VMware vCenter Configuration Manager Installation Guide
vCenter Configuration Manager 5.5

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

Updated Information 9

About This Book 11

Achieving a Successful VCM Installation 13
  Agent and Collector OS Platform Support 13
  VCM Agent Support on Non-English Windows Platforms 13

Hardware Requirements for Collector Machines 15
  Determine the Size of Your Environment 15
  Identify Your Specific Hardware Requirements 16
    Database Sizing for Managed vCenter Server Instances 16
    Hardware and Disk Requirements By Number of Managed Machines 17

Software and Operating System Requirements for Collector Machines 19
  Sizing Impacts on Software Requirements 19
  Software Installation and Configuration Overview 19
  VCM Upgrades and Migrations 20

Preparing for Installation 21
  File System Permissions 21
  VCM Installation Configurations 22

System Prerequisites to Install VCM 23
  Establish Local Administration Rights 24
  Verify Browser Compatibility 25
  Verify the Default Network Authority Account 25
  Specify the Collector Services Account 26
  Verify the VMware Application Services Account 26
  Verify the VCM Agent is Not Installed 27
  Verify the SQLXML Version 28

Configure Resources to Install VCM on a Virtual Machine 29
  Configure the Disk to Install VCM on a Virtual Machine 30
  Configure the CPU to Install VCM on a Virtual Machine 30
  Configure the Memory to Install VCM on a Virtual Machine 31

Secure Communications Certificates 33
  Authenticating the Server to the Client 33
    Enterprise and Collector Certificates 34
    Delivering Initial Certificates to Agents 34

Single-Tier Server Installation 37
  Configure a Single-Tier Installation Environment 39
  Verify that the Installing User is an Administrator 40
  Install and Configure a Windows Server 2008 R2 Operating System 41
    Configure the Operating System Locale Settings 42
    Disable the Remote Desktop Session Host 42
Enable DCOM
Install the .NET Framework
  Verify the ASP.NET Client System Web Version
  Verify the ASP Role Service
  Verify ASP.NET Role Service
Configuring the Database Components of the VCM Collector
  Set the Internet Explorer Enhanced Security Mode
  Install SQL Server on the VCM Collector
  Verify and Configure the SQL Server Properties
  Verify Matching SQL Server and Computer Names
  Verify the SQL Server Agent Service Account is a sysadmin
  Select the SQL Server Agent Service Account
  Establish SQL Server Administration Rights
Configure the Web Components
  Configuring IIS
  Verify the ISAPI Extensions
Configure SSRS on the VCM Collector
  Back Up Your SSRS Key
  Disable IE Protected Mode for SSRS
  Configure SSRS
  Configure Kerberos Authentication
  Configure the VCM Collector Components

Two-Tier Split Installation
  Configuring a Two-Tier Split Installation Environment
  Verify that the Installing User is an Administrator
  Install and Configure a Windows Server 2008 R2 Operating System
    Configure the Operating System Locale Settings
    Disable the Remote Desktop Session Host
    Enable DCOM
  Configuring the VCM Database Server
    Set the Internet Explorer Enhanced Security Mode
    Install SQL Server on the Database Server
    Verify and Configure the SQL Server Properties
    Verify Matching SQL Server and Computer Names
    Verify the SQL Server Agent Service Account is a sysadmin
    Select the SQL Server Agent Service Account
    Establish SQL Server Administration Rights
  Configure the Combined VCM Collector and Web Server
    Install the .NET Framework
    Configure the Web Components
    Installing and Configuring SSRS on the Combined VCM Collector and Web Server
    Configure Kerberos Authentication
    Configure the VCM Collector Components

Three-Tier Split Installation
  Configuring a Three-Tier Split Installation Environment
  Verify that the Installing User is an Administrator
  Install and Configure a Windows Server 2008 R2 Operating System
    Configure the Operating System Locale Settings
    Disable the Remote Desktop Session Host
    Enable DCOM
  Configuring the VCM Database Server
    Set the Internet Explorer Enhanced Security Mode
    Install SQL Server on the Database Server
    Verify and Configure the SQL Server Properties
    Verify Matching SQL Server and Computer Names
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the SQL Server Agent Service Account is a sysadmin</td>
<td>95</td>
</tr>
<tr>
<td>Select the SQL Server Agent Service Account</td>
<td>96</td>
</tr>
<tr>
<td>Establish SQL Server Administration Rights</td>
<td>97</td>
</tr>
<tr>
<td>Configure the Web Server</td>
<td>97</td>
</tr>
<tr>
<td>Configuring IIS</td>
<td>99</td>
</tr>
<tr>
<td>Verify the ISAPI Extensions</td>
<td>101</td>
</tr>
<tr>
<td>Place the Web Server in the Internet Explorer Trusted Zone</td>
<td>101</td>
</tr>
<tr>
<td>Access to Patch Download Folder for Windows Patch Deployment</td>
<td>102</td>
</tr>
<tr>
<td>Installing and Configuring SSRS on the Web Server</td>
<td>103</td>
</tr>
<tr>
<td>Configure Kerberos Authentication</td>
<td>108</td>
</tr>
<tr>
<td>Modify the SQLCMD Path Variable</td>
<td>111</td>
</tr>
<tr>
<td>Configure the VCM Collector</td>
<td>112</td>
</tr>
<tr>
<td>Install the .NET Framework</td>
<td>112</td>
</tr>
<tr>
<td>Using VCM Remote</td>
<td>114</td>
</tr>
<tr>
<td>Installing VCM</td>
<td>117</td>
</tr>
<tr>
<td>DCOM and Port Requirements for VCM</td>
<td>117</td>
</tr>
<tr>
<td>Use Installation Manager to Install VCM</td>
<td>117</td>
</tr>
<tr>
<td>Install VCM</td>
<td>118</td>
</tr>
<tr>
<td>Change Permissions On Machine Certificate Keys</td>
<td>119</td>
</tr>
<tr>
<td>Verify VCM Remote Virtual Directory Permissions</td>
<td>120</td>
</tr>
<tr>
<td>Configuring SQL Server for VCM</td>
<td>121</td>
</tr>
<tr>
<td>SQL Server Database Settings</td>
<td>121</td>
</tr>
<tr>
<td>SQL Server Processor Settings</td>
<td>122</td>
</tr>
<tr>
<td>SQL Server IO Configuration</td>
<td>122</td>
</tr>
<tr>
<td>Using the RAID Levels with SQL Server</td>
<td>123</td>
</tr>
<tr>
<td>Disk Interface and Disk Drive Performance</td>
<td>124</td>
</tr>
<tr>
<td>Use SQLIO to Determine IO Channel Throughput</td>
<td>125</td>
</tr>
<tr>
<td>Upgrading or Migrating VCM</td>
<td>127</td>
</tr>
<tr>
<td>Upgrades</td>
<td>127</td>
</tr>
<tr>
<td>Migrations</td>
<td>127</td>
</tr>
<tr>
<td>Prerequisites to Migrate VCM</td>
<td>128</td>
</tr>
<tr>
<td>Back Up Your Databases</td>
<td>129</td>
</tr>
<tr>
<td>Back up Your Files</td>
<td>129</td>
</tr>
<tr>
<td>Export and Back up Your Certificates</td>
<td>129</td>
</tr>
<tr>
<td>Migrating VCM</td>
<td>130</td>
</tr>
<tr>
<td>Migrate Only Your Database</td>
<td>130</td>
</tr>
<tr>
<td>Replace Your Existing 32-Bit Environment with a Supported 64-bit Environment</td>
<td>131</td>
</tr>
<tr>
<td>Migrate a 32-bit Environment Running VCM 5.3 or Earlier to VCM 5.6</td>
<td>132</td>
</tr>
<tr>
<td>Migrate a 64-bit Environment Running VCM 5.3 or Earlier to VCM 5.6</td>
<td>134</td>
</tr>
<tr>
<td>Migrate a Split Installation of VCM 5.3 or Earlier to a Single-Server Installation</td>
<td>135</td>
</tr>
<tr>
<td>How to Recover Your Collector Machine if the Migration is not Successful</td>
<td>138</td>
</tr>
<tr>
<td>Upgrading VCM and Components</td>
<td>138</td>
</tr>
<tr>
<td>Upgrade VCM</td>
<td>139</td>
</tr>
<tr>
<td>Upgrade Existing Windows Agents</td>
<td>140</td>
</tr>
<tr>
<td>Upgrade Existing VCM Remote Clients</td>
<td>141</td>
</tr>
<tr>
<td>Upgrade Existing UNIX Agents</td>
<td>141</td>
</tr>
<tr>
<td>Red Hat Server and Workstation Licensing</td>
<td>142</td>
</tr>
<tr>
<td>Upgrade UNIX Agents Using a Local Package</td>
<td>142</td>
</tr>
<tr>
<td>Upgrade UNIX Agents Using a Remote Package</td>
<td>143</td>
</tr>
<tr>
<td>Upgrade Virtual Environments Collections</td>
<td>144</td>
</tr>
<tr>
<td>Upgrade Agent Proxy Machines</td>
<td>144</td>
</tr>
<tr>
<td>Use VCM to Upgrade an Agent Proxy Machine</td>
<td>145</td>
</tr>
<tr>
<td>Manually Upgrade an Agent Proxy Machine</td>
<td>146</td>
</tr>
<tr>
<td>Unregister the Previous Version of the vSphere Client VCM Plug-In</td>
<td>147</td>
</tr>
</tbody>
</table>
Upgrade the vSphere Client VCM Plug-In 147

Maintaining VCM After Installation 149
  Customize VCM and Component-Specific Settings 149
  Database Recovery Models 151
  Configure Database File Growth 151
  Configure Database Recovery Settings 152
  Create a Maintenance Plan for SQL Server 2008 R2 153
  Incorporate the VCM CMDB into your Backup and Disaster Recovery Plans 155

Hardware and Operating System Requirements for VCM Managed Machines 157
  VCM Managed Machine Requirements 157
  Windows Custom Information Supports PowerShell 2.0 159
  Supported OS Provisioning Target Systems 160
  Software Provisioning Requirements 160
  UNIX and Linux Patch Assessment and Deployment Requirements 161
  Support for VMware Cloud Infrastructure 163
    Cloud and Virtualization Infrastructure Platforms 163
    Managing Agent Requirements 163
    Agent Proxy Requirements for VMware ESX and ESXi 163
  FIPS Requirements 164
    FIPS for Windows 164
    FIPS for VCM Agent Proxies 166
  Agent Sizing Information 167
    Windows Machines 167
    UNIX and Linux Machines 168
    Mac OS X Machines 169

Hardware and Software Requirements for the Operating System Provisioning Server 171
  Supported OS Provisioning Server Platform 171
  OS Provisioning Server System Requirements 171
  OS Provisioning Server Software Requirements 172
    Required Packages 172
    Disallowed Packages 172
  OS Provisioning Server Network Requirements 172
    Provisioning Network Interface 172
    Configure the OS Provisioning Server Firewall 173

Installing, Configuring, and Upgrading the OS Provisioning Server and Components 175
  Restricted Network Environment 175
  Install and Configure the OS Provisioning Server 175
    Install the Operating System Provisioning Server 176
    Uninstall the OS Provisioning Server 177
    Configure DHCP 178
    Configure a DHCP Server Other Than the OS Provisioning Server 179
    Configure TFTP 179
    Create a Windows Boot Image 180
    Copy the VCM Certificate to the OS Provisioning Server for Linux Provisioning 181
  Import Distributions into the OS Provisioning Server Repository 182
    Create Directories for Windows Distributions 182
    Import Windows Distributions 183
    Import Linux Distributions 185
    Using the basicimport Command Options 186
  Working with Custom Linux ISO Distributions 187
  Upgrade the OS Provisioning Server to 5.5 187
  Managing the OS Provisioning Server System Logs 189
  ospctrl Command Options 190
Index
Updated Information

VCM Installation Guide was updated with the 5.5.1 release of the product. Unless identified as 5.5 or 5.5.1 only, the information provided applies to VCM 5.5 and 5.5.1.

