If the service account does not have Administrator privileges to use VCM Patching to deploy patches, the system Administrator must modify the file permissions.
- `SUM_Input`: Provides access to text files that are used to create new imported templates to patch managed machines.
- `UNIX_Remote_Command_Files`: Provides access to the UNIX remote command files that are required to run remote commands in VCM.

Change Permissions On Machine Certificate Keys

If you plan to use certificate keys generated by Installation Manager for HTTP communication between the VCM Collector and the VCM Agents on managed machines, you must review your security policy. You can change the permissions on the certificate key to allow the Administrators group to have full control after you install VCM.

The Foundation Checker system check reports a warning message about the security policy used to create new objects. The security policy sets the permission on new files to the Administrators group instead of the creator of the object. The system check does not stop the installation process, but instead creates a certificate and associated cryptographic keys.

If the security policy is not set appropriately when Installation Manager generates the certificate, the certificate private key is not accessible to other members of the Administrators group and causes HTTP communication with the Agents to fail.

The TLS certificate private key to be generated on the Windows machine must have permissions that include the Administrators group as the owner or as having full control. You cannot resolve this warning before you install VCM. If an error occurs, after installation, you must either change the group policy so that new files are assigned to the Administrators group and run Installation Manager again, or add the Administrators group with full control to the generated certificate key file in the Machine Keys folder.

Prerequisites

- Install VCM. See "Installing VCM" on page 125.

Procedure

1. Browse to `C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys`.

   This path is the default location for your private keys. This path might differ depending on your organizational policies.

2. Expand the `MachineKeys` folder.

   The key that matches the date and time when you generated the certificate during installation is most likely the correct key. Because another reliable method does not exist to identify the key, use the date and time.

3. Right-click the key file and click **Properties**.
4. In the Machine Key Properties dialog box, click the **Security** tab.
5. Click **Continue** to continue as an administrative user.
6. In Advanced Security Settings, select the account and click **OK** to take ownership of an account.
7. In the Permissions dialog box, click **Administrators** and confirm whether the Administrators group has Full Control.
8. If the Administrators group does not have full control, click **Add** to add the group.
9. In the Select Users, Computers, Service Accounts, or Groups dialog box, type the name of the Administrators group and click **Check Names**.

   When the name is validated, click **OK** to return to the Permissions dialog box and add the Administrators group to the Group or user names area.

10. In the Allow column, click **Full Control**.
11. Click **OK** and click **OK** again to save changes.

What to do next

Set the VCM Remote Virtual Directory Permissions for Installation. See "Verify VCM Remote Virtual Directory Permissions" below.

Verify VCM Remote Virtual Directory Permissions

The VCM Remote Virtual Directory is required for client access to VCM over HTTP. During VCM installation, you specify the VCM Remote virtual directory. To change the account later, use the IIS Management console.

IMPORTANT To minimize security risks to your accounts, when you specify the VCM Remote virtual directory, always use an account that differs from the account used for your Default Network Authority Account or your Services Account.

Prerequisites

VCM uses virtual directories for several functions. Before starting Installation Manager, verify that the user who installs VCM has local administration rights for the default Web site.

Procedure

1. Click **Start** and select **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.

What to do next

Configure SQL Server database file growth and database recovery settings to tune your VCM database. See the *VCM Installation Guide*.

Configuring SQL Server for VCM 12

VCM relies heavily on its SQL databases for operation. You must update the default settings to optimize SQL Server performance. These settings include the SQL Server database settings, processor settings, and the Input/Output (I/O) configuration.

To ensure that VCM runs at peak performance and requires little operator intervention during its lifecycle, set up a routine maintenance plan. See the *VCM Administration Guide*.

About VCM Databases

Data associated with VCM is stored in its SQL Server databases.

All VCM databases are installed in the same SQL Server instance and must not be manually moved to separate instances.

Table 12–1. VCM SQL Server Databases

Database Name	Description
VCM	Contains configuration data for the VCM application itself, collected data from Window systems and virtual infrastructure, change details from all systems, and results of patch and compliance assessments. The base name VCM is a default that may be changed.
VCM_Coll	Provides operational state information for the Collector service, mainly used to track details of running jobs and last contact state of managed client systems.
VCM_UNIX	Contains the collected managed machine data gathered from any Linux, UNIX, or Mac Agents in the environment.
VCM_Raw	For performance improvement, a database that temporarily holds collection data before transformation into the VCM and VCM_UNIX databases. The raw database should not be backed up and should not be included in maintenance plans.

SQL Server Database Settings

Configure the database settings for VCM to optimize SQL Server performance.

Procedure

1. Launch **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. Configure the following settings.
   - **Default index fill factor.** Sets a percentage value for the amount of free space in each index page when the page is rebuilt. Set the fill factor to 80% to keep 20% free space available in each index page. This setting is part of the SQL maintenance plan wizard. If you configure the default fill factor using this setting, keep free space in an index when you run a maintenance plan.
   - **Recovery interval (minutes).** Configures the approximate amount of time that SQL Server takes to run the recovery process. Set the value to 5. The default setting is 0, which causes SQL Server to adjust this value and base the values on the historical operation of the server. In large environments, the recovery interval can affect the overall performance of VCM. Because VCM constantly updates how it interacts with SQL Server to process activities whose intervals differ, such as an inspection request and a compliance run, the server expends much time constantly adjusting this value. By setting the recovery interval to 5 minutes, SQL Server no longer must tune this value.
5. Click **OK** to save the settings.

SQL Server Processor Settings

In multiprocessor environments, you must configure the SQL Server use of the processors. To do this, you reserve a processor by removing it from SQL Server, to be used for other functions such as the VCM Collector service and Internet Information Services (IIS). Because IIS cannot make use of processor affinity in multiprocessor machines, it uses them all equally.

The hyper-threading machine-level setting must be controlled through 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. If the threads are each working with a relatively large block of data, such as 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.

Configure SQL Server Processor Settings

Configure the SQL Server Processor settings to set the maximum worker threads or boost the SQL Server priority.

Procedure

1. Launch **SQL Server Management Studio**.
2. Right-click the SQL instance that you installed and select **Properties**.
3. In the navigation pane, select **Processors**.
4. In the Enable processors area, select **Automatically set I/O affinity mask for all processors**.
5. Select **I/O Affinity** for all processors in the Enable processors list.
6. Configure the following settings as needed for your configuration and restart the SQL Server service for the changes to take effect.

- To remove a processor from SQL Server and reserve it for the OS, uncheck the check box next to the processor. Remove the processor that the network card will use so that network communication does not affect SQL Server. Most network cards use the first processor, but some Intel network cards use the last processor.
- When hyperthreading is enabled, the processor list normally starts at 0 and lists the number of physical cores, and then repeats to include the hyperthread-created processors. For example, to unlink the first core from SQL in a four-CPU hyperthreaded system, which includes eight processors according to the OS, clear the check boxes next to CPU 0 and CPU 4. This is the preferred logical processor enumeration sequence recommended to BIOS vendors by Intel as part of its Netburst architecture. A BIOS that uses this preferred sequence shows the two threads of the first Hyper-threaded CPU as logical CPU 0 and 1. To confirm which algorithm is used, verify with the BIOS vendor or compare the SQL Server processor affinity options with and without hyperthreading enabled.

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

SQL Server I/O Configuration

IT organizations do not analyze the technical drivers behind Disk I/O 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, the more work it takes 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 database administrators configure the disk I/O 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 circular order, which means each disk in the array holds only a portion of the total data written. Depending on the array configuration, this method 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. This configuration uses mirroring on a single channel or 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 two physical disks, which means the array is capable of increasing the read performance. In a duplexed environment, the performance is theoretically doubled while providing fault tolerance in case a drive fails. Write performance is not affected by RAID 1. Only two 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 one disk. For example, 80GB + 80GB + 80GB is equal to the total array size of 160GB.

- **RAID 0+1.** Mirror of Stripes. In this configuration, two 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.

Using the RAID Levels with SQL Server

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, use RAID 1.
- 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. Where possible, do not mix the log files or data files with the OS or application files. For example, at a minimum SQL Server prefers three separate disk channels.

Disk Interface and Disk Drive Performance

In addition to selecting the appropriate RAID configuration, consider the 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 an adequate 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 for the SA6404) and on-board, battery-backed-up cache. The cache provides 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 data rate up to 600MB/s for newer controllers, which is higher than the U320. 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.

When you design RAIDs, regardless of the technology, a consideration is to use 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 that has four drives on each channel of a two-channel U320 controller that is 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 provides fault tolerance for cabinet failures.

An alternative to local storage for VCM is to use SAN storage. A common problem with SANs and older versions of VCM 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 VCM 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, because 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. Achieving that throughput also depends 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, consider throughput, which includes the read and write speed, and access latency. Throughput and latency are important factors, 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 small queries before it can perform the next task.

After you install a VCM Collector, use Performance Monitor to analyze the performance of the disk subsystem. 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 on whether a logical drive has sufficient throughput and access speed for the tasks being required. The Disk Queue Length should not typically 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 might show high queuing due to insufficient RAM, but the counter can be useful to determine whether disk subsystem resources are appropriate and whether the resources are optimally arranged, such as disks per channel, RAID type, and so on.

Use SQLIO to Determine I/O 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 I/O configuration and to obtain a baseline of how well the I/O subsystem functions, run SQLIO before you install VCM.

After you download and install SQLIO, configure the following SQLIO settings to ensure an accurate report of I/O throughput.

- 64K Block Size
- 4 Threads
- 2GB File Size minimum
- Sequential I/O

When you execute SQLIO, verify that you create baseline information for each I/O channel (logical disk) to be used for VCM data, as well as testing both read and write operations.

Upgrading or Migrating VCM 13

Upgrade or migrate your existing VCM environment to VCM 5.8, which supports 64-bit environments that include 64-bit hardware, 64-bit Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2, and SQL Server 2008 R2, 2012, or 2014.

Determine whether your VCM environment requires an upgrade or a migration. The prerequisites and steps differ depending on whether you perform an upgrade or a migration of VCM.

⚠ **CAUTION** VCM 5.8 does not include the Patch Administrator role. If you previously assigned the Patch Administrator role to a user, either reassign a different role to the user or let the user know that the role no longer exists.

Upgrading VCM and Components

An upgrade converts an earlier VCM version to VCM 5.8. VCM 5.8 supports the following upgrade paths.

- Upgrade directly from VCM 5.6 or later by running the VCM 5.8 Installation Manager.