This table provides the update history of the VCM Installation Guide.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- &quot;Two-Tier Split Installation&quot; on page 61 updated to add install of SSRS on the Web server. Updated description of VCM support for Active/Passive SQL clusters. Updated SQL Server Agent Service Account procedure to add Agent in SQL Server Agent (MSSQLSERVER). Updated description of VCM support for SSRS on Web server or DB server in Install SQL Server on the Database Server.</td>
</tr>
<tr>
<td></td>
<td>- &quot;Three-Tier Split Installation&quot; on page 87 updated to add install of SSRS on the Web server. Updated description of VCM support for Active/Passive SQL clusters. Updated SQL Server Agent Service Account procedure to add Agent in SQL Server Agent (MSSQLSERVER). Updated description of VCM support for SSRS on Web server or DB server in Install SQL Server on the Database Server.</td>
</tr>
<tr>
<td>EN-000675-01</td>
<td>- &quot;Identify Your Specific Hardware Requirements&quot; on page 16 update to include VMware knowledge base reference for two-tier and three-tier hardware and disk requirements sizing recommendations.</td>
</tr>
<tr>
<td></td>
<td>- &quot;Preparing for Installation&quot; on page 21 reorganized to support tasks to install VCM.</td>
</tr>
<tr>
<td></td>
<td>- &quot;File System Permissions&quot; on page 21 added to support users who install VCM.</td>
</tr>
<tr>
<td></td>
<td>- &quot;System Prerequisites to Install VCM&quot; on page 23 reorganized to better support single-tier, two-tier, and three-tier installation configurations.</td>
</tr>
<tr>
<td>Revision</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>&quot;Single-Tier Server Installation&quot;</strong> on page 37 reorganized to support tasks to install VCM.</td>
</tr>
<tr>
<td></td>
<td>Configure Basic Authentication on the Report Server added to support single-tier installations.</td>
</tr>
<tr>
<td></td>
<td><strong>&quot;Two-Tier Split Installation&quot;</strong> on page 61 reorganized to support tasks to install VCM.</td>
</tr>
<tr>
<td></td>
<td><strong>&quot;Three-Tier Split Installation&quot;</strong> on page 87 reorganized to support tasks to install VCM.</td>
</tr>
<tr>
<td></td>
<td><strong>&quot;Access to Patch Download Folder for Windows Patch Deployment&quot;</strong> on page 102 added to support three-tier installation configurations.</td>
</tr>
<tr>
<td>EN-000675-00</td>
<td><strong>&quot;VCM Managed Machine Requirements&quot;</strong> on page 157 updated to include Red Hat Enterprise Linux 5.8 and 6.3. These versions of Red Hat are supported in VCM 5.5 and 5.5.1.</td>
</tr>
<tr>
<td></td>
<td><strong>&quot;Support for VMware Cloud Infrastructure&quot;</strong> on page 163 updated to include VCM 5.5.1 support for vSphere 5.1, vCenter Server 5.0 Update 1a and 5.1, ESXi 5.1, vCloud Director 5.1, and vShield 5.1. vCloud Director 1.0.1 is supported only with VCM 5.5, not 5.5.1.</td>
</tr>
<tr>
<td></td>
<td>Initial VCM 5.5 release.</td>
</tr>
</tbody>
</table>
About This Book

The VCM Installation Guide describes the hardware and software requirements necessary for a successful VMware vCenter Configuration Manager (VCM) installation, and the steps to install VCM in all supported installation configurations.

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
- Hardware and software requirements for the OS Provisioning Server

Read this document and follow the procedures to successfully install VCM.

The VCM Installation Guide applies to VCM 5.6, Foundation Checker 5.6, and Service Desk Connector 1.3.0.

Intended Audience

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

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

Document Feedback

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

VMware VCM Documentation

The vCenter Configuration Manager (VCM) documentation consists of the VCM Installation Guide, VCM Administration 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

Perform the requirements to successfully install VMware vCenter 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 vCenter 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, 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?
- What additional VCM components will you use? See the Download VMware vCenter Configuration Manager Web site for available VCM components.
- Do you understand the VCM security requirements? See the VCM Security Guide on the Download VMware vCenter Configuration Manager Web site.

Before you install VCM, perform the tasks and procedures in the order presented.

Agent and Collector OS Platform Support

All Agent and Collector OS platform support is specific to versions and editions indicated in the supported platforms table. Some configurations can reduce or block the performance or functionality of VCM components, such as configurations by vendors, third-party, custom lock downs, endpoint security products, policies, and restricted system. Troubleshooting and support of VCM components in locked-down or reconfigured environments is not included under the standard product maintenance agreement. Support in these environments is available through an additional Professional Services engagement.

See "Hardware and Operating System Requirements for VCM Managed Machines" on page 157. All tested installations use the vendor’s default configuration except as noted.

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.

**What to do next**

Determine the hardware requirements for the VCM Collector machine. See "Hardware Requirements for Collector Machines" on page 15.
Hardware Requirements for Collector Machines

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

Use this information to determine how many machines you plan to manage. You can determine the individual hardware requirements to ensure a successful VCM installation.

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**

VCM hardware requirements are recommended based on whether your environment contains 1–1000, 1000–2000, 2000–5000, or more managed machines. To determine the number of managed machines on which to base your collector size, consider the number of vCenter instances, Windows servers and workstations, UNIX or Linux 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 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 definition includes AD objects that you plan to have in your environment in the next 12 to 24 months.

Use the formulas in the worksheets to determine how your AD objects will increase your managed machine count and affect your final sizing requirements. After you complete the worksheet and determined the number of managed machines, size your Collector machine. Use the blank worksheet to record the managed machines in your environment.
<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
<th>Anticipated Number of Managed Machines in the Next 12-24 Months</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCM</td>
<td>Windows Servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi Servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Virtual Machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Workstations</td>
<td></td>
</tr>
<tr>
<td>VCM</td>
<td>Divide total number of AD objects by 100 to determine the</td>
<td></td>
</tr>
<tr>
<td>for AD</td>
<td>approximate &quot;machine count&quot; for your AD environment.</td>
<td></td>
</tr>
</tbody>
</table>

**Total Managed Machines:** _____

In the following example, an enterprise environment contains machines and objects that represent 1177 managed machines, which places it in the 1000–2000 managed machines category.

**Table 2–2. Example of Sizing Worksheet with Sample Data**

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
<th>Anticipated Number of Managed Machines in the Next 12-24 Months</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCM</td>
<td>Windows Servers</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>vSphere/ESX/ESXi Servers</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Virtual Machines (VM)</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Windows Workstations</td>
<td>920</td>
</tr>
<tr>
<td>VCM</td>
<td>Divide total number of AD objects by 100 to determine the</td>
<td></td>
</tr>
<tr>
<td>for AD</td>
<td>approximate &quot;machine count&quot; for your AD environment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10,000 AD Objects/100 = 100 managed machines to accommodate VCM for AD</td>
<td></td>
</tr>
</tbody>
</table>

**Total Managed Machines:** 1177

**What to do next**

See "Identify Your Specific Hardware Requirements" on page 16.

**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. 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**

<table>
<thead>
<tr>
<th>Hosts</th>
<th>Guests</th>
<th>Est. Daily Change</th>
<th>Data Retention in Days</th>
<th>Data Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>250</td>
<td>10%</td>
<td>15</td>
<td>3GB</td>
</tr>
<tr>
<td>Hosts</td>
<td>Guests</td>
<td>Est. Daily Change</td>
<td>Data Retention in Days</td>
<td>Data Size</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>-------------------</td>
<td>------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>50</td>
<td>500</td>
<td>10%</td>
<td>15</td>
<td>6GB</td>
</tr>
<tr>
<td>250</td>
<td>2500</td>
<td>10%</td>
<td>15</td>
<td>30GB</td>
</tr>
</tbody>
</table>

The Managing Agent processes requests for a single vCenter Server. Configure one Managing Agent machine per vCenter Server. In single vCenter Server instance environments, the VCM Collector can be the 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.

**Prerequisites**

If you run SQL Server on a virtual machine, refer to the following documents.


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 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.

The following table provides hardware requirements for a single-tier server installation of VCM. If you are installing in a two-tier or three-tier environment, approximate sizing requirements are provided in the VMware Knowledge Base. See [http://kb.vmware.com/kb/2033894](http://kb.vmware.com/kb/2033894).

**Table 2-4. Minimum Hardware Requirements by Number of Managed Machines for Single-Tier Server Installations**

<table>
<thead>
<tr>
<th>Requirements</th>
<th>1–1000</th>
<th>1000–2000</th>
<th>2000+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>Dual Xeon or single Dual Core 2GHz minimum</td>
<td>Quad Xeon or two Dual Core 2GHz minimum</td>
<td>Eight-way Xeon or four Dual Core 2GHz minimum</td>
</tr>
<tr>
<td>Number of Separate Disk Channels</td>
<td>8GB+ minimum</td>
<td>12GB+ minimum</td>
<td>16GB+ minimum</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

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 2–5. Minimum Disk Configuration Requirements by Number of Managed Machines**

<table>
<thead>
<tr>
<th>Number of VCM Managed Machines</th>
<th>RAID Channel and RAID Level</th>
<th>Partitions</th>
<th>Usable Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–500</td>
<td>Channel 0 – RAID 1</td>
<td>OS</td>
<td>36GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Collector Data Files</td>
<td>36GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TempDB</td>
<td>36GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQL Log Files</td>
<td>28GB</td>
</tr>
<tr>
<td></td>
<td>Channel 1 – RAID 0+1 (recommended) or RAID 10</td>
<td>SQL Data Files</td>
<td>56GB</td>
</tr>
<tr>
<td>501–1000</td>
<td>Channel 0 – RAID 1</td>
<td>OS</td>
<td>36GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Collector Data Files</td>
<td>36GB</td>
</tr>
<tr>
<td></td>
<td>Channel 1 – RAID 1</td>
<td>TempDB</td>
<td>56GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQL Log Files</td>
<td>56GB</td>
</tr>
<tr>
<td></td>
<td>Channel 2 – RAID 0+1 (recommended) or RAID 10</td>
<td>SQL Data Files</td>
<td>113GB</td>
</tr>
<tr>
<td>1001–2000</td>
<td>Channel 0 – RAID 1</td>
<td>OS</td>
<td>36GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Collector Data Files</td>
<td>54GB</td>
</tr>
<tr>
<td></td>
<td>Channel 1 – RAID 1</td>
<td>TempDB</td>
<td>113GB</td>
</tr>
<tr>
<td></td>
<td>Channel 2 – RAID 1</td>
<td>SQL Log Files</td>
<td>113GB</td>
</tr>
<tr>
<td></td>
<td>Channel 3 – RAID 0+1 (recommended) or RAID 10</td>
<td>SQL Data Files</td>
<td>227GB</td>
</tr>
</tbody>
</table>

**What to do next**

Determine your software and operating system requirements. See "Software and Operating System Requirements for Collector Machines" on page 19.
Software and Operating System Requirements for Collector Machines

Your VCM environment software configuration must meet the requirements to install VCM 5.6. 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 22.

### Sizing Impacts on Software Requirements

Use the total number of managed machines that you identified in "Determine the Size of Your Environment” on page 15 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 for your specific requirements.


⚠️ **CAUTION** If your Windows machine has an evaluation version of SQL Server Standard Edition or Enterprise Edition, use it only for evaluation purposes. Do not use an evaluation version in a production environment, because it is not officially released for production.

| Table 3–1. Minimum Software Requirements by Number of VCM Managed Machines |
|---------------------------------|-----------------|-----------------|-----------------|
| **Software Component** | **1–1000** | **1000–2000** | **2000–5000** |
| SSRS Version | SQL Server 2008 Reporting Services | SQL Server 2008 Reporting Services | SQL Server 2008 Reporting Services |

### Software Installation and Configuration Overview

VCM supports the Collector running on a Windows Server 2008 R2 operating system. Complete the preparatory steps to prepare your Windows Server 2008 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 21. To understand the requirements to upgrade or migrate your environment to the latest version of VCM, see "VCM Upgrades and Migrations" on page 20.

**VCM Upgrades and Migrations**

To upgrade your version of VCM to the current version, you must have VCM 5.4.0 or 5.4.1. To migrate your environment to the current version of VCM, you must have version 4.11.1 or later installed and running.

---

**CAUTION** VCM 5.6 and later do 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.

---

**What to do next**

To upgrade VCM, see the upgrade and migration examples at "Upgrading or Migrating VCM" on page 127.
Preparing for Installation

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.

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.

## 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 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 the Windows Server 2008 R2 database server machine, and the VCM Collector and Web components reside on the second Windows Server 2008 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 machines.

To perform the prerequisite steps for VCM installation, see [“System Prerequisites to Install VCM” on page 23](#).
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 must run without errors before you install VCM. For more information about Foundation Checker, see the VCM Foundation Checker User’s Guide on the Download VMware vCenter Configuration Manager Web site.

Use the following topics to verify your system requirements.

- Verify that your environment meets the security requirements. See the VCM Security Guide on the Download VMware vCenter Configuration Manager Web site.
- "Establish Local Administration Rights" on page 24
  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 page 25
  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 page 25
  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 26
  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 VMware Application Services Account" on page 26
  Verify that the VMware Application Services Account is a domain user.
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.
- Domain account in the Local Administrators group on the machine where the user installs or upgrades VCM.

The installing user account must not be the account used to run SQL Server services.
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" on page 25.
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.
- Mozilla Firefox version 6.0 or later with the Internet Explorer IE Tab add-on. This add-on requires Internet Explorer 6.0 to be installed on the machine.

What to do next

Verify the default Network Authority account. See “Verify the Default Network Authority Account” on page 25.

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.

The Local System account, NT AUTHORITY\System, has unrestricted access to all local system resources. This account is a member of the Windows Administrators group on the local machine and a member of the SQL Server sysadmin fixed server role.

If the NT AUTHORITY\System account does not have access to the VCM installation binary files, the installation results in an access denied error. You must grant access to the NT AUTHORITY\System account from the installation source directory and then run the installation again. A user or user’s group has access when they have full control of the file or folder.

It is acceptable, but not preferred, to use the same account for the Application services account, Collector service account, VCM Remote account, and the Tomcat Services account. If you use a single account, the permissions required for the Collector service account will be 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" on page 26.

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, add the user or group to the list. Ensure that the user has Windows administrator rights issued by the network administrator.

What to do next

Keep Server Manager open to specify the VCM Application Services account in Server Manager. See "Verify the VMware Application Services Account" on page 26.

Verify the VMware Application Services Account

Verify that the VMware Application Services Account is a domain user.

**IMPORTANT** Never use this account as a VCM login or for any other purpose. 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.

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 application services account is listed as a member of the Administrators group.
   If the user or administrator’s group is not listed, add the user or group to the list. Ensure that the user has Windows administrator rights issued by the network administrator.

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 page 27.
Verify the VCM Agent is Not Installed

The VCM Collector installation installs an updated Agent. The target Windows machine must not have a VCM Agent installed before you install VCM. If an Agent is installed, VCM will not install.

If a VCM Agent is installed, uninstall the Agent.

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.
   a. If a working VCM Collector exists, use the VCM Web console to unlicense this machine and remove the VCM Agent.
   b. 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.
   a. 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.
   b. Examine the uninstall data to confirm that this is the VCM Agent.
   c. Open the setting UninstallString and copy the value.

      An example value is as follows.

      MsiExec.exe /X{7C51E2CA-C932-44EF-8B77-3C03356A24CC}
   d. 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.
   a. 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}.
   b. 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" on page 28.

Verify the SQLXML Version

Verify that the correct version of SQLXML is installed on the database server.

SQLXML 4.0 SP1 is installed with SQL Server 2008 R2.

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. Verify that the version is 10.0.1600.60.
5. If the version is not SQLXML 4.0 SP1 10.0.1600.60 or later, or only an earlier version of SQLXML is installed, download and install SQLXML 4.0 SP1.

To resolve this issue, uninstall the installed SQL XML version from Add/Remove Programs, then access the Microsoft Download Center and install SQL XML 4.0 SP1. See VMware knowledge base article at http://kb.vmware.com/kb/2015821.

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 29.
- Understand the use of secure communications certificates and be prepared to specify the certificates during VCM installation. See "Secure Communications Certificates" on page 33.
Configure Resources to Install VCM on a Virtual Machine

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. 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 an ESX server that has over-allocated resources.

**Prerequisites**

- Follow the requirements for physical hardware. See "Hardware Requirements for Collector Machines" on page 15.
- Perform the system prerequisite tasks. See "System Prerequisites to Install VCM" on page 23.

**Procedure**

- "Configure the Disk to Install VCM on a Virtual Machine" on page 30
  Configure the disk for the virtual machine. For large scale environments, you might need to alter the requirements.
- "Configure the CPU to Install VCM on a Virtual Machine" on page 30
  Configure the CPU for the virtual machine. For large scale environments, you might need to alter the requirements.
- "Configure the Memory to Install VCM on a Virtual Machine" on page 31
  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 "Secure Communications Certificates" on page 33.
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

- Configure resources. See "Configure Resources to Install VCM on a Virtual Machine" on page 29.
- 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.
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 change the disk resource allocation.
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" on page 30.

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

- Configure resources. See "Configure Resources to Install VCM on a Virtual Machine" on page 29.
- 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.
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" on page 31.

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
- Configure resources. See "Configure Resources to Install VCM on a Virtual Machine" on page 29.
- 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.
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
Understand the use of secure communications certificates and be prepared to specify the certificates during VCM installation. See "Secure Communications Certificates" on page 33.
Secure Communications Certificates

During VCM installation, specify the Collector and Enterprise certificates. VCM uses Transport Layer Security (TLS) to secure all HTTP communication with all Windows Agents and UNIX Agents in HTTP mode, 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 on the Download VMware vCenter Configuration Manager Web site.

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 over HTTP. 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 two 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 page 33.

- 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.

- A Collector Certificate can issue Agent certificates. When all Collector Certificates are issued by the same Enterprise Certificate, any Agent Certificate may be issued by any Collector Certificate, and all Agents can trust all Collectors. All Collectors can validate all Agent Certificates. Agent Certificates are used for Mutual Authentication only. VCM supports Mutual Authentication, which requires interaction with VMware Technical Support and a Collector Certificate that has certificate signing capability.

- The Collector Certificate and associated private key must be available to the Collector. This certificate is stored in the local machine personal system store.

**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.

- 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.

■ Using the MSI Install Package
   When you specify HTTP, the MSI Agent install package also requires access to the .pem file.

■ Installing the Agent for UNIX/Linux
   See Install the Agent on UNIX/Linux Machines in the VCM Administration Guide.

What to do next
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 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.

**Figure 8–1.** Single-Tier Server Installation Components
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.

In addition to the VCM Collector, the single-tier installation configuration includes an Operating System Provisioning Server. The OS Provisioning Server manages the OS provisioning actions as commanded by VCM.

For hardware and software requirements for the OS Provisioning Server, see "Hardware and Software Requirements for the Operating System Provisioning Server" on page 171.
Configure a Single-Tier Installation Environment

In a single-tier installation configuration, you configure the single Windows Server 2008 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 23.
- Connect the single Windows Server 2008 R2 VCM Collector machine to your domain.
- Obtain the SQL Server 2008 R2 Enterprise or Standard edition installation disk or verify access to a file share where the installer resides.
Procedure

1. "Verify that the Installing User is an Administrator" on page 40
   The user who installs the Windows Server 2008 R2 operating system must be an Administrator and a domain account.

2. "Install and Configure a Windows Server 2008 R2 Operating System" on page 41
   To prepare your Windows machine for VCM installation, install the Windows Server 2008 R2 operating system on each Windows machine in your installation configuration and verify that the settings are configured for VCM operation.

3. "Install the .NET Framework" on page 43
   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 44
   To set up 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 50
   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 used to generate VCM reports. Before you install and configure SSRS, you must back up your SSRS key and clear the Internet Explorer Protected Mode.