  To upgrade software licenses for the VMware vCloud Suite or vRealize Operations Manager Suite, use the JLicense utility.

- Upgrade VCM versions earlier than 5.6 to VCM 5.6, and then upgrade from VCM 5.6 to VCM 5.8.

  Earlier versions include VMware VCM 5.5.x, 5.4, 5.3, 5.2.1, EMC Ionix SCM 5.0 or later, or Configuresoft ECM 4.11.1 or later. Only database upgrade is supported for the earlier mentioned versions.

  An earlier version upgrade might require that you also upgrade to Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 and SQL Server 2008 R2, 2012, or 2014.

Prerequisites

- Verify that your VCM Collector meets all of the hardware requirements for a 64-bit environment. See "Hardware Requirements for Collector Machines" on page 11.
- Verify that your VCM Collector meets all of the software requirements for a 64-bit environment. See "Software and Operating System Requirements for Collector Machines" on page 17.
- Obtain the installation package from the Download VMware vRealize Configuration Manager Web site or the VCM 5.8 CD.

Procedure

- "Upgrade VCM" below

  An upgrade converts an earlier VCM version to VCM 5.8. You can upgrade a 64-bit environment that is running VCM 5.6 or later directly to VCM 5.8.

- "Upgrade Existing Windows Agents" on page 141

  Use the Upgrade Agent wizard to upgrade the Agent files on one or more Windows machines. If you are upgrading VCM from 5.4, an upgrade to your Windows Agents is not required.

- "Upgrade Existing VCM Remote Clients" on page 142

  The VCM Collector can determine whether the VCM Remote client machine is running an older version of the client software, and can automatically upgrade the version on the client.

- "Upgrade Existing UNIX Agents" on page 143

  Use the UNIX Agent upgrade packages to update the VCM Agents on your UNIX machines. You can use a local package or a remote package to upgrade the UNIX Agents.

- "Upgrading Virtual Environments Collections" on page 146

  To upgrade vCenter Server collections, install the VCM 5.4 Agent or later on the Windows machines running vCenter Server.

Upgrade VCM

An upgrade converts an earlier VCM version to VCM 5.8. You can upgrade a 64-bit environment that is running VCM 5.6 or later directly to VCM 5.8.

This procedure describes a single-tier VCM upgrade. For split configurations, see "Upgrade a Two-Tier Split VCM Configuration" on the facing page or "Upgrade a Three-Tier Split VCM Configuration" on page 140.

Prerequisites

Correct any missing prerequisites to upgrade VCM in a 64-bit environment. See "Upgrading VCM and Components" on the previous page.

Procedure

1. If it is not already installed, upgrade the operating system to Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
2. If it is not already installed, upgrade SQL Server to SQL Server 2008 R2, 2012, or 2014.

   Also upgrade SSRS as part of that process.

   a. Uninstall the 32-bit version of SSRS 2005.

   b. Run the SQL Server 2008 R2, 2012, or 2014 installer, and add SSRS.

   c. Launch **Reporting Services Configuration Manager**.

   d. Select the existing `ReportServer` database.

   e. Configure the Web Service and Report Manager URLs.

   f. Select the **Encryption Keys** option to delete encrypted content so that the new installation of SSRS can use the existing SSRS database.

3. From the VCM 5.8 installer, run the Advanced Installation, and select the **Upgrade** option.
4. Complete the classic VCM Installation Manager dialogs to upgrade VCM.

   Some dialogs are populated with values from the previous VCM installation so that you can quickly click through or make changes.

What to do next

Log in to VCM and upgrade your VCM Windows Agents. See "Upgrade Existing Windows Agents" on page 141.

Upgrade a Two-Tier Split VCM Configuration

An upgrade converts an earlier VCM version to VCM 5.8. You can upgrade a 64-bit environment that is running VCM 5.6 or later directly to VCM 5.8.

Prerequisites

Correct any missing prerequisites to upgrade VCM in a 64-bit environment. See "Upgrading VCM and Components" on page 137.

Procedure

1. Log in to the VCM database server.
2. If it is not already installed, upgrade the operating system to Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
3. If it is not already installed, upgrade SQL Server to SQL Server 2008 R2, 2012, or 2014.

   Also upgrade SSRS as part of that process, if SSRS is configured on the database server.

   a. Uninstall the 32-bit version of SSRS 2005.
   b. Run the SQL Server 2008 R2, 2012, or 2014 installer, and add SSRS.
   c. Launch **Reporting Services Configuration Manager**.
   d. Select the existing `ReportServer` database.
   e. Configure the Web Service and Report Manager URLs.
   f. Select the **Encryption Keys** option to delete encrypted content so that the new installation of SSRS can use the existing SSRS database.
4. From the VCM 5.8 installer, run the Advanced Installation, and select the **Remove** option.
5. Complete the classic VCM Installation Manager dialogs.

   Let Installation Manager uninstall VCM from the database server, which leaves the VCM databases intact.

   NOTE Do not install VCM 5.8 on the database server.

6. Log in to the Collector-Web server.
7. If it is not already installed, upgrade the operating system to Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
8. If it is not already installed, upgrade SSRS to SSRS 2008 R2, 2012, or 2014, if SSRS is configured on the

Collector-Web server.

   a. Uninstall the 32-bit version of SSRS 2005.

   b. Run the SQL Server 2008 R2, 2012, or 2014 installer, and add SSRS.

   c. Launch **Reporting Services Configuration Manager**.

   d. Select the existing `ReportServer` database.

   e. Configure the Web Service and Report Manager URLs.

   f. Select the **Encryption Keys** option to delete encrypted content so that the new installation of SSRS can use the existing SSRS database.

9. From the VCM 5.8 installer, run the Advanced Installation, and select the **Upgrade** option.

10. Complete the classic VCM Installation Manager dialogs to upgrade VCM.

    Some dialogs are populated with values from the previous VCM installation so that you can quickly click through or make changes. To specify the VCM database, select the database instance on the other server.

What to do next

Log in to VCM and upgrade your VCM Windows Agents. See "Upgrade Existing Windows Agents" on the facing page.

Upgrade a Three-Tier Split VCM Configuration

An upgrade converts an earlier VCM version to VCM 5.8. You can upgrade a 64-bit environment that is running VCM 5.6 or later directly to VCM 5.8.

Prerequisites

Correct any missing prerequisites to upgrade VCM in a 64-bit environment. See "Upgrading VCM and Components" on page 137.

Procedure

1. Log in to the VCM database server.

2. If it is not already installed, upgrade the operating system to Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.

3. If it is not already installed, upgrade SQL Server to SQL Server 2008 R2, 2012, or 2014.

   Also upgrade SSRS as part of that process, if SSRS is configured on the database server.

   a. Uninstall the 32-bit version of SSRS 2005.

   b. Run the SQL Server 2008 R2, 2012, or 2014 installer, and add SSRS.

   c. Launch **Reporting Services Configuration Manager**.

   d. Select the existing `ReportServer` database.

   e. Configure the Web Service and Report Manager URLs.

   f. Select the **Encryption Keys** option to delete encrypted content so that the new installation of SSRS can use the existing SSRS database.

4. From the VCM 5.8 installer, run the Advanced Installation, and select the **Remove** option.

5. Complete the classic VCM Installation Manager dialogs.

Let Installation Manager uninstall VCM from the database server, which leaves the VCM databases intact.

NOTE Do not install VCM 5.8 on the database server.

6. Log in to the Web server.
7. If it is not already installed, upgrade the operating system to Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
8. If it is not already installed, upgrade SSRS to SSRS 2008 R2, 2012, or 2014, if SSRS is configured on the Web server.
   a. Uninstall the 32-bit version of SSRS 2005.
   b. Run the SQL Server 2008 R2, 2012, or 2014 installer, and add SSRS.
   c. Launch **Reporting Services Configuration Manager**.
   d. Select the existing `ReportServer` database.
   e. Configure the Web Service and Report Manager URLs.
   f. Select the **Encryption Keys** option to delete encrypted content so that the new installation of SSRS can use the existing SSRS database.
9. From the VCM 5.8 installer, run the Advanced Installation, and select the **Upgrade** option.
10. Complete the classic VCM Installation Manager dialogs to upgrade VCM.

    Some dialogs are populated with values from the previous VCM installation so that you can quickly click through or make changes. To specify the VCM database, select the database instance on the database server.
11. Log in to the Collector.
12. If it is not already installed, upgrade the operating system to Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
13. From the VCM 5.8 installer, run the Advanced Installation, and select the **Upgrade** option.
14. Complete the classic VCM Installation Manager dialogs to upgrade VCM.

    Some dialogs are populated with values from the previous VCM installation so that you can quickly click through or make changes. To specify the VCM database, select the database instance on the database server.

What to do next

Log in to VCM and upgrade your VCM Windows Agents. See "Upgrade Existing Windows Agents" below.

Upgrade Existing Windows Agents

Use the Upgrade Agent wizard to upgrade the Agent files on one or more Windows machines. If you are upgrading VCM from 5.4, an upgrade to your Windows Agents is not required.

The upgrade process uses the current settings of the Agent installed on the Windows machine. For example, if the Agent uses DCOM, or HTTP on port 26542, the upgrade process retains that setting. This process will not upgrade components that do not require an upgrade.

Prerequisites

- Review the supported platforms. See "Hardware and Operating System Requirements for VCM Managed Machines" on page 167.
- Install the VCM Agent on the managed machines to upgrade.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. Select the Windows machines to upgrade.
4. On the toolbar, click the **Upgrade Agent** icon.
5. On the Machines page, select the Windows machines to upgrade and click the arrow to move the machines to the Selected pane.

Option	Description
All machines	Upgrades the Agent on all machines that appear in the list of licensed machines.
Filtered machines only	Upgrades the Agent on all machines that appear in the filtered list of machines. This option is only available if the Licensed Machines list is being filtered.
Selected machine(s) only	Upgrades the Agent only on selected individual machines.

6. Click **Next**.
7. On the Install Options page, select or verify the option for the Agent installation and click **Next**.

   The default source of the Agent files is the Collector machine. If you created an Alternate Source, select it from the drop-down list.
8. On the Schedule page, schedule the operation and click **Next**.
9. On the Important page, verify the summary and click **Finish**.

What to do next

Upgrade your VCM Remote clients.

Upgrade Existing VCM Remote Clients

The VCM Collector can determine whether the VCM Remote client machine is running an older version of the client software, and can automatically upgrade the version on the client.

Prerequisites

Install the VCM Agent on the managed machines to upgrade.