7. "Configure the VCM Collector Components" on page 59
   The VCM Collector contains the VCM software application, VCM services, and the OS Provisioning Server. To prepare the VCM Collector components for VCM installation, configure the required utilities.

What to do next

Use VCM Installation Manager to install the VCM components. See "Installing VCM" on page 117.

Verify that the Installing User is an Administrator

The user who installs the Windows Server 2008 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


Install and Configure a Windows Server 2008 R2 Operating System

To prepare your Windows machine for VCM installation, install the Windows Server 2008 R2 operating system on each Windows machine in your installation configuration and verify that the settings are configured for VCM operation.

Prerequisites

- Verify that the person who performs these procedures uses a domain account with local administrator rights.
- The user who installs the Windows Server 2008 R2 operating system must be an Administrator and a domain account. See "Verify that the Installing User is an Administrator" on page 40.

Procedure

1. Install Microsoft Windows Server 2008 R2 on your Windows machine.
2. Verify that the computer name settings for your Windows machine is a valid DNS machine name with no underscores.
   
   If you attempt to change the machine name after the machine is identified as a Collector, problems might occur with VCM, SQL Server, and SQL Server Reporting Services.
Configure the Operating System Locale Settings
To set the language for VCM installation, verify that your Windows Server Locale Setting is configured correctly.

Procedure
1. In Windows Explorer, click Start and select Control Panel > Clock, Language, and Region.
2. Click Region and Language.
3. Click the Administrative tab and set the language to English (United States).

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 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" on page 43.
Install the .NET Framework

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

VCM 5.6 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.

The VCM Collector requires the .NET 3.5.1 Framework. Software provisioning Package Studio requires .NET 3.5.1 and Software provisioning Package Manager requires either .NET 3.5.1 or .NET 4.0.

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, install it from the Microsoft Web site.

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 database components. See "Configuring the Database Components of the VCM Collector" on page 44.

**Configuring the Database Components of the VCM Collector**

To set up 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.

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 5.6 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 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 or Enterprise edition of SQL Server. You must install the 64-bit SQL Server 2008 R2, English (United States) 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.

**Set the Internet Explorer Enhanced Security Mode**

Depending on the security level required for your environment, you might need to turn off Internet Explorer Enhanced Security Mode for Administrators and Users to ensure that the database components are configured correctly.
Procedure

1. On the database server, click **Start** and select **All Programs > Administrative Tools > Server Manager**.
2. In the left pane, click **Server Manager**.
3. In the Server Summary pane, locate the Security Information area.
4. Click **Configure IE ESC**.
5. In the Internet Explorer Enhanced Security Configuration pop-up window, under Administrators, select **Off**.

**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.

---

**CAUTION** If your Windows machine has an evaluation version of SQL Server Standard Edition or Enterprise Edition, use it only for evaluation purposes. Do not use an evaluation version in a production environment, because it is not officially released for production.

---

**Prerequisites**

Obtain the SQL Server 2008 R2 Enterprise or Standard edition installation disk or verify access to a file share where the installer resides.

**Procedure**

1. Start the SQL Server 2008 R2 installation.
2. Perform the actions to install SQL Server 2008 R2 Enterprise or Standard edition.

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server Installation Center</td>
<td>Click <strong>New installation or add features to an existing installation.</strong></td>
</tr>
<tr>
<td>Setup Support Rules</td>
<td>Click <strong>Install</strong> and verify that all of the rules pass. To view the detailed system configuration check report, click the link.</td>
</tr>
<tr>
<td>Setup Support Files</td>
<td>Click <strong>Install</strong> to install the setup support files.</td>
</tr>
<tr>
<td>Setup Support Rules – for SQL Server Setup support files</td>
<td>Verify that all of the rules passed.</td>
</tr>
<tr>
<td>Installation Type</td>
<td>Select <strong>New installation or add shared features.</strong></td>
</tr>
<tr>
<td>Product Key</td>
<td>Verify that the product key is entered.</td>
</tr>
<tr>
<td>Wizard Page</td>
<td>Action</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>License Terms</td>
<td>Accept the license terms.</td>
</tr>
<tr>
<td>Setup Role</td>
<td>Select <strong>SQL Server Feature Installation</strong>.</td>
</tr>
<tr>
<td>Feature Selection</td>
<td>Select the following features.</td>
</tr>
<tr>
<td></td>
<td>Instance Features:</td>
</tr>
<tr>
<td></td>
<td>- Database Engine Services</td>
</tr>
<tr>
<td></td>
<td>- Reporting Services</td>
</tr>
<tr>
<td></td>
<td>Shared Features:</td>
</tr>
<tr>
<td></td>
<td>- Client Tools Connectivity</td>
</tr>
<tr>
<td></td>
<td>- SQL Server Books online</td>
</tr>
<tr>
<td></td>
<td>- Management Tools - Basic and Management Tools - Complete</td>
</tr>
<tr>
<td>Installation Rules</td>
<td>Verify that the rules passed. To view the detailed system configuration check report, click the link.</td>
</tr>
<tr>
<td>Instance Configuration</td>
<td>Select <strong>Default Instance</strong>. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is installed, select <strong>Named Instance</strong> and assign a name.</td>
</tr>
<tr>
<td>Disk Space Requirements</td>
<td>Review the disk usage summary.</td>
</tr>
<tr>
<td>Server Configuration</td>
<td>Click <strong>Use the same account for all SQL Server services</strong> and enter the NT AUTHORITY\SYSTEM account and password.</td>
</tr>
<tr>
<td>Database Engine Configuration</td>
<td>Select <strong>Mixed Mode (SQL Server authentication and Windows authentication)</strong>, enter and confirm the password, and click <strong>Add Current User</strong> to add the account to the SQL Server administrators. Although the VCM installation system checks require that SQL Server Mixed Mode authentication is enabled during the installation of VCM, you can change SQL Server back to Windows Integrated authentication after the installation is finished.</td>
</tr>
<tr>
<td>Error Reporting</td>
<td>Review the summary information.</td>
</tr>
<tr>
<td>Installation Configuration Rules</td>
<td>Verify that the rules passed. To view the detailed system configuration check report, click the link.</td>
</tr>
<tr>
<td>Ready to Install</td>
<td>Review the summary of features and click <strong>Install</strong> to install SQL Server 2008 R2. When the installation is finished, click the link to view the log file.</td>
</tr>
</tbody>
</table>

**What to do next**

- Reboot the single-server machine.
- Configure the SQL Server properties. See "Verify and Configure the SQL Server Properties" on page 47.
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. Click Start and select All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio.
2. Right-click the SQL instance and select Properties.
3. Confirm the General page server properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>10.50.1600.1</td>
</tr>
<tr>
<td>Language</td>
<td>English (United States). If the language is not correct, uninstall and install the correct version of SQL Server.</td>
</tr>
<tr>
<td>Server Collation</td>
<td>SQL_Latin1_General_CP1_CI_AS. If the server collation is not correct, uninstall and reinstall SQL Server.</td>
</tr>
</tbody>
</table>

4. Select and confirm the Security page server properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Authentication mode</td>
<td>Recommended. Select this mode.</td>
</tr>
<tr>
<td>SQL Server and Windows Authentication mode</td>
<td>Although this setting is acceptable for VCM, Windows Authentication mode is recommended.</td>
</tr>
</tbody>
</table>

5. Select and confirm the Database Settings page server properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default index fill factor</td>
<td>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.</td>
</tr>
<tr>
<td>Recovery interval (minutes)</td>
<td>Type or select 5.</td>
</tr>
</tbody>
</table>

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" on page 48.
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 2008 R2, 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 2008 R2 were installed, verify and reset the SQL Server server name.

Procedure
1. Click Start and select All Programs > Microsoft SQL Server 2008 R2 > 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.