Procedure

1. Click **Administration**.
2. Select **Settings** > **General Settings** > **VCM Remote**.
3. Select the **Will Remote automatically upgrade old Remote clients?** setting.
4. Click **Edit Setting** and select **Yes**.

   When this setting is enabled, the next contact between the client and server automatically downloads and installs the upgrade files and upgrades the VCM Remote client software on the client machine.

   If the VCM Remote client does not have a certificate, the upgrade process automatically extracts the certificate and sends it to the client, along with the new Agent.
5. Click **Next** and **Finish**.

What to do next

Upgrade your VCM UNIX Agents. See "Upgrade Existing UNIX Agents" below.

Red Hat Server and Workstation Licensing

When you upgrade the UNIX Agent on Red Hat machines, be aware of the licensing changes between VCM versions. In VCM 5.8, physical and virtual machines are licensed as servers or workstations.

Upgrade Existing UNIX Agents

Use the UNIX Agent upgrade packages to update the VCM Agents on your UNIX machines. You can use a local package or a remote package to upgrade the UNIX Agents.

VCM supports upgrading the UNIX Agent on most Linux and UNIX platforms. Other UNIX platforms are only supported up to a specific Agent version. For a complete list of UNIX Agents supported on Linux and UNIX platforms, see "Hardware and Operating System Requirements for VCM Managed Machines" on page 167.

Prerequisites

- Identify UNIX machines that are not supported for upgrade to the VCM 5.8 Agent. See "Hardware and Operating System Requirements for VCM Managed Machines" on page 167.
- Understand Red Hat server and workstation licensing for different versions of VCM. See "Red Hat Server and Workstation Licensing" above.
- Understand VCM support for the Transport Layer Security protocol. See the *VCM Security Guide*.
- If you install the VCM Agent on HP-UX 11.11 platforms, install patch `PHSS_30966`.

Procedure

- "Upgrade UNIX Agents Using a Local Package" on the next page

  Use UNIX remote commands and the local Agent package to upgrade the VCM UNIX Agent on the UNIX platforms in your environment.
- "Upgrade UNIX Agents Using a Remote Package" on page 145

  Use VCM remote commands and a remote Agent package to upgrade the VCM UNIX Agent on the UNIX platforms in your environment.

Upgrade UNIX Agents Using a Local Package

Use UNIX remote commands and the local Agent package to upgrade the VCM UNIX Agent on the UNIX platforms in your environment.

The `Agent Upgrade - Local Package` UNIX remote command upgrades existing UNIX Agents when the Agent package exists locally or in a remote location that is accessible by the target machine, such as on a file share.

Prerequisites

- Install the VCM UNIX Agent on the managed machines to upgrade.
- Determine which Agent version is installed on a UNIX machine. Click **Administration** and select **Machines Manager > Licensed Machines > Licensed UNIX Machines**.

Procedure

1. On your VCM Collector, open Windows Explorer.
2. Select `\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\UNIX_Remote_Command_Files`.
3. Locate the `AgentUpgradeLocal.sh` UNIX Agent upgrade package.
4. Open `AgentUpgradeLocal.sh` in a text editor.
5. Locate the following entry:

   ```
   CSI_INSTALL_PACKAGE_LOCATION = CHANGE_THIS_TO_A_LOCAL_OR_NFS_DIRECTORY
   ```

6. Change this entry to a local directory or network file share where the VCM Agent installation packages reside.

   For example, `/tmp/VCMu_Agent`.

   Agent installation packages reside on the Collector in `\Program Files (x86)\VMware\VCM\Installer\Packages`.

7. Save and close `AgentUpgradeLocal.sh`.
8. Log in to VCM.
9. Click **Console**.
10. Select **UNIX Remote Commands > UNIX Agent Upgrade**.

    Although you can select any of the UNIX Agent types listed, this procedure upgrades the UNIX Agent when the Agent package exists locally or in a remote location that is accessible by the target machine.

11. In the UNIX Agent Upgrade data grid, select **Agent Upgrade - Local Package** and click **Run**.
12. Select the machines on which to upgrade the UNIX Agent.

    To determine which Agent is installed on a UNIX machine, click **Administration** and select **Machines Manager > Licensed Machines > Licensed UNIX Machines**.

13. Click the arrow button to move the machines from the **Available list** to the **Selected list** and click **Next**.
14. Select whether to upgrade the Agent now or later.

    When you schedule the action, it appears in the **Administration > Job Manager > Scheduled** list.

The Time of Day settings are based on your user time zone. All VCM jobs run based on the VCM database time zone. Account for the time and date differences between your VCM user time and your VCM database time. For example, if your VCM database server is in the Eastern time zone, and your VCM user is in the Pacific time zone, to run your job at midnight, enter 9 PM.

15. Click **Next** and **Finish**.

What to do next

Upgrade your UNIX Agents using a remote package. See "Upgrade UNIX Agents Using a Remote Package" below.

Upgrade UNIX Agents Using a Remote Package

Use VCM remote commands and a remote Agent package to upgrade the VCM UNIX Agent on the UNIX platforms in your environment.

The UNIX Agents use Transport Layer Security (TLS) and the Enterprise Certificate is embedded in the Agent package. If multiple Collectors must communicate with a single Agent, all of the Collectors must share an Enterprise Certificate. If the Collectors have different Enterprise Certificates, the Enterprise Certificate from each Collector must be uploaded to the Agent. See the *VCM Security Guide*.

The UNIX remote commands use existing configuration settings to upgrade the UNIX Agents using a remote Agent package. VCM sends the Agent package to the target machine.

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

- AIX 5 Agent Upgrade
- HP-UX (Itanium) Agent Upgrade
- HP-UX (PA-RISC) Agent Upgrade
- Mac OS X Agent Upgrade
- Red Hat Enterprise 3.0, 4.0, 5.0, 5.1, 5.2, and SUSE Enterprise 9 and above Agent Upgrade
- Solaris (SPARC) Agent Upgrade
- Solaris (x86) Agent Upgrade

Older machines use the following packages.

- For AIX 4.3.3 Agent Upgrade, use only `CMAgent.5.1.0.AIX.4`.
- For Red Hat Enterprise 2.1 Agent Upgrade, use only `CMAgent.5.1.0.Linux.2.1.`

The following procedure upgrades the UNIX Agents using one of the remote upgrade packages.

Prerequisites

- Install the VCM UNIX Agent on the managed machines to upgrade.

Procedure

1. Click **Console**.
2. Select **UNIX Remote Commands > UNIX Agent Upgrade**.
3. In the UNIX Agent Upgrade data grid, click the appropriate remote upgrade package for the operating system and version of the machines to upgrade.
4. Click **Run** and follow the wizard to send the remote command and upgrade package to the Agents on

the selected machines.

The Agent executes the upgrade package.

What to do next

Upgrade VCM for Virtualization. See "Upgrading Virtual Environments Collections" below.

Upgrading Virtual Environments Collections

VCM 5.5 and later collect data directly from instances of vCenter Server, vCloud Director, and vShield Manager using a Managing Agent. See the *VCM Administration Guide*. To upgrade your virtual environment,you might upgrade the Windows Managing Agent, the vSphere Client VCM Plug-In, or the Agent Proxy.

Upgrade the Managing Agent

A Managing Agent is a Windows machine on which the VCM 5.5 Agent or later is installed, and which is configured as a Managing Agent in VCM. To upgrade the Managing Agent, upgrade the VCM Agent on the Windows machine. See "Upgrade Existing Windows Agents" on page 141.

Upgrading the vSphere Client VCM Plug-In

Before you upgrade to the new version of the vSphere Client VCM Plug-In that is available when you upgrade VCM, you must unregister a previous version of the plug-in.

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

The VCM upgrade removes the previous plug-in files and installs the new plug-in files in new locations with new names. The VCM upgrade does not register the new plug-in with the vSphere Client.

Procedure

1. On your Collector machine, navigate to `C:\Program Files (x86)\VMware\VCM\Tools\vSphere Client VCM Plug-in\bin`.
2. Double-click `VCVPInstaller.exe`.
3. In the vSphere Client VCM Plug-In Registration dialog box, click **Unregister**.
4. In the Server URL text box, enter the name of your vCenter Server.

   For example, `https//vcenter05/sdk`.
5. In the Administrator User Name and Password text boxes, enter the Administrator user name and password.
6. Click **OK**.

What to do next

Upgrade the vSphere Client VCM Plug-In. See "Upgrade the vSphere Client VCM Plug-In" below.

Upgrade the vSphere Client VCM Plug-In

If your version of the vSphere Client VCM Plug-In is 5.3 or earlier, or if the URL to the VCM instance has changed, upgrade the vSphere Client VCM Plug-In.

Prerequisites

- Unregister the previous version of the vSphere Client VCM Plug-In. See "Unregister the Previous Version of the vSphere Client VCM Plug-In" on the previous page.
- Locate the procedure to upgrade VCM. See "Upgrading VCM and Components" on page 137.

Procedure

1. Upgrade VCM.

What to do next

Register the new vSphere Client VCM Plug-In. See the *VCM Administration Guide*.

Upgrading Agent Proxy Machines

When you upgrade a Collector to VCM 5.8, the Agent Proxy on the Collector is automatically upgraded and the Agent Proxy protected storage and user account configuration settings are preserved. For existing non-Collector Agent Proxy machines, you must upgrade VCM for Virtualization and retain the Secure Communication settings.

The Agent Proxy configuration is only used to collect the ESX logs and Linux data types form the ESX Service Console OS.

Prerequisites

- Do not change the password for the CSI Communication Proxy service when you upgrade VCM for Virtualization. If you change the password, you might need to reinstall and reconfigure the Agent Proxy.
- Do not install the Agent Proxy and Active Directory on the same machine. The operations required to install, uninstall, upgrade, and reinstall these products can cause you to reinstall and reconfigure the Agent Proxy.
- Before you uninstall VCM for Virtualization manually, you must execute `RetainSecureCommSettings.exe`. Otherwise, the Agent Proxy configuration settings will be removed, and you will need to reconfigure the Agent Proxy. The `RetainSecureCommSettings.exe` is located in `C:\Program Files (x86)\VMware\VCM\Installer\Packages`, or in the path relative to where you installed the software. For more information about configuring vCenter Server data collections, see the *VCM Administration Guide*.

Procedure

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

- "Use VCM to Upgrade an Agent Proxy Machine" on the next page

  Use VCM to upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine. If a new version of the Agent Proxy becomes available, the upgrade process installs the newer version on your Agent Proxy machine.