   ```sql
   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 2008 R2 > Configuration Tools > SQL Server Configuration Manager > SQL Server 2008 R2 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" on page 48.

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. Click Start and select All Programs.
2. Click Microsoft SQL Server 2008 R2 and select SQL Server Management Studio.
3. Expand the server, expand Security, expand Server Roles.
4. Double-click sysadmin and view the members of the sysadmin role.
5. Verify that the account to use for the SQL Server Agent service is a member of the sysadmin fixed role.
6. If the account is not a member of the sysadmin fixed role, add this role to the account.

What to do next
Select the SQL Server Agent service account See "Select the SQL Server Agent Service Account" on page 49.
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 on 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 5.6 supports Active/Passive 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 48.

Procedure

1. On the VCM database server machine, click Start and select All Programs.
2. Click Microsoft SQL Server 2008 R2 and select 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 on option and provide the account information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-in account</td>
<td>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.</td>
</tr>
<tr>
<td>This account</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 page 50.
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. Click Start and select All Programs > Microsoft SQL Server 2008 R2 > 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" on page 50.

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.

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 5.6 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 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

- 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 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 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common HTTP Features</td>
<td>Select these options:</td>
</tr>
<tr>
<td></td>
<td>- Static Content</td>
</tr>
<tr>
<td></td>
<td>- Default Document</td>
</tr>
<tr>
<td></td>
<td>- Directory Browsing</td>
</tr>
<tr>
<td></td>
<td>- HTTP Errors</td>
</tr>
<tr>
<td>Application Development</td>
<td>Select these options:</td>
</tr>
<tr>
<td></td>
<td>- ASP .NET</td>
</tr>
<tr>
<td></td>
<td>- .Net Extensibility</td>
</tr>
<tr>
<td></td>
<td>- ASP</td>
</tr>
<tr>
<td></td>
<td>- ISAPI Extension</td>
</tr>
<tr>
<td></td>
<td>- ISAPI Filters</td>
</tr>
<tr>
<td></td>
<td>- Server Side Includes</td>
</tr>
<tr>
<td>Health and Diagnostics</td>
<td>Select these options:</td>
</tr>
<tr>
<td></td>
<td>- HTTP Logging</td>
</tr>
<tr>
<td></td>
<td>- Request Monitor</td>
</tr>
<tr>
<td>Security</td>
<td>Select these options:</td>
</tr>
<tr>
<td></td>
<td>- Basic Authentication</td>
</tr>
<tr>
<td></td>
<td>- Request Filtering</td>
</tr>
<tr>
<td>Performance</td>
<td>Select:</td>
</tr>
<tr>
<td></td>
<td>- Static Content Compression</td>
</tr>
</tbody>
</table>
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

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

Procedure

1. On the Collector, right-click Computer and select Manage to open Server Manager.
2. In Server Manager, 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.
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.

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

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 Bindings**

IIS bindings 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 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous Authentication</td>
<td>Set to <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>ASP.NET Impersonation</td>
<td>Set to <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Basic Authentication</td>
<td>Set to <strong>Enabled</strong>.</td>
</tr>
<tr>
<td>Option</td>
<td>Action</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Forms Authentication</td>
<td>Set to Disabled.</td>
</tr>
</tbody>
</table>

**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 page 54.

**Configure SSRS on the VCM Collector**

SQL Server Reporting Services (SSRS) is used to generate VCM reports. Before you install and configure SSRS, you must back up your SSRS key and clear the Internet Explorer Protected Mode.

**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. For details about how to use this utility, see the online Microsoft Support center.

**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. Double-click `rskeymgmt.exe` and follow the prompts to copy your SSRS key set to a removable media device and store it in a secure location.

**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

SQL Server Reporting Services (SSRS) is a server-based report generation software system that is administered using a web interface and used to deliver reports. You must configure SSRS manually in your single-tier 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 54.
- Disable the Internet Explorer Protected Mode. See "Disable IE Protected Mode for SSRS" on page 54.

Procedure

1. On your single server, start SQL Server 2008 R2 Reporting Services Configuration Manager.
   a. Click Start and select Run.
   b. Type rsconfigtool.exe.
   c. In the Reporting Services Configuration Connection dialog box, click Connect to connect and log in to SQL Server 2008 R2 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 and select the language as English (United States).

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

i. In the Credentials pane, change the Authentication Type to Windows Credentials.

j. Specify an account that has permission to connect from the Web service on the single server to the database on the single server, specify the password for the account, and click Next.

k. In the Summary pane, review the selections and click Next.

l. 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Set to All Assigned (Recommended).</td>
</tr>
<tr>
<td>TCP Port</td>
<td>Set to 80.</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>Not Selected</td>
</tr>
</tbody>
</table>

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 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 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 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 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](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=usenglish;`

  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, VCM services, and the OS Provisioning Server. To prepare the VCM Collector components for VCM installation, configure the required utilities.

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

Prerequisites

- Perform the prerequisite tasks for your installation configuration. See "Single-Tier Server Installation" on page 37.

- From the VCM Collector, verify that you can access the Microsoft Download Center, Microsoft SQL Server 2008 Feature Pack to download SQL XML 4.0 and SP1 in the following procedure. See the online Microsoft Download Center.

- Verify that you can access the Microsoft Download Center, Microsoft SQL Server 2008 R2 Feature Pack to download and install the SQLCMD utility x64 package (SqlCmdLnUtils.msi) and the Native Client (sqlncli.msi) in the following procedure. See the online Microsoft Download Center. The SQL
Command Line Tools in the SQL Server 2008 R2 Feature Pack are required.

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

Procedure

1. Download and install SQL XML 4.0 and SP1, X64 Package.

2. Download and install SQL Server 2008 R2 Command Line Utilities, which includes the SQLCMD utility, X64 Package (SqlCmdLnUtils.msi).
   The SQL Command Line Tools in the SQL Server 2008 R2 Feature Pack are required.

3. Download and install the SQL Server 2008 R2 Native Client, X64 Package (sqlncli.msi).
   The Native Client from the SQL Server 2008 R2 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 117.
Two-Tier Split Installation

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

**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**

**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.
Prerequisites

- Perform the general system prerequisite steps. See "System Prerequisites to Install VCM" on page 23.
- Connect the database server machine to the domain.
- Connect the combined VCM Collector and Web server machine to the domain.
- Obtain the SQL Server 2008 R2 Enterprise or Standard edition installation disk or verify access to a file share where the installer resides.

Procedure

1. "Verify that the Installing User is an Administrator" on page 62
   The user who installs the Windows Server 2008 R2 operating system must be an Administrator and a domain account.
2. "Install and Configure a Windows Server 2008 R2 Operating System" on page 63
   To prepare your Windows machine for VCM installation, install the Windows Server 2008 R2 operating system on each Windows machine in your installation configuration and verify that the settings are configured for VCM operation.
3. "Configuring the VCM Database Server" on page 65
   To set up 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 dedicated machine. The databases include VCM, VCM_Coll, VCM_Raw, and VCM_UNIX.
4. "Configure the Combined VCM Collector and Web Server " on page 71
   In a two-tier split installation configuration, the VCM Collector and the Web server components reside together on a dedicated Windows Server 2008 R2 machine, and the VCM database server resides on a separate Windows Server 2008 R2 machine.
5. "Configure the Web Components" on page 72
   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.
6. "Configure the VCM Collector Components" on page 84
   The combined VCM Collector and Web server contains the VCM software application, VCM services, and the OS Provisioning Server. 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

Use VCM Installation Manager to install the VCM components. See "Installing VCM" on page 117.

Verify that the Installing User is an Administrator

The user who installs the Windows Server 2008 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


Install and Configure a Windows Server 2008 R2 Operating System

To prepare your Windows machine for VCM installation, install the Windows Server 2008 R2 operating system on each Windows machine in your installation configuration and verify that the settings are configured for VCM operation.

Prerequisites

- Verify that the person who performs these procedures uses a domain account with local administrator rights.
- The user who installs the Windows Server 2008 R2 operating system must be an Administrator and a domain account. See "Verify that the Installing User is an Administrator" on page 62.

Procedure

1. Install Microsoft Windows Server 2008 R2 on your Windows machine.
2. Verify that the computer name settings for your Windows machine is a valid DNS machine name with no underscores.
   If you attempt to change the machine name after the machine is identified as a Collector, problems might occur with VCM, SQL Server, and SQL Server Reporting Services.
Configure the Operating System Locale Settings
To set the language for VCM installation, verify that your Windows Server Locale Setting is configured correctly.

Procedure
1. In Windows Explorer, click Start and select Control Panel > Clock, Language, and Region.
2. Click Region and Language.
3. Click the Administrative tab and set the language to English (United States).

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 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" on page 65.
Configuring the VCM Database Server

To set up 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 dedicated machine. The databases include VCM, VCM_Coll, VCM_Raw, and VCM_UNIX.

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 5.6 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 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 or Enterprise edition of SQL Server. You must install the 64-bit SQL Server 2008 R2, English (United States) 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.

Set the Internet Explorer Enhanced Security Mode

Depending on the security level required for your environment, you might need to turn off Internet Explorer Enhanced Security Mode for Administrators and Users to ensure that the database components are configured correctly.

**Procedure**

1. On the database server, click **Start** and select **All Programs > Administrative Tools > Server Manager**.
2. In the left pane, click **Server Manager**.
3. In the Server Summary pane, locate the Security Information area.
4. Click **Configure IE ESC**.
5. In the Internet Explorer Enhanced Security Configuration pop-up window, under Administrators, select **Off**.

Install SQL Server on the Database Server

In a two-tier split installation configuration, the VCM database server resides on a dedicated 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.
**CAUTION** If your Windows machine has an evaluation version of SQL Server Standard Edition or Enterprise Edition, use it only for evaluation purposes. Do not use an evaluation version in a production environment, because it is not officially released for production.

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 5.6 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 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**

Obtain the SQL Server 2008 R2 Enterprise or Standard edition installation disk or verify access to a file share where the installer resides.

**Procedure**

1. Start the SQL Server 2008 R2 installation.
2. Perform the actions to install SQL Server 2008 R2 Enterprise or Standard edition.

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

<table>
<thead>
<tr>
<th>Installation Rules</th>
<th>Verify that the rules passed. To view the detailed system configuration check report, click the link.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Configuration</td>
<td>Select <strong>Default Instance</strong>. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is installed, select <strong>Named Instance</strong> and assign a name.</td>
</tr>
<tr>
<td>Disk Space Requirements</td>
<td>Review the disk usage summary.</td>
</tr>
<tr>
<td>Server Configuration</td>
<td>Click <strong>Use the same account for all SQL Server services</strong> and enter the NTAUTHORITY\SYSTEM account and password.</td>
</tr>
<tr>
<td>Database Engine Configuration</td>
<td>Select <strong>Mixed Mode (SQL Server authentication and Windows authentication)</strong>, enter and confirm the password, and click <strong>Add Current User</strong> to add the account to the SQL Server administrators. Although the VCM installation system checks require that SQL Server Mixed Mode authentication is enabled during the installation of VCM, you can change SQL Server back to Windows Integrated authentication after the installation is finished.</td>
</tr>
<tr>
<td>Error Reporting</td>
<td>Review the summary information.</td>
</tr>
<tr>
<td>Installation Configuration Rules</td>
<td>Verify that the rules passed. To view the detailed system configuration check report, click the link.</td>
</tr>
</tbody>
</table>

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. Click Start and select All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio.

2. Right-click the SQL instance and select Properties.

3. Confirm the General page server properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>10.50.1600.1</td>
</tr>
<tr>
<td>Language</td>
<td>English (United States). If the language is not correct, uninstall and install the correct version of SQL Server.</td>
</tr>
<tr>
<td>Server Collation</td>
<td>SQL_Latin1_General_CP1_CI_AS. If the server collation is not correct, uninstall and reinstall SQL Server.</td>
</tr>
</tbody>
</table>

4. Select and confirm the Security page server properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Authentication mode</td>
<td>Recommended. Select this mode.</td>
</tr>
<tr>
<td>SQL Server and Windows Authentication mode</td>
<td>Although this setting is acceptable for VCM, Windows Authentication mode is recommended.</td>
</tr>
</tbody>
</table>

5. Select and confirm the Database Settings page server properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default index fill factor</td>
<td>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.</td>
</tr>
<tr>
<td>Recovery interval (minutes)</td>
<td>Type or select 5.</td>
</tr>
</tbody>
</table>

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" on page 68.

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 2008 R2, 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 2008 R2 were installed, verify and reset the SQL Server server name.
Procedure

1. Click Start and select All Programs > Microsoft SQL Server 2008 R2 > 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 2008 R2 > Configuration Tools > SQL Server Configuration Manager > SQL Server 2008 R2 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 page 69.

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. Click Start and select All Programs.
2. Click Microsoft SQL Server 2008 R2 and select SQL Server Management Studio.
3. Expand the server, expand Security, expand Server Roles.
4. Double-click sysadmin and view the members of the sysadmin role.