- "Manually Upgrade an Agent Proxy Machine" on the next page

  Manually upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine. Use this method to upgrade an Agent Proxy machine if you do not use the upgrade option in VCM.

Use VCM to Upgrade an Agent Proxy Machine

Use VCM to upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine. If a new version of the Agent Proxy becomes available, the upgrade process installs the newer version on your Agent Proxy machine.

Procedure

1. On your VCM Collector, click **Administration**.
2. Select **Machines Manager > Additional Components > Agent Proxies**.
3. In the Agent Proxies data grid, select the machines on which to upgrade the Agent Proxy.
4. Click **Upgrade**.
5. On the Upgrade Agent Proxies Machines page, select an action and click **Next**.

Option	Description
All Machines	Runs the process on all eligible machines.
Selected Machines Only	Runs the process on all machines listed in the lower pane.
Filtered Machines	Creates a filter based on the machine name or domain name.
Arrow buttons	Moves a selected machine name between panes.

6. On the Option page, configure the options and click **Next**.

Option	Description
Install From	Selects the name of the Collector used to manage virtual machines.
Schedule	Sets the schedule to run the action.

7. On the Important page, review the summary, click **Back** to make any necessary alterations, and click **Finish**.

   VCM upgrades the Agent Proxy at the specified time.

What to do next

Verify that the upgrade process finished. Click **Jobs** to display the Jobs Summary. To verify jobs for the past 24 hours click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.

Manually Upgrade an Agent Proxy Machine

Manually upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine. Use this method to upgrade an Agent Proxy machine if you do not use the upgrade option in VCM.

After the upgrade, all managed Windows machines include the VCM Agent extension for VCM Provisioning.

Prerequisites

- Upgrade your Collector to VCM 5.8.
- Confirm that `\VMware\VCM\AgentFiles\CMAgentInstall.exe` is accessible from your non-Collector Agent Proxy machine. The path on the Collector machine is `C:\Program Files (x86)\VMware\VCM\AgentFiles\CMAgentInstall.exe`, or in the path relative to where you installed the software.

- For Agent Proxy machines, if the Virtualization proxy and VCM Agent extensions for Provisioning are installed, you must run `ProvisioningProductInstall.exe` from the VCM Collector.
- If you previously used this Agent Proxy to collect data from your upgraded Collector, the first collection might fail because of password encryption. If the collection fails, reset the VM Host password. You can set the password for multiple hosts at the same time. Click **Administration** and select **Machines Manager > Licensed Machines > Licensed ESX/ESXi Hosts**.

Procedure

1. On your Agent Proxy machine, execute `CMAgentInstall.exe`.
2. When the installer detects the previous version of VCM and requests permission to uninstall it, select **Yes**.
3. When the installer detects that Secure Communication is installed and requests whether you want to retain your settings, select **Yes**.

   The installer removes VCM for Virtualization and the VCM Agent from your Agent Proxy machine. During this process, your Secure Communication settings are retained.
4. When the installer displays the license agreement, read and accept the conditions.
5. When the installer prompts whether to perform the installation of the VCM Windows Agent in HTTP mode, select **Allow HTTP** and click **Next**.

   Allowing HTTP communication enables the Agent to communicate through the HTTP port if DCOM is not available. Locking an Agent prevents the Agent from being removed or upgraded.
6. When the VCM Windows Agent is installed, click **Finish**.
7. Copy the Virtualization product installation executable file from your upgraded Collector machine to any location on your non-Collector Agent Proxy machine.

   The path to this file is as follows, or is in the path relative to where you installed the software.

   ```
   C:\Program Files (x86)
   \VMware\VCM\AgentFiles\Products\VirtualizationProductInstall.exe
   ```
8. On your non-Collector Agent Proxy machine, run `VirtualizationProductInstall.exe` to install VCM for Virtualization.
9. When VCM for Virtualization is installed, click **Finish**.

What to do next

Use your upgraded Agent Proxy to collect data from managed machines.

Migrating VCM

A migration to VCM 5.8 requires you to prepare new hardware and software for your environment, migrating the databases to the upgraded SQL Server, and moving the VCM files. To prepare your environment for VCM 5.8, you can choose to migrate only your databases, replace an existing 32-bit environment, migrate an existing 32-bit or 64-bit environment, or migrate a split installation.

VCM 5.8 supports the following migration paths.

- Migrate from a 32-bit or 64-bit environment that includes VCM, SCM, or ECM.
- Migrate a split installation of VCM to a single-tier, two-tier, or three-tier installation of VCM 5.8.

For a migration, you must update your hardware to 64-bit, update the operating system to the 64-bit Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system, update to SQL Server 2008 R2, 2012, or 2014, and update SQL Server Reporting Services. Then you can migrate your existing VCM, SCM, or ECM installation to your new VCM 5.8 environment.

Prerequisites

Before you migrate any part of your existing VCM environment to VCM 5.8, you must perform the prerequisites. See "Prerequisites to Migrate VCM" below.

Procedure

- "Migrate Only Your Database " on page 152

  Migrate only your VCM database from version 4.11.1 or later.

- "Replace Your Existing 32-Bit Environment with a Supported 64-bit Environment" on page 153

  Replace an existing 32-bit environment of VMware VCM, EMC Ionix SCM, or Configureoft ECM.

- "Migrate a 32-bit Environment Running VCM 5.3 or Earlier to VCM 5.8" on page 154

  Migrate an existing 32-bit Collector to VCM 5.8. A migration to VCM 5.8 requires you to prepare new hardware and software for your environment and install the required software components.

- "Migrate a 64-bit Environment Running VCM 5.3 or Earlier toVCM 5.8" on page 155

  Migrate an existing 64-bit Collector to VCM 5.8. A migration to VCM 5.8 requires you to prepare new software for your environment and install the required software components.

- "Migrate a Split Installation of VCM 5.3 or Earlier to a Single-Tier, Two-Tier, or Three-Tier Server Installation" on page 157

  Migrate an existing split installation to a single-tier, two-tier, or three-tier installation configuration for VCM 5.8.

Prerequisites to Migrate VCM

Before you migrate any part of your existing VCM environment to VCM 5.8, you must perform several prerequisite steps.

- Review and understand the migration scenarios. See "Upgrading or Migrating VCM" on page 137.
- Verify that your existing VCM installation is functional.
- Verify that your VCM Collector meets all of the hardware and software requirements for a 64-bit environment. For a complete list of requirements, see the "Software and Operating System Requirements for Collector Machines" on page 17.
- Verify that your VCM version to migrate is either VMware VCM 5.3, EMC Ionix SCM 5.0 or later, or Configuresoft ECM 4.11.1 or later.
- If your VCM Collector is installed on a 32-bit Windows machine, understand the system requirements for VCM 5.8. See "Software and Operating System Requirements for Collector Machines" on page 17.
- Verify that an existing 32-bit environment includes SQL Server 2005 and SP3.
- Verify that an existing 64-bit environment includes 64-bit SQL Server 2005 and SP2, 32-bit SQL Server Reporting Services (SSRS), and SSRS SP3. The 32-bit version of SSRS is required in 64-bit environments of VCM 5.3 and earlier.
- Verify that your environment includes the required versions of the Microsoft .NET Framework. See "Preparing for Installation" on page 19.

- Back up your databases. See "Back Up Your Databases" below.
- Back up the CMFILES$ share. See "Back up Your Files" below.
- Back up any files that you used to customize your Collector.
- Back up any reports that you exported to a non-default location.
- Back up your certificates. See "Export and Back up Your Certificates" on the next page.
- Verify that all jobs have finished running.
- Verify that no jobs are scheduled to begin during the migration process. The migration process stops the SQLAgent service, which prevents jobs from starting.
- Verify that all users have logged off of VCM.
- Ensure that users will not attempt to access VCM until you finish the migration process.
- Obtain the installation package from the Download VMware vRealize Configuration Manager Web site or the VCM 5.8 CD. You will install VCM as a final step in the migration process.
- Run the VCM Installation Manager to perform system checks on your VCM Collector to ensure that it is ready for the installation of VCM 5.8. See "Install VCM using Advanced Installation" on page 126.
- Download the VCM SQL Migration Helper Tool from the Download VMware vRealize Configuration Manager Web site to help you reconfigure scheduled jobs and membership logins in your new environment.

Back Up Your Databases

Before you migrate an existing VCM environment to VCM 5.8, back up your databases to avoid any potential loss of data.

Depending on your existing version of VCM, SCM, or ECM, or the custom names that you chose during installation, the database names differ.

Table 13–1. Back Up Your Databases Before You Start the Migration Process

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

Back up Your Files

Before you migrate an existing VCM environment to VCM 5.8, back up your files to avoid any potential loss of data.

1. Back up the entire content of the CMFILES$ share.
   - For **64-bit systems:** C:\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\, or in the path relative to where you installed the software.
   - For **32-bit systems:** C:\Program Files\VMware\VCM\WebConsole\L1033\Files\, or in the path relative to where you installed the software.

   If your VCM Collector is part of an installation of EMC Ionix SCM or Configuresoft ECM, the path differs.

2. Back up any files used to customize your Collector.
3. Back up any reports that exist in a location other than the default location.

Export and Back up Your Certificates

Export and back up your VCM Collector and Enterprise certificates.

Procedure

1. On your VCM Collector, click **Start** and click **Run**. Type `mmc`.
2. In the Console window, click **File** and select **Add/Remote Snap-in**.
3. In the Add/Remote Snap-in dialog box, click the **Standalone** tab and click **Add**.
4. In the Add Standalone Snap-in dialog box, select **Certificates** and click **Add**.
5. In the Certificates snap-in dialog box, select **Computer account** and click **Next**.
6. In the Select Computer dialog box, select **Local Computer** and click **Finish**.

   The Certificates (Local Computer) is added to the list of certificates on the Standalone tab.
7. Click **Close** to close the Add Standalone Snap-in dialog box.
8. In the Add/Remove Snap-in dialog box, click **OK**.

   The Certificates (Local Computer) is added to the Console Root.
9. Expand **Console Root** and click **Certificates** > **Personal** > **Certificates**.
10. In the right pane, right-click the Collector certificate and click **All Tasks** > **Export**.
11. On the Certificate Export Wizard Welcome page, click **Next**.
12. On the Export Private Key page, select **No** and click **Next**.
13. On the Export File Format page, select **DER encoded binary** and click **Next**.
14. On the File to Export page, type the path and name or click **Browse** to specify the location of the file on the Collector or shared location, and click **Next**.
15. On the Completing the Certificate Export Wizard page, click **Finish**.