5. Verify that the account to use for the SQL Server Agent service is a member of the sysadmin fixed role.
6. If the account is not a member of the sysadmin fixed role, add this role to the account.

What to do next
Select the SQL Server Agent service account See “Select the SQL Server Agent Service Account” on page 70.
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 on 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 5.6 supports Active/Passive 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 69.

Procedure

1. On the VCM database server machine, click Start and select All Programs.
2. Click Microsoft SQL Server 2008 R2 and select 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 on option and provide the account information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-in account</td>
<td>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.</td>
</tr>
<tr>
<td>This account</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 page 71.
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. Click Start and select All Programs > Microsoft SQL Server 2008 R2 > 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 page 71.

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 machine, and the VCM database server resides on a separate Windows Server 2008 R2 machine.

Before you configure the combined VCM Collector and Web server, which includes SQL Server Reporting Services, you must perform the prerequisite tasks for a two-tier split installation configuration.

Install the .NET Framework

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

VCM 5.6 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.

The VCM Collector requires the .NET 3.5.1 Framework. Software provisioning Package Studio requires .NET 3.5.1 and Software provisioning Package Manager requires either .NET 3.5.1 or .NET 4.0.

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, install it from the Microsoft Web site.
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” on page 72.

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.

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 5.6 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 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.
- 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 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 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common HTTP Features</td>
<td>Select these options:</td>
</tr>
<tr>
<td></td>
<td>■ Static Content</td>
</tr>
</tbody>
</table>
Option | Action
--- | ---
| | Default Document
| | Directory Browsing
| | HTTP Errors

Application Development Select these options:
| | ASP .NET
| | .Net Extensibility
| | ASP
| | ISAPI Extension
| | 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**

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

**Procedure**

1. On the Collector, right-click **Computer** and select **Manage** to open Server Manager.
2. In Server Manager, 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**.
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.

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

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 Bindings**

IIS bindings 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous Authentication</td>
<td>Set to Disabled.</td>
</tr>
<tr>
<td>ASP.NET Impersonation</td>
<td>Set to Disabled.</td>
</tr>
<tr>
<td>Basic Authentication</td>
<td>Set to Enabled.</td>
</tr>
<tr>
<td>Forms Authentication</td>
<td>Set to Disabled.</td>
</tr>
</tbody>
</table>

**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" on page 77.
Installing and Configuring SSRS on the Combined VCM Collector and Web Server

SQL Server Reporting Services (SSRS) is used to generate VCM reports. Before you install and configure SSRS, you must back up your SSRS key and clear the Internet Explorer Protected Mode.

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. For details about how to use this utility, see the online Microsoft Support center.

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. Double-click rskeymgmt.exe and follow the prompts to copy your SSRS key set to a removable media device and store it in a secure location.

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 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 page 77.
- Disable the Internet Explorer Protected Mode. See "Disable IE Protected Mode for SSRS" on page 77.
- Obtain the SQL Server 2008 R2 Enterprise or Standard edition installation disk or verify access to a file share where the installer resides.

Procedure

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

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server Installation Center</td>
<td>Click <strong>New installation or add features to an existing installation.</strong></td>
</tr>
<tr>
<td>Setup Support Rules</td>
<td>Click <strong>Install</strong> and verify that all of the rules pass. To view the detailed system configuration check report, click the link.</td>
</tr>
<tr>
<td>Setup Support Files</td>
<td>Click <strong>Install</strong> to install the setup support files.</td>
</tr>
<tr>
<td>Setup Support Rules – for SQL Server Setup support files</td>
<td>Verify that all of the rules passed.</td>
</tr>
<tr>
<td>Installation Type</td>
<td>Select <strong>New installation or add shared features.</strong></td>
</tr>
<tr>
<td>Product Key</td>
<td>Verify that the product key is entered.</td>
</tr>
<tr>
<td>License Terms</td>
<td>Accept the license terms.</td>
</tr>
<tr>
<td>Setup Role</td>
<td>Select <strong>SQL Server Feature Installation.</strong></td>
</tr>
<tr>
<td>Feature Selection</td>
<td>Select the following options.</td>
</tr>
<tr>
<td></td>
<td>- Reporting Services</td>
</tr>
<tr>
<td></td>
<td>- Client Tools Connectivity</td>
</tr>
<tr>
<td></td>
<td>- SQL Server Books Online</td>
</tr>
<tr>
<td></td>
<td>- Management Tools - Basic</td>
</tr>
<tr>
<td></td>
<td>- Management Tools - Complete</td>
</tr>
<tr>
<td>Installation Rules</td>
<td>Verify that the rules passed. To view the detailed system configuration check report, click the link.</td>
</tr>
<tr>
<td>Instance Configuration</td>
<td>Select <strong>Default Instance</strong>. If an instance of SQL Server is not installed, the installation creates a default instance. If an instance of SQL Server is installed, select <strong>Named Instance</strong> and assign a name.</td>
</tr>
</tbody>
</table>
Wizard Page | Action
--- | ---
Disk Space Requirements | (Optional) Review the disk usage summary.
Server Configuration | Click *Use the same account for all SQL Server services* and enter the NTAUTHORITY\SYSTEM account and password.
Database Engine Configuration | Select *Mixed Mode (SQL Server authentication and Windows authentication)*, enter and confirm the password, and click *Add Current User* to add the account to the SQL Server administrators. Although the VCM installation system checks require that SQL Server Mixed Mode authentication is enabled during the installation of VCM, you can change SQL Server back to Windows Integrated authentication after the installation is finished.
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.

**Configure SSRS**

SQL Server Reporting Services (SSRS) is a server-based report generation software system that is administered using a web interface and used to deliver reports. You must configure SSRS manually in your two-tier split 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 77.
- **Disable the Internet Explorer Protected Mode.** See "Disable IE Protected Mode for SSRS" on page 77.

**Procedure**

1. On your combined VCM Collector and Web server, start SQL Server 2008 R2 Reporting Services Configuration Manager.
   a. Click **Start** and select **Run**.
   b. Type `rsconfigtool.exe`.
   c. In the Reporting Services Configuration Connection dialog box, click **Connect** to connect and log in to SQL Server 2008 R2 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 and select the language as **English (United States)**.
h. Set the Report Server Mode to **Native Mode** and click **Next**.
i. In the Credentials pane, change the Authentication Type to **Windows Credentials**.

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Directory</td>
<td>Set to <strong>ReportServer</strong>.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Set to <strong>All Assigned (Recommended)</strong>.</td>
</tr>
<tr>
<td>TCP Port</td>
<td>Set to <strong>80</strong>.</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>Not Selected</td>
</tr>
</tbody>
</table>

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 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" on page 81.

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 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, locate the rsreportserver.config file.
   - The default location is C:\Program Files\Microsoft SQL Server\Reporting Services\Instance\ReportServer\rsreportserver.config.
2. Stop the SSRS service.
3. Open the rsreportserver.config file for editing.
4. In the file, locate the <AuthenticationTypes> block.
   - The block resembles the following example.
   ```xml
   <Authentication>
   <AuthenticationTypes>
   <RSWindowsNegotiate/>
   <RSWindowsNTLM/>
   </AuthenticationTypes>
   ... 
   </Authentication>
   ```
5. Remove any existing parameters and add the <RSWindowsBasic/> parameter to the <AuthenticationTypes> XML element.
   - The modified block resembles the following block.
   ```xml
   <Authentication>
   <AuthenticationTypes>
   <RSWindowsBasic/>
   </AuthenticationTypes>
   ... 
   </Authentication>
   ```
6. Save the configuration file.
7. Start the SSRS service.
What to do next

To authenticate VCM reports with Kerberos, see "Configure Kerberos Authentication" on page 82.

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 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 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 84.

Configure the VCM Collector Components

The combined VCM Collector and Web server contains the VCM software application, VCM services, and the OS Provisioning Server. 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, you configure the Web server and VCM Collector components on the same VCM Collector machine.

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 2008 Feature Pack to download SQL XML 4.0 and SP1 in the following procedure. See the online Microsoft Download Center.
- Verify that you can access the Microsoft Download Center, Microsoft SQL Server 2008 R2 Feature Pack to download and install the SQLCMD utility x64 package (SqlCmdLnUtils.msi) and the Native Client (sqlncli.msi) in the following procedure. See the online Microsoft Download Center. The SQL Command Line Tools in the SQL Server 2008 R2 Feature Pack are required on the combined VCM Collector and Web server.

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

**Procedure**

1. Download and install SQL XML 4.0 and SP1, X64 Package.

2. Download and install SQL Server 2008 R2 Command Line Utilities, which includes the SQLCMD utility, X64 Package (SqlCmdLnUtils.msi).

   The SQL Command Line Tools in the SQL Server 2008 R2 Feature Pack are required on the combined VCM Collector and Web server.

3. Download and install the SQL Server 2008 R2 Native Client, X64 Package (sqlncli.msi).

   The Native Client from the SQL Server 2008 R2 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 install VCM. See "Installing VCM" on page 117.
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 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.

Figure 10–1. Three-Tier Split Installation

### 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 23.
- Connect the database server machine, Web server machine, and VCM Collector machine to the domain.
- Obtain the SQL Server 2008 R2 Enterprise or Standard edition installation disk or verify access to a file share where the installer resides.

Procedure

1. "Verify that the Installing User is an Administrator" on page 88
   The user who installs the Windows Server 2008 R2 operating system must be an Administrator and a domain account.

2. "Install and Configure a Windows Server 2008 R2 Operating System" on page 89
   To prepare your Windows machine for VCM installation, install the Windows Server 2008 R2 operating system on each Windows machine in your installation configuration and verify that the settings are configured for VCM operation.

3. "Configuring the VCM Database Server" on page 91
   To set up the VCM databases, you must configure the before you install VCM. In a two-tier split installation configuration, the resides on . The databases include VCM, VCM_Coll, VCM_Raw, and VCM_UNIX.

4. "Configure the Web Server" on page 97
   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.

5. "Configure the VCM Collector" on page 112
   The combined VCM Collector and Web server contains the VCM software application, VCM services, and the OS Provisioning Server. 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

Use VCM Installation Manager to install the VCM components. See "Installing VCM" on page 117.

Verify that the Installing User is an Administrator

The user who installs the Windows Server 2008 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 a Windows Server 2008 R2 Operating System" on page 89.

Install and Configure a Windows Server 2008 R2 Operating System

To prepare your Windows machine for VCM installation, install the Windows Server 2008 R2 operating system on each Windows machine in your installation configuration and verify that the settings are configured for VCM operation.

Prerequisites

- Verify that the person who performs these procedures uses a domain account with local administrator rights.
- The user who installs the Windows Server 2008 R2 operating system must be an Administrator and a domain account. See "Verify that the Installing User is an Administrator" on page 88.

Procedure

1. Install Microsoft Windows Server 2008 R2 on your Windows machine.

2. Verify that the computer name settings for your Windows machine is a valid DNS machine name with no underscores.
   If you attempt to change the machine name after the machine is identified as a Collector, problems might occur with VCM, SQL Server, and SQL Server Reporting Services.
Configure the Operating System Locale Settings
To set the language for VCM installation, verify that your Windows Server Locale Setting is configured correctly.

Procedure
1. In Windows Explorer, click Start and select Control Panel > Clock, Language, and Region.
2. Click Region and Language.
3. Click the Administrative tab and set the language to English (United States).

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 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" on page 91.
Configuring the VCM Database Server

To set up 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 dedicated machine. The databases include VCM, VCM_Coll, VCM_Raw, and VCM_UNIX.

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 5.6 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 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 or Enterprise edition of SQL Server. You must install the 64-bit SQL Server 2008 R2, English (United States) 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.

Set the Internet Explorer Enhanced Security Mode

Depending on the security level required for your environment, you might need to turn off Internet Explorer Enhanced Security Mode for Administrators and Users to ensure that the database components are configured correctly.

Procedure

1. On the database server, click Start and select All Programs > Administrative Tools > Server Manager.
2. In the left pane, click Server Manager.
3. In the Server Summary pane, locate the Security Information area.
4. Click Configure IE ESC.
5. In the Internet Explorer Enhanced Security Configuration pop-up window, under Administrators, select Off.

Install SQL Server on the Database Server

In a three-tier split installation configuration, the VCM database server resides on a dedicated 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.
CAUTION  If your Windows machine has an evaluation version of SQL Server Standard Edition or Enterprise Edition, use it only for evaluation purposes. Do not use an evaluation version in a production environment, because it is not officially released for production.

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 5.6 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 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
Obtain the SQL Server 2008 R2 Enterprise or Standard edition installation disk or verify access to a file share where the installer resides.

Procedure
1. Start the SQL Server 2008 R2 installation.
2. Perform the actions to install SQL Server 2008 R2 Enterprise or Standard edition.

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

Instance Features:
<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Database Engine Services</td>
</tr>
<tr>
<td></td>
<td>Shared Features:</td>
</tr>
<tr>
<td></td>
<td>• Client Tools Connectivity</td>
</tr>
<tr>
<td></td>
<td>• SQL Server Books online</td>
</tr>
<tr>
<td></td>
<td>• Management Tools - Basic and Management Tools - Complete</td>
</tr>
</tbody>
</table>

**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.

**Disk Space Requirements**
Review the disk usage summary.

**Server Configuration**
Click Use the same account for all SQL Server services and enter the NTAUTHORITY\SYSTEM account and password.