    The `.cer` file is now in the location that you specified in the export process.

Migrate Only Your Database

Migrate only your VCM database from version 4.11.1 or later.

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.8. See "Upgrading or Migrating VCM" on page 137.
- Understand the prerequisites to migrate your VCM environment to VCM 5.8. See "Prerequisites to Migrate VCM" on page 150.
- Understand how to attach a SQL server database in SQL Server Management Studio. See the Microsoft MSDN Library.
- Install SQL Server 2008 R2, 2012, or 2014 on the Windows machine that will host the VCM database.

Procedure

1. Move the VCM database to a prepared machine that has 64-bit SQL Server 2008 R2, 2012, or 2014 installed.
2. On the prepared machine, start SQL Server Management Studio.
3. Attach the database to SQL Server.
4. Confirm that the `sa` account or the VCM service account is the owner of the newly attached database.

What to do next

Install VCM 5.8. See "Install VCM using Advanced Installation" on page 126.

Replace Your Existing 32-Bit Environment with a Supported 64-bit Environment

Replace an existing 32-bit environment of VMware VCM, EMC Ionix SCM, or Configureoft ECM.

Previous versions of VMware VCM, EMC Ionix SCM, and Configureoft ECM support older versions of SQL Server. Your 32-bit environment must include specific software components before you replace your 32-bit environment and upgrade to VCM 5.8.

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.8. See "Upgrading or Migrating VCM" on page 137
- Perform the prerequisites to migrate your VCM environment to VCM 5.8. See "Prerequisites to Migrate VCM" on page 150.
- Ensure that your environment is functional before you replace it and upgrade to VCM 5.8.

Procedure

1. Verify that your existing 32-bit installation of VCM is version 4.11.1 or later.
2. If your existing 32-bit installation is not VCM 4.11.1 or later, use the appropriate installation packages and documentation to upgrade your existing installation to version 4.11.1 or later.
3. Verify that your 32-bit environment includes the following software components.

   If these software components are not installed, install them in the order listed.

   a. SQL Server 2005
   b. SQL Server Reporting Services, 32-bit version
   c. SQL Server 2005 SP3
   d. VMware VCM 5.3, EMC Ionix SCM 5.0 or later, or Configuresoft ECM 4.11.1 or later
4. Replace your 32-bit Windows Collector machine with a 64-bit machine.
5. Install the 64-bit Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 operating system on the 64-bit Windows Collector machine.
6. Upgrade VCM to VCM 5.8.

What to do next

- Configure the SQL Server settings to tune your VCM database in SQL Server Management Studio, including the VCM database file growth and database recovery. See "Maintaining VCM After Installation" on page 161.
- Log in to VCM.

Migrate a 32-bit Environment Running VCM 5.3 or Earlier to VCM 5.8

Migrate an existing 32-bit Collector to VCM 5.8. A migration to VCM 5.8 requires you to prepare new hardware and software for your environment and install the required software components.

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

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.8. See "Upgrading or Migrating VCM" on page 137.
- Perform the prerequisite steps to migrate your VCM environment to VCM 5.8. See "Prerequisites to Migrate VCM" on page 150.
- Understand how to detach and attach a SQL server database in SQL Server Management Studio. See the online Microsoft MSDN Library.
- Understand how to use the `sp_changedbowner` stored procedure. See SQL Server Books Online in the online Microsoft MSDN Library.
- Determine if your 64-bit Collector machine is configured for Secure Sockets Layer (SSL).
- Use the SQL Migration Helper Tool to create a script for scheduled jobs on your Collector. You can then import the scheduled jobs into your 64-bit Collector.
- Use the SQL Migration Helper Tool to create a script that contains your existing login and role membership information on your Collector. You can then import your logins and roles into your 64-bit Collector.
- Locate the VCM 5.8 installation package on the Download VMware vRealize Configuration Manager Web site or obtain the VCM 5.8 CD.
- Ensure that your environment is functional before you migrate VCM 5.3 or earlier to VCM 5.8.

Procedure

1. On your 64-bit VCM Collector Windows machine, install Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
2. Install SQL Server 2008 R2, 2012, or 2014 on your 64-bit VCM Collector.
3. Stop the VCM Collector service and the VCM Patch Management service.
4. On your VCM Collector, use SQL Server Management Studio Object Explorer to detach the VCM databases.
5. On your 64-bit Collector, use SQL Server Management Studio Object Explorer to attach or restore the VCM databases to SQL Server 2008 R2, 2012, or 2014.
6. On your 64-bit Collector, verify that the owner for the restored or attached databases is set to the `sa`

account or the VCM service account.

You can use the built-in `sp_changedbowner` stored procedure to change the ownership of the databases.

7. Start the VCM 5.8 installation and select the **Install** option.

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

   When the installation begins, VCM Foundation Checker gathers information about the Collector machine. If errors occur, you must resolve them before you can proceed.

8. Make sure that you select all of the components for installation.

   If a component cannot be upgraded due to an invalid upgrade or an incomplete copy of the install image, Installation Manager clears the check box and displays a message.

9. If you plan to upgrade VCM Remote and continue to use older Agents, use the same name for the new Remote virtual directory as used in your previous installation.

   If you change the Remote virtual directory name, you must update all corresponding Agents to use the new virtual directory.

10. Select your existing databases to migrate them to VCM 5.8.

    If Installation Manager requests that you create a new database, select the previous wizard page and verify that your existing database, which you attached, is selected.

11. Do not select SSL unless your machine is already configured for SSL.

12. After the upgrade is finished, copy the content of `WebConsole\L1033\Files` from your Collector to your 64-bit Collector.

    Any existing remote commands, discovery files, and imported template files in this directory are available on the 64-bit Collector.

13. On your 64-bit Collector, run your script to import your VCM scheduled jobs.

14. On your 64-bit Collector, run your script to import your VCM membership logins.

15. Re-import any custom SQL Server Reporting Service Report Definition Language (RDL) files.

What to do next

- Configure the SQL Server settings to tune your VCM database in SQL Server Management Studio, including the VCM database file growth and database recovery. See "Maintaining VCM After Installation" on page 161.
- Log in to VCM.

Migrate a 64-bit Environment Running VCM 5.3 or Earlier toVCM 5.8

Migrate an existing 64-bit Collector to VCM 5.8. A migration to VCM 5.8 requires you to prepare new software for your environment and install the required software components.

Use this method as part of the VCM 5.8 installation process to replace the VCM hardware, change the operating system version, or install a new operating system. You install a new environment, copy the VCM databases and other components, and then install VCM 5.8. During the installation, you select the existing VCM database.

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

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.8. See "Upgrading or Migrating VCM" on page 137.
- Perform the prerequisite steps to migrate your VCM environment to VCM 5.8. See "Prerequisites to Migrate VCM" on page 150.
- Understand how to detach and attach a SQL server database in SQL Server Management Studio. See the online Microsoft MSDN Library.
- Understand how to use the `sp_changedbowner` stored procedure. See SQL Server Books Online in the online Microsoft MSDN Library.
- Determine if your 64-bit Collector machine is configured for Secure Sockets Layer (SSL).
- Use the SQL Migration Helper Tool to create a script for scheduled jobs on your existing 64-bit Collector. You can then import the scheduled jobs into your new 64-bit Collector.
- Use the SQL Migration Helper Tool to create a script that contains your existing login and role membership information on your existing 64-bit Collector. You can then import your logins and roles into your new 64-bit Collector.
- Locate the VCM 5.8 installation package on the Download VMware vRealize Configuration Manager Web site or obtain the VCM 5.8 CD.
- Ensure that your environment is functional before you migrate VCM 5.3 or earlier to VCM 5.8.

Procedure

1. On your 64-bit VCM Collector Windows machine, install Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
2. Install SQL Server 2008 R2, 2012, or 2014 on your 64-bit VCM Collector.
3. Stop the VCM Collector service and the VCM Patch Management service.
4. On your existing 64-bit VCM Collector, use SQL Server Management Studio Object Explorer to detach the VCM databases.
5. On your new 64-bit Collector, use SQL Server Management Studio Object Explorer to attach or restore the VCM databases to SQL Server 2008 R2, 2012, or 2014.
6. On your 64-bit Collector, verify that the owner for the restored or attached databases is set to the `sa` account or the VCM service account.

   You can use the built-in `sp_changedbowner` stored procedure to change the ownership of the databases.
7. Start the VCM 5.8 installation and select the **Install** option.

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

When the installation begins, VCM Foundation Checker gathers information about the Collector machine. If errors occur, you must resolve them before you can proceed.

8. Make sure that you select all of the components for installation.

   If a component cannot be upgraded due to an invalid upgrade or an incomplete copy of the install image, Installation Manager clears the check box and displays a message.

9. If you plan to upgrade VCM Remote and continue to use older Agents, use the same name for the new Remote virtual directory as used in your previous installation.

   If you change the Remote virtual directory name, you must update all corresponding Agents to use the new virtual directory.

10. Select your existing databases to migrate them to VCM 5.8.

    If Installation Manager requests that you create a new database, select the previous wizard page and verify that your existing database, which you attached, is selected.

11. Do not select SSL unless your machine is already configured for SSL.

12. After the upgrade is finished, copy the content of `WebConsole\L1033\Files` from your existing 64-bit Collector to your new 64-bit Collector.

    Any existing remote commands, discovery files, and imported template files in this directory are available on the 64-bit Collector.

13. On your 64-bit Collector, run your script to import your VCM scheduled jobs.

14. On your 64-bit Collector, run your script to import your VCM membership logins.

15. Re-import any custom SQL Server Reporting Service Report Definition Language (RDL) files.

What to do next

- Configure the SQL Server settings to tune your VCM database in SQL Server Management Studio, including the VCM database file growth and database recovery. See "Maintaining VCM After Installation" on page 161.

- Log in to VCM.

Migrate a Split Installation of VCM 5.3 or Earlier to a Single-Tier, Two-Tier, or Three-Tier Server Installation

Migrate an existing split installation to a single-tier, two-tier, or three-tier installation configuration for VCM 5.8.

In a previous split installation, the VCM databases were installed on separate Windows machines. The Collector machine hosted the `VCM_Coll` database only, and the database server machine hosted the `VCM`, `VCM_UNIX`, `ReportServer`, `master`, and `msdb` databases.

In VCM 5.8, you can migrate a previous split installation to any of the following configurations.