**Database Engine Configuration**
Select Mixed Mode (SQL Server authentication and Windows authentication), enter and confirm the password, and click Add Current User to add the account to the SQL Server administrators. Although the VCM installation system checks require that SQL Server Mixed Mode authentication is enabled during the installation of VCM, you can change SQL Server back to Windows Integrated authentication after the installation is finished.

**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 2008 R2. 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. Click Start and select All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio.
2. Right-click the SQL instance and select Properties.
3. Confirm the General page server properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>10.50.1600.1</td>
</tr>
<tr>
<td>Language</td>
<td>English (United States). If the language is not correct, uninstall and install the correct version of SQL Server.</td>
</tr>
<tr>
<td>Server Collation</td>
<td>SQL_Latin1_General_CP1_CI_AS. If the server collation is not correct, uninstall and reinstall SQL Server.</td>
</tr>
</tbody>
</table>

4. Select and confirm the Security page server properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Authentication mode</td>
<td>Recommended. Select this mode.</td>
</tr>
<tr>
<td>SQL Server and Windows Authentication mode</td>
<td>Although this setting is acceptable for VCM, Windows Authentication mode is recommended.</td>
</tr>
</tbody>
</table>

5. Select and confirm the Database Settings page server properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default index fill factor</td>
<td>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.</td>
</tr>
<tr>
<td>Recovery interval (minutes)</td>
<td>Type or select 5.</td>
</tr>
</tbody>
</table>

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" on page 94.

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 2008 R2, 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 2008 R2 were installed, verify and reset the SQL Server server name.
Procedure

1. Click Start and select All Programs > Microsoft SQL Server 2008 R2 > 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.
      ```sql
      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 2008 R2 > Configuration Tools > SQL Server Configuration Manager > SQL Server 2008 R2 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 page 95.

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. Click Start and select All Programs.
2. Click Microsoft SQL Server 2008 R2 and select SQL Server Management Studio.
3. Expand the server, expand Security, expand Server Roles.
4. Double-click sysadmin and view the members of the sysadmin role.
5. Verify that the account to use for the SQL Server Agent service is a member of the sysadmin fixed role.
6. If the account is not a member of the sysadmin fixed role, add this role to the account.

What to do next

Select the SQL Server Agent service account. See "Select the SQL Server Agent Service Account" on page 96.
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 on 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 5.6 supports Active/Passive 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 95.

Procedure

1. On the VCM database server machine, click Start and select All Programs.
2. Click Microsoft SQL Server 2008 R2 and select 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 on option and provide the account information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-in account</td>
<td>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.</td>
</tr>
<tr>
<td>This account</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 page 97.
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. Click Start and select All Programs > Microsoft SQL Server 2008 R2 > 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 dedicated Web server. See "Configure the Web Server" on page 97.

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.

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 5.6 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 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 87.
- 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 101.
- 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 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 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| 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 Extension  
- ISAPI Filters  
- Server Side Includes |
| Health and Diagnostics | Select these options:  
- HTTP Logging  
- Request Monitor |
| Security | Select these options:  
- Basic Authentication  
- Request Filtering |
<p>| Performance | Select: |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Static Content Compression</td>
</tr>
</tbody>
</table>

**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**

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

**Procedure**

1. On the Collector, right-click **Computer** and select **Manage** to open Server Manager.
2. In Server Manager, 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**.
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.

<table>
<thead>
<tr>
<th>Role Service Category</th>
<th>Role Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common HTTP Features</td>
<td>Static Content&lt;br&gt;Default Document&lt;br&gt;Directory Browsing&lt;br&gt;HTTP Errors&lt;br&gt;HTTP Redirection</td>
</tr>
<tr>
<td>Application Development</td>
<td>ASP.NET&lt;br&gt;.NET Extensibility&lt;br&gt;ASP&lt;br&gt;ISAPI Extensions&lt;br&gt;ISAPI Filters&lt;br&gt;Server Side Includes</td>
</tr>
<tr>
<td>Health and Diagnostics</td>
<td>HTTP Logging&lt;br&gt;Logging Tools&lt;br&gt;Request Monitor&lt;br&gt;Tracing</td>
</tr>
<tr>
<td>Role Service Category</td>
<td>Role Service</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td>IP and Domain Restrictions</td>
</tr>
<tr>
<td>Performance</td>
<td>Static Content Compression</td>
</tr>
<tr>
<td></td>
<td>Dynamic Content Compression</td>
</tr>
<tr>
<td>Management Tools</td>
<td>IIS Management Console</td>
</tr>
<tr>
<td></td>
<td>IIS Management Scripts and Tools</td>
</tr>
<tr>
<td></td>
<td>Management Service</td>
</tr>
</tbody>
</table>

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 Bindings**

IIS bindings 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.
<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous Authentication</td>
<td>Set to <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>ASP.NET Impersonation</td>
<td>Set to <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Basic Authentication</td>
<td>Set to <strong>Enabled</strong>.</td>
</tr>
<tr>
<td>Forms Authentication</td>
<td>Set to <strong>Disabled</strong>.</td>
</tr>
</tbody>
</table>

**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](#)" on page 101.

**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" on page 102.

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 page 103.

Installing and Configuring SSRS on the Web Server

SQL Server Reporting Services (SSRS) is used to generate VCM reports. Before you install and configure SSRS, you must back up your SSRS key and clear the Internet Explorer Protected Mode.

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. For details about how to use this utility, see the online Microsoft Support center.

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. Double-click rskeymgmt.exe and follow the prompts to copy your SSRS key set to a removable media device and store it in a secure location.

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 page 103.
- Disable the Internet Explorer Protected Mode. See "Disable IE Protected Mode for SSRS" on page 103.
- Obtain the SQL Server 2008 R2 Enterprise or Standard edition installation disk or verify access to a file share where the installer resides.

Procedure

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

<table>
<thead>
<tr>
<th>Wizard Page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server Installation Center</td>
<td>Click New installation or add features to an existing installation.</td>
</tr>
<tr>
<td>Setup Support Rules</td>
<td>Click Install and verify that all of the rules pass. To view the detailed system configuration check report, click the link.</td>
</tr>
<tr>
<td>Setup Support Files</td>
<td>Click Install to install the setup support files.</td>
</tr>
<tr>
<td>Setup Support Rules – for SQL Server Setup support files</td>
<td>Verify that all of the rules passed.</td>
</tr>
<tr>
<td>Installation Type</td>
<td>Select New installation or add shared features.</td>
</tr>
<tr>
<td>Product Key</td>
<td>Verify that the product key is entered.</td>
</tr>
<tr>
<td>License Terms</td>
<td>Accept the license terms.</td>
</tr>
<tr>
<td>Setup Role</td>
<td>Select SQL Server Feature Installation.</td>
</tr>
<tr>
<td>Feature Selection</td>
<td>Select the following options.</td>
</tr>
<tr>
<td></td>
<td>Reporting Services</td>
</tr>
</tbody>
</table>
Wizard Page | Action
--- | ---
- Client Tools Connectivity
- SQL Server Books Online
- Management Tools - Basic
- 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.

Disk Space Requirements | (Optional) Review the disk usage summary.

Server Configuration | Click Use the same account for all SQL Server services and enter the NTAUTHORITY\SYSTEM account and password.

Database Engine Configuration | Select Mixed Mode (SQL Server authentication and Windows authentication), enter and confirm the password, and click Add Current User to add the account to the SQL Server administrators. Although the VCM installation system checks require that SQL Server Mixed Mode authentication is enabled during the installation of VCM, you can change SQL Server back to Windows Integrated authentication after the installation is finished.

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.

### Configure SSRS

SQL Server Reporting Services (SSRS) is a server-based report generation software system that is administered using a web interface and used to deliver reports. You must configure SSRS manually in your three-tier split 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 103.
- Disable the Internet Explorer Protected Mode. See "Disable IE Protected Mode for SSRS" on page 103.
Procedure

1. On your Web server, start SQL Server 2008 R2 Reporting Services Configuration Manager.
   a. Click **Start** and select **Run**.
   b. Type `rsconfigtool.exe`.
   c. In the Reporting Services Configuration Connection dialog box, click **Connect** to connect and log in to SQL Server 2008 R2 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 and select the language as **English (United States)**.
   h. Set the Report Server Mode to **Native Mode** and click **Next**.
   i. In the Credentials pane, change the Authentication Type to **Windows Credentials**.
   j. Specify an account that has permission to connect from the Web server to the database server, specify the password for the account, and click **Next**.
   k. In the Summary pane, review the selections and click **Next**.
   l. 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Set to All Assigned (Recommended).</td>
</tr>
<tr>
<td>TCP Port</td>
<td>Set to 80.</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>Not Selected</td>
</tr>
</tbody>
</table>

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 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" on page 107.

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 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, locate the rsreportserver.config file.

   The default location is C:\Program Files\Microsoft SQL Server\ReportingServices\ReportServer\rsreportserver.config.

2. Stop the SSRS service.

3. Open the rsreportserver.config file for editing.
4. In the file, locate the `<AuthenticationTypes>` block.  
   The block resembles the following example.
   
   ```xml
   <Authentication>
     <AuthenticationTypes>
       <RSWindowsNegotiate/>
       <RSWindowsNTLM/>
     </AuthenticationTypes>
   ...  
   </Authentication>
   ```

5. Remove any existing parameters and add the `<RSWindowsBasic/>` parameter to the `<AuthenticationTypes>` XML element.  
   The modified block resembles the following block.
   
   ```xml
   <Authentication>
     <AuthenticationTypes>
       <RSWindowsBasic/>
     </AuthenticationTypes>
   ...  
   </Authentication>
   ```

6. Save the configuration file.

7. Start the SSRS service.

**What to do next**

To authenticate VCM reports with Kerberos, see "Configure Kerberos Authentication" on page 108.

**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 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 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\ReportingServices\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 111.

**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**

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" on page 112.
Configure the VCM Collector

The VCM Collector contains the VCM software application, VCM services, and the OS Provisioning Server. 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, dedicated machines.

Prerequisites

- Perform the prerequisite tasks for your three-tier split installation configuration. See “Three-Tier Split Installation” on page 87.
- From the VCM Collector, verify that you can access the Microsoft Download Center, Microsoft SQL Server 2008 Feature Pack to download SQL XML 4.0 and SP1 in the following procedure. See the online Microsoft Download Center.
- Verify that you can access the Microsoft Download Center, Microsoft SQL Server 2008 R2 Feature Pack to download and install the SQLCMD utility x64 package (SqlCmdLnUtils.msi) and the Native Client (sqlncli.msi) in the following procedure. See the online Microsoft Download Center. The SQL Command Line Tools in the SQL Server 2008 R2 Feature Pack are required on the Web server and the VCM Collector.
- Install .NET Framework 3.5.1 on the Windows Server 2008 R2 machines where Package Studio will be installed.

Procedure

1. Download and install SQL XML 4.0 and SP1, X64 Package.
2. Download and install SQL Server 2008 R2 Command Line Utilities, which includes the SQLCMD utility, X64 Package (SqlCmdLnUtils.msi).
   The SQL Command Line Tools in the SQL Server 2008 R2 Feature Pack are required on the Web server and the VCM Collector.
3. Download and install the SQL Server 2008 R2 Native Client, X64 Package (sqlncli.msi).
   The Native Client from the SQL Server 2008 R2 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 5.6 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.

The VCM Collector requires the .NET 3.5.1 Framework. Software provisioning Package Studio requires .NET 3.5.1 and Software provisioning Package Manager requires either .NET 3.5.1 or .NET 4.0.
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, install it from the Microsoft Web site.

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.

Procedure
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
Prepare to use VCM Remote. See "Using VCM Remote" on page 114.
**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.
- Install and Configure the VCM Remote client on the VCM managed machine.

**What to do next**

Export the Collector Certificate. See "Export the Collector Certificate from the VCM Collector" on page 114.

**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 87.

**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" on page 115.

**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 page 114.

**Procedure**

1. Open a command prompt and use the `xcopy` command to copy and paste the VCM Collector certificate file from the VCM 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**

Configure the VCM Remote Client. See "Configure the VCM Remote Client” on page 116.
**Configure the VCM Remote Client**

The VCM Remote client is the communication and management mechanism that you use to manage mobile Windows machines as they connect to and disconnect from the network. VCM Remote is composed of the VCM Remote Server and VCM Remote Client.

The VCM Remote Server is installed when you run the VCM Installation Manager and install VCM. You must install and configure the VCM Remote Client separately.

When you install the VCM Remote Client, you must enter the name of the Web server name and the VCM Collector Certificate.

**Prerequisites**

- Export the VCM Collector certificate from the VCM Collector machine.
- Import the VCM Collector certificate to the Web server machine.
- Locate the *VCM Administration Guide* to install and configure the VCM Remote Client in the following procedure.
- Run the VCM Remote Client installation from a command line or with a remote command. See the *VCM Administration Guide*. During the VCM Remote Client installation, you enter the name of the Web server name and the VCM Collector Certificate.

**Procedure**

1. After the VCM Remote Client installation is finished, go to the directory where you installed the software. The location is typically at `C:\Program Files\VMware\VCM Remote Client`.

2. Open the `CSIRemoteHTTP_debug.txt` log file and verify that no errors occurred.
   
   You must resolve any errors before you proceed.

3. Set the HTTP polling interval at the VCM Remote Client with the following command.

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Configuresoft\ECMRemoteClient] "Collector"= ">>Name of theAppserver<<"
   "MinTimeBetweenHTTPPostInSeconds"=dword:_>>Seconds<< "Debug"=dword:00000001
   ```