- "Single-Tier Server Installation" on page 35

  In a single-tier server installation, the VCM database server, Web server, and the VCM Collector components reside on a single Windows Server 2008 R2, 2012, or 2012 R2 machine, which is referred to as the VCM Collector. The installation installs all of the core VCM components, including the databases, console, and services. This configuration enables integrated security by default.

- "Two-Tier Split Installation" on page 61

In a two-tier split installation, the VCM database resides on a Windows Server 2008 R2, 2012, or 2012 R2 database server machine, and the VCM Collector and Web components reside together on a separate Windows Server 2008 R2, 2012, or 2012 R2 machine.

- "Three-Tier Split Installation" on page 91

  In a three-tier split installation, the VCM databases, the Web applications, and the VCM Collector components reside on three different Windows Server 2008 R2, 2012, or 2012 R2 machines.

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

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.8. See "Upgrading or Migrating VCM" on page 137.
- Perform the prerequisite steps to migrate your VCM environment to VCM 5.8. See "Prerequisites to Migrate VCM" on page 150.
- Understand how to detach and attach a SQL server database in SQL Server Management Studio. See the online Microsoft MSDN Library.
- Understand how to use the `sp_changedbowner` stored procedure. See SQL Server Books Online in the online Microsoft MSDN Library.
- Determine if your 64-bit Collector machine is configured for Secure Sockets Layer (SSL).
- Use the SQL Migration Helper Tool to create a script for scheduled jobs on your Collector. You can then import the scheduled jobs into your 64-bit Collector.
- Use the SQL Migration Helper Tool to create a script that contains your existing login and role membership information on your Collector. You can then import your logins and roles into your 64-bit Collector.
- Locate the VCM 5.8 installation package on the Download VMware vRealize Configuration Manager Web site or obtain the VCM 5.8 CD.
- Ensure that your environment is functional before you migrate VCM 5.3 or earlier to VCM 5.8.

Procedure

1. On your 64-bit VCM Collector Windows machine, install Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
2. Install SQL Server 2008 R2, 2012, or 2014 on your 64-bit VCM Collector.
3. Stop the VCM Collector service and the VCM Patch Management service.
4. On your VCM Collector, use SQL Server Management Studio Object Explorer to detach the VCM databases.
5. On your 64-bit Collector, use SQL Server Management Studio Object Explorer to attach or restore the VCM databases to SQL Server 2008 R2, 2012, or 2014.

   For a split installation, you must attach the databases from the database server to SQL Server 2008 R2, 2012, or 2014.
6. On your 64-bit Collector, verify that the owner for the restored or attached databases is set to the `sa`

account or the VCM service account.

You can use the built-in `sp_changedbowner` stored procedure to change the ownership of the databases.

7. Start the VCM 5.8 installation and select the **Install** option.

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

   When the installation begins, VCM Foundation Checker gathers information about the Collector machine. If errors occur, you must resolve them before you can proceed.

8. Make sure that you select all of the components for installation.

   If a component cannot be upgraded due to an invalid upgrade or an incomplete copy of the install image, Installation Manager clears the check box and displays a message.

9. If you plan to upgrade VCM Remote and continue to use older Agents, use the same name for the new Remote virtual directory as used in your previous installation.

   If you change the Remote virtual directory name, you must update all corresponding Agents to use the new virtual directory.

10. Select your existing databases to migrate them to VCM 5.8.

    If Installation Manager requests that you create a new database, select the previous wizard page and verify that your existing database, which you attached, is selected.

11. Do not select SSL unless your machine is already configured for SSL.

12. After the upgrade is finished, copy the content of `WebConsole\L1033\Files` from your Collector to your 64-bit Collector.

    Any existing remote commands, discovery files, and imported template files in this directory are available on the 64-bit Collector.

13. On your 64-bit Collector, run your script to import your VCM scheduled jobs.

14. On your 64-bit Collector, run your script to import your VCM membership logins.

15. Re-import any custom SQL Server Reporting Service Report Definition Language (RDL) files.

What to do next

- Configure the SQL Server settings to tune your VCM database in SQL Server Management Studio, including the VCM database file growth and database recovery. See "Maintaining VCM After Installation" on page 161.
- Log in to VCM.

How to Recover Your Collector Machine if the Migration is not Successful

If the migration to VCM 5.8 failed, you must perform several steps to recover your VCM Collector machine. Before you attempt another migration to VCM 5.8, contact VMware Technical Support to identify what caused the migration to fail and answer any questions about the migration procedures.

Prerequisites

- Identify the available migration options. See "Migrating VCM" on page 149.
- Understand the scenarios to migrate your VCM environment to VCM 5.8. See "Upgrading or Migrating VCM" on page 137.
- Understand the prerequisites to migrate your VCM environment to VCM 5.8. See "Prerequisites to Migrate VCM" on page 150.
- Understand how to attach a SQL server database in SQL Server Management Studio. See the Microsoft MSDN Library.

Procedure

1. On your VCM Collector, reinstall the software that was installed before you started the migration. Install the software in the order listed.
   a. SQL Server 2005
   b. SQL Server Reporting Services, 32-bit version
   c. SQL Server 2005 SP3
   d. VMware VCM 5.3, EMC Ionix SCM 5.0 or later, or Configuresoft ECM 4.11.1 or later
2. Use SQL Server Management Studio Object Explorer to connect the databases from your backed up copies.
3. Recopy the files to the `CMFILES$` share.

What to do next

Configure the SQL Server settings to tune your VCM database in SQL Server Management Studio, including the VCM database file growth and database recovery. See "Maintaining VCM After Installation" on page 161.

14 Maintaining VCM After Installation

Perform routine maintenance on your VCM configuration management database to keep VCM running smoothly and performing efficiently. Maintenance includes configuring settings specific to your environment, configuring the database file growth and recovery settings, creating a maintenance plan, and incorporating the database into your backup and disaster recovery plans.

Prerequisites

- Install VCM. See "Install VCM using Advanced Installation" on page 126.
- Understand the database recovery models. See "Database Recovery Models" on page 163.

Procedure

1. "Customize VCM and Component-Specific Settings" below

   Customize the general VCM settings and the component-specific settings for your environment.

2. "Configure Database File Growth" on page 163

   Configure the autogrowth properties of the VCM database and log file to restrict the file growth from affecting VCM performance.

3. "Configure Database Recovery Settings" on page 164

   SQL Server supports several database recovery models to control transaction log maintenance. Set a specific recovery model for each database.

4. "Create a Maintenance Plan for SQL Server" on page 164

   To ensure that VCM runs at peak performance and requires little operator intervention during its lifecycle, you must set up a routine maintenance plan. VCM relies heavily on its SQL databases for operation.

5. "Incorporate the VCM Database into Your Backup and Disaster Recovery Plans" on page 166

   Consider your VCM database as any other SQL database in your environment and incorporate the database into your corporate strategy for backup and disaster recovery.

Customize VCM and Component-Specific Settings

Customize the general VCM settings and the component-specific settings for your environment. You can customize general settings for the VCM Collector, customer information, database, input or output directories, VCM Remote, the VCM installer, auditing, and operating system patching. You can customize specific settings for installed components.

Procedure

1. In VCM, select **Administration**.
2. Click **Settings** and review the available general and product-specific configuration settings to customize for your environment.
3. Click **Windows** and configure the settings to communicate with the VCM Windows Agent for your collection types.

Option	Description
Agent - General	Configures the general characteristics of the Windows Agent operation.
Agent - Thread Priority	Configures priorities for collections while running on managed machines.
Data Retention	Configures the time to retain each VCM data type in the database.
Custom Information	Displays the Windows Custom Information script and output types.

4. Click **UNIX** and configure the settings to communicate with the VCM UNIX Agent for your collection types.

Option	Description
Agent - General	Configures the general characteristics of the UNIX Agent operation.
Agent - RunAsSuid	Configures data types as RunAsSuid for selected operating systems during Agent operation.
Agent - Nice	Configures the Nice settings for each data type during Agent operation.
Data Retention	Configures the time to retain each VCM data type in the database.
Custom Information Types	Adds custom data types and directives to collect data and parse text files.
Restricted Path	Configures restricted paths for editing file properties.

5. For the VCM functional areas and the network authority, review and update the component-specific settings for your environment.

Option	Description
Asset Extensions	Configures the hardware device and software configuration item settings.
Integrated Products	Configures settings for the VMware and EMC products that integrate with VCM.
Scripted Remediation Framework	Sets values for administrative parameters used in remediation scripts.
VCM for Active Directory	Configures the data retention settings for AD objects and the AD display settings.
VCM for Virtualization	Configures the data retention settings for vCenter Server, virtual machine hosts and guests, and the virtual machine logs.
Network Authority	Configures and manages the available domains, available accounts, and assigned accounts by domain or machine group, and the proxy servers used during the HTTP Agent installation.

What to do next

- See the online help for each product component for more information about the specific settings.
- Configure the database file growth. See "Configure Database File Growth" below.

Configure Database File Growth

Configure the autogrowth properties of the VCM database and log file to restrict the file growth from affecting VCM performance.

The VCM installer creates a 2GB data file and a 1GB log file. These files grow as ongoing operations add data to VCM.

The file growth for each file is set to the default value for Microsoft SQL Server. In some environments, these default values can result in file fragmentation or reduced performance. The following procedure sets the autogrowth property in each database.

Procedure

1. Launch**SQL Server Management Studio**.
2. Expand the SQL instance, and expand **Databases**.
3. Right-click **VCM**, select **Properties**, and in the left pane, select **Files**.
4. In the Autogrowth column, click the ellipsis button and select **Enable Autogrowth**.
5. In the File Growth area, select **In Percent** and type or select **10**.

   A value of 10% allows the transaction log file to grow by 10% of its current size. This value is critical in large environments where the log file can increase significantly even when using the Simple recovery model.

   Reserve as much space as possible for your transaction log file so that it does not ever have to grow. This configuration will result in the best performance.
6. In the Maximum File Size area, select **Unrestricted File Growth** and click **OK**.
7. Repeat this procedure for **VCM_Log**.

What to do next

Return to the database list and set the **AutoGrowth** value for all VCM related databases.

Database Recovery Models

SQL Server supports several database recovery models to control transaction log maintenance. You set a specific model to each database. The VCM database settings are set to Simple by default. Retain these settings for all VMware databases, and use the nightly full or incremental backups.

- **Simple Recovery.** The VCM database settings are set to Simple by default. The transaction log retains enough information to recover the database to a known good state when the server restarts. Transaction log backups are not allowed and point-in-time recovery is not available. Simple recovery causes the transaction log file to grow. SQL Server is in Auto Truncate mode, so the log file periodically rolls over as data moves from the log file to the data file.
- **Bulk Logged Recovery.** The transaction log retains all normal transaction information and discards transactions that result from a bulk operation. VCM uses the `IROWSETFASTLOAD` interface extensively, which is bulk logged.

- **Full Recovery.** The transaction log retains all information until it is purged through the SQL Server LOG backup operation, which the database administrator uses to perform point-in-time recovery. Full recovery allows incremental backups of the database. Do not use point-in-time recovery, because certain factors in VCM weaken the point-in-time recovery model. If you implement Full Recovery, you must set up scheduled daily backups of the transaction log. The log files will continue to grow and accumulate changes until you back them up. A Full Recovery database that does not have scheduled backups can fill its disk and stop the system.

Configure Database Recovery Settings

SQL Server supports several database recovery models to control transaction log maintenance. Set a specific recovery model for each database.

The VCM database settings are set to **Simple** by default. If you change the VCM database recovery setting to **Full**, you must manage your own log backups.

Prerequisites

- Understand the database recovery models. See "Database Recovery Models" on the previous page.

Procedure

1. Launch **SQL Server Management Studio**.
2. Expand the **SQL instance**.
3. Expand **Databases**.
4. Right-click **VCM** and select **Properties**.
5. Click **Options**.
6. In the Recovery model drop-down, select the recovery model and click **OK**.

What to do next

Create a maintenance plan for SQL Server. See "Create a Maintenance Plan for SQL Server" below.

Create a Maintenance Plan for SQL Server

To ensure that VCM runs at peak performance and requires little operator intervention during its lifecycle, you must set up a routine maintenance plan. VCM relies heavily on its SQL databases for operation.

The maintenance plan uses the automated maintenance functions on SQL Server servers that host the VCM database.

Procedure

1. Launch **SQL Server Management Studio**.
2. Expand the Management folder, right-click **Maintenance Plans** and select **Maintenance Plan Wizard**.
3. On the Maintenance Plan wizard page, click **Next**.
4. On the Select Plan Properties page, enter a maintenance plan name, select **Single schedule for the entire plan or no schedule**, and click **Change**.
5. On the Job Schedule Properties - Maintenance Plan page, set the scheduling properties to run the maintenance plan when the SQL server is idle or has low usage.
6. Click **OK** to return to the Select Plan Properties page and click **Next**.
7. On the Select Maintenance Tasks page, select the following maintenance tasks and click **Next**.

- Check Database Integrity
- Rebuild Index
- Update Statistics
- Clean Up History

8. On the Select Maintenance Task Order page, order the maintenance tasks and click **Next**.
9. On the Define Database Check Integrity Task page, define how the maintenance plan will check the database integrity.

    a. Click the Databases drop-down menu.

    b. Select the following databases and click **OK**.

    - VCM
    - VCM_Coll
    - VCM_Raw
    - VCM_UNIX

    You must select the VCM_Raw database, because it contains transient data that the other databases consume.

    c. Select **Include indexes** and click **Next**.

10. On the Define Rebuild Index Task page, define how the maintenance plan will rebuild the Index.

    a. Click the Databases drop-down menu.

    b. Select the following databases and click **OK**.

    - VCM
    - VCM_Coll
    - VCM_UNIX

    Do not rebuild the index for the VCM_Raw database.

    c. In the Advanced options area, select **Sort results in tempdb** and click **Next**.

11. On the Define Update Statistics Task page, define how the maintenance plan will update the database statistics.

    a. Click the Databases drop-down menu.

    b. Select the following databases and click **OK**.

    - VCM
    - VCM_Coll
    - VCM_UNIX

    Do not update statistics for the VCM_Raw database.

12. On the Define History Cleanup Task page, define how the maintenance plan will clean up historical data from the SQL Server machine and click **Next**.

   a. Select **Backup and restore history**.
   b. Select **SQL Server Agent job history**.
   c. Select **Maintenance plan history**.
   d. Set the cleanup task to remove historical data older than **4 Months**.

13. On the Select Report Options page, save a report of the maintenance plan actions.
   a. Select **Write a report to a text file**.
   b. Select a folder for the report and click **Next**.
14. On the Complete the Wizard page, verify your selections in the Maintenance Plan Wizard summary, expand the selections to view the settings, and click **Finish**.
15. When the Maintenance Plan Wizard progress is finished, verify that each action is successful.

What to do next

- You have established a routine maintenance plan to ensure that SQL Server continues to operate efficiently. To view, save, copy, or send the report, click **Report** and select an option.
- Use VCM normally.

Incorporate the VCM Database into Your Backup and Disaster Recovery Plans

Consider your VCM database as any other SQL database in your environment and incorporate the database into your corporate strategy for backup and disaster recovery.

Hardware and Operating System Requirements for VCM Managed Machines

15

VCM collects data from Windows and UNIX machines that VCM manages. The VCM Agent is supported on many different machine and operating system types.

This chapter includes the following topics:

VCM Agent Support on Non-English Windows Platforms

If you install the VCM Agent on non-English (non-ENU) Windows machines, and collect data from these machines, review the following dependencies and limitations.

- You might need additional language packs on Windows machines where VCM administrators run the VCM Web console interface to display non-western data that VCM collects from these machines.
- Non-English versions of Microsoft patches in Spanish, French, and Danish are currently supported.
- Compliance rules that refer to Services must use the internal names rather than the display names, because the display names might be localized.

VCM Managed Machine Requirements

VCM can manage various machines and operating systems. The table below lists the supported VCM Agents, operating system, and hardware platforms.

If the list of supported machines and operating systems does not include your specific combination of platform and operating system, contact VMware Technical Support to confirm whether your configuration is supported by a later version of VCM.

Machines that are noted with a specific Agent version are supported with the Agent version listed. For machines that are noted with support up to the a certain Agent version, you could install an earlier version of the Agent on these platforms, but you cannot install a newer Agent, which means that you cannot use the latest features on those machines. Contact VMware Technical Support for previously supported Agents.

The following x64 platforms are tested.

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

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

Machines marked with an asterisk (*) include a pre-VCM 5.6 Agent and might not report the name of the operating system correctly. You should upgrade the Agents on these machines.

Table 15–1. Agent Operating System and Hardware Requirements

Agent	Supported Operating System	Supported Hardware Platform	Platforms To Be Upgraded
Windows	Microsoft Windows Server 2003 SP2	x86 and x64	
	Microsoft Windows Server 2003 R2 SP2	x86 and x64	
	Microsoft Vista Business (Gold and SP1)	x86 and x64	
	Microsoft Vista Ultimate (Gold and SP1)	x86 and x64	
	Microsoft Vista Enterprise (Gold and SP1)	x86 and x64	
	Microsoft Vista Business SP2	x86 and x64	
	Microsoft Vista Ultimate SP2	x86 and x64	
	Microsoft Vista Enterprise SP2	x86 and x64	
	Microsoft Windows Server 2008 Standard (Gold and SP1)	x86 and x64	
	Microsoft Windows Server 2008 Datacenter (Gold and SP1)	x86 and x64	
	Microsoft Windows Server 2008 Enterprise (Gold and SP1)	x86 and x64	
	Microsoft Windows Server 2008 Standard SP2	x86 and x64	
	Microsoft Windows Server 2008 Datacenter SP2	x86 and x64	
	Microsoft Windows Server 2008 Enterprise SP2	x86 and x64	
	Microsoft Windows Server 2008 R2 Standard Gold	x64	
	Microsoft Windows Server 2008 R2 Datacenter Gold	x64	
	Microsoft Windows Server 2008 R2 Enterprise Gold	x64	
	Microsoft Windows Server 2008 R2 Standard SP1	x64	
	Microsoft Windows Server 2008 R2 Datacenter SP1	x64	
	Microsoft Windows Server 2008 R2 Enterprise SP1	x64	
	Microsoft Windows 7 Business Gold	x86 and x64	

Agent	Supported Operating System	Supported Hardware Platform	Platforms To Be Upgraded
	Microsoft Windows 7 Ultimate Gold	x86 and x64	
	Microsoft Windows 7 Enterprise Gold	x86 and x64	
	Microsoft Windows 7 Business SP1	x86 and x64	
	Microsoft Windows 7 Ultimate SP1	x86 and x64	
	Microsoft Windows 7 Enterprise SP1	x86 and x64	
	Microsoft Windows 8 Pro	x86 and x64	*
	Microsoft Windows 8 Enterprise	x86 and x64	*
	Microsoft Windows 8.1 Pro	x86 and x64	*
	Microsoft Windows 8.1 Enterprise	x64	*
	Microsoft Windows Server 2012 Datacenter	x64	*
	Microsoft Windows Server 2012 Standard	x64	*
	Microsoft Windows Server 2012 Essentials	x64	*
	Microsoft Windows Server 2012 R2 Datacenter	x64	*
	Microsoft Windows Server 2012 R2 Standard	x64	*
	Microsoft Windows Server 2012 R2 Essentials	x64	*
Linux and UNIX	AIX 6L, 6.1, 7.1	RISC and PowerPC	
	CentOS 5.0–5.11, 6.0–6.5, and 7.0 (x64)	x86 and x64	
	ESX 4.1, 4.1 Update 1 ESXi 4.1, 4.1 Update 1, Update 2, Update 3 ESXi 5.0, 5.0 Update 1 ESXi 5.1		
	HP-UX 11i v2.0 (11.23) (up to 5.4 Agent only)	Itanium	
	HP-UX 11i v3.0 (11.31)	Itanium	
	Oracle Enterprise Linux (OEL) 5.0–5.11, 6.0–6.5, and 7.0 (x64)	x86 and x64	
	Red Hat Enterprise Linux 5.0–5.11, 6.0–6.5, and 7.0 (x64) Server, Desktop with Workstation, and Advanced Platform	x86 and x64	
	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	

Agent	Supported Operating System	Supported Hardware Platform	Platforms To Be Upgraded
	Solaris 11 (Not supported for Patching)	SPARC, SPARC-V9, x86, and x64	
	SUSE Linux Enterprise Server (SLES) 10.0–10.2 (up to 5.5.0 Agent only) SUSE Linux Enterprise Server (SLES) 10.3–10.4, 11.0–11.3	x86 and x64	
Mac OS X (Servers and Workstations)	Mac OS X 10.6 (up to 5.5.0 Agent only) Mac OS X 10.7 and 10.8	Intel-based Apple platforms only	
Active Directory	Microsoft Windows Server 2003	x86 and x64	
	Microsoft Windows Server 2003 R2	x86 and x64	
	Microsoft Windows Server 2008	x86 and x64	
	Microsoft Windows Server 2008 R2	x64	
	Microsoft Windows Server 2012	x64	
	Microsoft Windows Server 2012 R2	x64	
VCM Remote	Supports the same platforms as the VCM Windows Agent.		

Linux, UNIX, and Mac OS Agent Files

VCM Linux, UNIX, and Mac OS Agent files are architecture specific. When you install the Agent using VCM, the target operating systems are evaluated and the corresponding Agent is installed. If you are manually installing the Agent on the target machine, you must ensure that you use to correct Agent binary packages.

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

Table 15–2. VCM Linux, UNIX, and Mac OS Agent Files

Operating System Version	Agent Binary
Red Hat Enterprise Linux 5.0–5.11, 6.0–6.5, and 7.0 SUSE Linux Enterprise Server 10.0–10.4, 11.0–11.3 Oracle Enterprise Linux (OEL) 5.0–5.11, 6.0–6.5, and 7.0 CentOS 5.0–5.11, 6.0–6.5, and 7.0	`CMAgent.5.8.0.Linux`
Solaris 10 and 11 for SPARC	`CMAgent.5.8.0.SunOS`
Solaris 10 and 11 for x86	`CMAgent.5.8.0.SunOS.x86.5.10`
HP-UX 11i 1.0 and 2.0 (11.11 and 11.23 for PA-RISC)	`CMAgent.5.4.0.HP-UX.11.pa`
HP-UX 11i 3.0 (11.31 for PA-RISC)	`CMAgent.5.7.0.HP-UX.11.pa`
HP-UX 11i 2.0 (11.23 for Itanium)	`CMAgent.5.4.0.HPUX.11.ia64`

Operating System Version	Agent Binary
HP-UX 11i 3.0 (11.31 for Itanium)	`CMAgent.5.8.0.HPUX.11.ia64`
AIX 6L, 6.1, 7.1	`CMAgent.5.8.0.AIX.5`
Mac OS X 10.6	`CMAgent.5.5.0.Darwin`
Mac OS X 10.7, 10.8	`CMAgent.5.8.0.Darwin`

Windows Custom Information Supports PowerShell 2.0

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

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

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

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

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

For more information, see the *VCM Administration Guide*.

Linux and UNIX Patch Assessment and Deployment Requirements

VCM 5.8 supports UNIX patch assessments and deployments for various machine types and operating systems. The PLS files used for UNIX patch assessments require 20MB of disk space.

Table 15–3. Linux and UNIX Patch Assessment and Deployment Operating System and Hardware Requirements

Supported Operating System	Supported Hardware
AIX 6.1	RISC and PowerPC
AIX 7.1	RISC and PowerPC
HP-UX 11i v2.0 (11.23) (up to 5.4 Agent only)	Itanium
HP-UX 11i v3.0 (11.31)	Itanium
Mac OS X 10.6 (up to 5.5.0 Agent only)	Intel-based Apple platforms only
Mac OS X 10.7, 10.8	Intel-based Apple platforms only
Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 7.0 (x64), Server, Desktop with Workstation, and Advanced Platform	x86 and x64 (includes Intel and AMD architectures, excludes Itanium)

Supported Operating System	Supported Hardware
Solaris 10	SPARC, SPARC-V9, x86, and x64
SUSE Linux Enterprise Server (SLES) 10.0–10.2 (up to 5.5.0 Agent only) SUSE Linux Enterprise Server (SLES) 10.3–10.4, 11.0–11.3	x86 and x64 (includes Intel and AMD architectures, excludes Itanium)

VCM 5.8 provides UNIX patch assessment content in a new format for the following operating systems.

- Red Hat RHEL 5 and 6
- SUSE SLES 10.0–10.4 and 11.0–11.3

For information about the new content format, see the *VCM Administration Guide* or the VCM online help.

Support for VMware Cloud Infrastructure

Use VCM to collect data from vCenter Server, vCloud Director, and vShield Manager. The collection runs on the supported platforms using the VMware API/SDK through a Managing Agent.

To collect ESX Linux Data Types from the ESX Service Console OS, including ESX Logs, you use an Agent Proxy.

Cloud and Virtualization Infrastructure Platforms

Use the VMware product interoperability matrix to determine the cloud and virtualization infrastructure platforms from which VCM can collect. See partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php.

Managing Agent Requirements

To collect virtual environments data, you use Managing Agent machines. A Managing Agent is a Windows machine running Windows 7, 64-bit, or Windows Server 2008, 64-bit.

Agent Proxy Requirements for VMware ESX and ESXi

To collect ESX Service Console OS Linux data types, including ESX logs, you use an Agent Proxy rather than installing the VCM Agent directly on the ESX Servers.

When collecting data from ESX 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 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 the following criteria.

- 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 for Agent Proxy Machines

The Agent Proxy machine must be running Windows Server 2008 R2, 2012, 2012 R2, or Windows Server 2003 SP2. For more information to install and configure the Agent Proxy, see the *VCM Administration Guide*.

Minimum Hardware Requirements for Agent Proxy Machines

The Agent Proxy is installed on the Collector by default. Although the 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 for Virtualization Agent Proxy

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

Virtual Requirements for Virtualization Agent Proxy

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

vRealize Operations Manager Integration Features

You can configure the following versions vRealize Operations Manager with VCM 5.8. Different integrated versions of vRealize Operations Manager support different features.

Table 15–4. vRealize Operations Manager Integration

vRealize Operations Manager Version	VCM Features in vRealize Operations Manager
5.0.x	VCM change events
5.6, 5.7, 5.8.x, 6.x	VCM change events, compliance template results, and machine groups

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 15–5. 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 Server 2003	SP2	x86 and 64-bit	875
Windows Server 2003	SP1	x86 and 64-bit	382
Windows Server 2003	SP1	x86 and 64-bit	381
Windows Server 2003	Gold	x86 and 64-bit	382
Windows Server 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
Windows 2000	All	x86	103
Windows Server 2008	1	x86 and 64-bit; Itanium is not supported.	See "Cryptographic RSA Enhanced Validated Modules" below and "Cryptographic DSS Enhanced Validated Modules" on page 175.
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 15–6. 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

RSAENH Validated Operating Systems	Validated Versions (Links to Security Policy)	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	#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 15–7. 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
Windows Server 2008	6.0.6001.18000	#1009	140–2

FIPS for VCM Agent Proxies

The VCM Agent Proxy uses the validation OpenSSL FIPS Object Module v2.0, FIPS 140-2 certificate #1747.

Agent Sizing Information

The disk space requirements are fairly constant for a Windows, UNIX, Linux, Mac OS X, or AD managed machine that runs a VCM Agent. Each machine requires no more than 200MB to run an Agent. However, the recommended memory to run the HP-UX Agent is 1GB.

The following information identifies the data files for default collections only. A 20MB overlap exists between the Agent Proxy Agent and the Active Directory Agent when both Agents are installed on the same machine.

Use the following information as a general guideline. Factors such as the types of data collected can affect the sizing. VMware makes every effort to validate the numbers but cannot guarantee that the quoted sizing information is accurate for all installations.

Windows Machines

For several components, the projected data file sizing information can vary. The data file size is the estimated amount after an initial data collection using the default filter set.

Table 15–8. Windows Agents and Component File Sizes

Agent Type	Installed File Size	Data File Size	Projected Data File Size
VCM Agent used as Managing Agent This default Agent includes Extension for Provisioning and Managing Agent.	130–135MB	200MB–1GB	The projected data file sizing information can vary depending on the size of your vCenter Server instances and the number of hosts and guests.
Agent Proxy for Virtualization	VCM Agent +40MB	See VCM Agent data file sizes	The projected data file size is determined the same as the default Agent.
VCM Agent used for Provisioning This default Agent includes Extension for Provisioning and Managing Agent.	130–135MB	10–20MB	The projected data file sizing information can vary depending on your collection filter set, and is determined by collected data types and actions. The size can vary from 10–20MB to more than 100MB. The File System-File Structure and System Logs data types can cause large data growth.
VCM Agent without Extension for Provisioning	70–76MB	10–20MB	The projected data file size is determined the same as the default Agent.
Active Directory Agent	VCM Agent +30MB	See VCM Agent data file sizes	The projected data file size is determined the same as the default Agent.
VCM Remote Client	VCM Agent +2MB (installs or upgrades Agent)	See VCM Agent data file sizes	The projected data file size is determined the same as the default Agent.
Patching Agent	VCM Agent +2MB	See VCM Agent data file sizes	The projected data file size is determined the same as the default Agent.

Agent Type	Installed File Size	Data File Size	Projected Data File Size
Package Manager (installed with VCM Agent Extension for Provisioning), which includes the database and cratecache.	Package Manager 4MB Database 140KB Cratecache 0MB	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 Software Repository. Increased size is based on the number of installed packages and the size of the packages, and 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.

Linux and UNIX Machines

The projected data file sizing information for Linux and UNIX machines information can vary depending on your collection filter set and is determined by collected data types and actions. 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.

The data file size is the estimated amount after an initial data collection with the default filter set.

Table 15–9. Linux and UNIX Agents File Sizes

Agent Type	Installed File Size	Data File Size
CMAgent.5.7.0.AIX.5	60–80MB	5–20MB
CMAgent.5.4.0.HP-UX.11.pa	120–125MB	45MB
CMAgent.5.7.0.HP-UX.11.pa	80MB	5–16MB
CMAgent.5.4.0.HP-UX.11.ia64	120–125MB	45MB
CMAgent.5.7.0.HP-UX.11.ia64	80MB	5–16MB
CMAgent.5.7.0.Linux	30–50MB	5–70MB

Agent Type	Installed File Size	Data File Size
CMAgent.5.7.0.SunOS	80–90MB	25MB
CMAgent.5.7.0.SunOS.x86.5.10	80–90MB	35MB

Mac OS X Machines

The projected data file sizing information for Mac OS X machines can vary depending on your collection filter set and is determined by collected data types and actions. 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.

The data file size is the estimated amount after an initial data collection with the default filter set.

Table 15–10. Mac OS X Agent File Sizes

Agent Type	Installed File Size	Data File Size
CMAgent.5.7.0.Darwin	120MB	40MB

Index