**What to do next**

Review the DCOM and port requirements, and install VCM. See "Installing VCM" on page 117.
Installing VCM

After you perform the system prerequisite tasks and set up your installation configuration, you must enable the required ports before you use Installation Manager to install VCM.

**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 page 117.

**Use Installation Manager to Install VCM**

The Installation Manager for VMware vCenter Configuration Manager (VCM) is a standalone application that evaluates your Windows machine to confirm that it is properly configured for VCM installation, and deploys the VCM packages to your server or servers.

VCM 5.6 supports 64-bit environments that include 64-bit hardware, the 64-bit Windows Server 2008 R2 operating system, and SQL Server 2008 R2.

VCM 5.6 supports single-tier, two-tier, and three-tier installation configurations. Installation Manager performs the following actions.

- Evaluates managed machines to verify that they meet the hardware and software prerequisites for VCM installation.
- Validates the VCM code during the installation.
- Installs the selected components and tools in the correct order on your physical or virtual Windows servers.
- Verifies that all components install successfully.

When you install VCM and related components, the default settings might not match your configuration. During the installation, read the information that appears for each configurable component and enter the required information.
When you prepare your Windows machine for a VCM installation, determine your requirements based on the components to install in your configuration. Use the hardware requirement worksheet and associated tables to assess your requirements based on your individual environment and whether your installation configuration includes a single server or multiple servers.

**CAUTION** The Microsoft Windows Installer (MSI) caches data in the %windir%\Installer\ folder, which includes the VCM MSI files. If this data is removed, any MSI modify, repair, or uninstall operations will not succeed.

### Install VCM

Use Installation Manager to install VCM in these configurations and configure the components during installation.

#### Prerequisites

- Review the list of supported platforms. See "Hardware and Operating System Requirements for VCM Managed Machines" on page 157.

- If you are migrating a version of VCM to VCM 5.6, a SQL Server version to 2008 R2, or a 32-bit environment to a 64-bit environment, see "Upgrading or Migrating VCM" on page 127.

**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 installation from a network location or insert the VCM installation disk into the Windows machine.

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

2. Select **Run Installation Manager** 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

- Although the VCM installation system checks require that SQL Server Mixed Mode authentication is enabled during the installation of VCM, you can change SQL Server back to Windows Integrated authentication after the installation is finished.

- 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.

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 117.

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" on page 120.

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 "Configuring SQL Server for VCM" on page 121.
Configuring SQL Server for VCM

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.

**SQL Server Database Settings**

Configure the database settings for VCM to optimize SQL Server performance.

**Procedure**

1. Click Start.
2. Select All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio.
3. Right-click the SQL instance that you installed and select Properties.
4. In the Select a page area, select Database Settings.
5. 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.
6. 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 the SQL Server Processor settings to set the maximum worker threads or boost the SQL Server priority.

**Procedure**

1. Click **Start**.
2. Select **All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
3. Right-click the SQL instance that you installed and select **Properties**.
4. In the navigation pane, select **Processors**.
5. In the Enable processors area, select **Automatically set I/O affinity mask for all processors**.
6. Select **I/O Affinity** for all processors in the Enable processors list.
7. 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.
8. Click **OK** to save the settings.

**SQL Server IO Configuration**

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

- **RAID 0.** Striping Without Parity. In this configuration, each block of data is written to each disk in the array in a 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 IO Channel Throughput**

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

After you download and install SQLIO, configure the following SQLIO settings to ensure an accurate report of IO throughput.

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

When you execute SQLIO, verify that you create baseline information for each IO channel (logical disk) to be used for VCM data, as well as testing both read and write operations.
You can upgrade or migrate your existing VCM environment to VCM 5.6, which supports 64-bit environments that include 64-bit hardware, 64-bit Windows Server 2008 R2 and SP1, and SQL Server 2008 R2 and SP1.

You can use Installation Manager to upgrade from VMware VCM 5.3, EMC Ionix SCM 5.0 or later, or ConfigureSoft ECM 4.11.1 or later to VCM 5.6.

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 5.6 and later do 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.

### Upgrades

An upgrade to VCM 5.6 uses an existing VCM Collector installation. You upgrade the operating system, SQL Server, and VCM to the versions associated with VCM 5.6.

VCM 5.6 supports the following upgrade paths.

- Upgrade from VCM 5.4 or 5.4.1, which are 64-bit single-server installations. Updates to Windows Server 2008 R2 or SQL Server 2008 R2 are not required.
- Upgrade from a 64-bit single-server installation that includes VMware VCM 5.3 or later, EMC Ionix SCM 5.0 or later, or ConfigureSoft ECM 4.11.1 or later. You must upgrade to Windows Server 2008 R2 and SQL Server 2008 R2.

**What to do next**

Upgrade your VCM environment to VCM 5.6. See "Upgrading VCM and Components" on page 138.

### Migrations

A migration to VCM 5.6 requires you to prepare new hardware and software for your environment. VCM 5.6 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 5.6.
For a migration, you must update your hardware to 64-bit, update the operating system to the 64-bit Windows Server 2008 R2 operating system, update to SQL Server 2008 R2, and update SQL Server Reporting Services. Then you can migrate your existing VCM, SCM, or ECM installation to your new VCM 5.6 environment.

What to do next

Understand the prerequisites to prepare and migrate your VCM environment to VCM 5.6. See "Prerequisites to Migrate VCM" on page 128.

Prerequisites to Migrate VCM

Before you migrate your existing VCM environment to VCM 5.6, you must perform several prerequisites.

- Review and understand the migration scenarios. See "Upgrading or Migrating VCM" on page 127.
- 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 19.
- 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 5.6. See "Software and Operating System Requirements for Collector Machines" on page 19.
- 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 21.
- Back up your databases. See "Back Up Your Databases" on page 129.
- Back up the CMFILES$ share. See "Back up Your Files" on page 129.
- 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 page 129.
- 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.
- Run the VCM Installation Manager to perform system checks on your VCM Collector to ensure that it is ready for the installation of VCM 5.6. See "Use Installation Manager to Install VCM" on page 117.
- Obtain the installation package from theDownload VMware vCenter Configuration Manager Web site
or the VCM 5.6 CD. You will install VCM as a final step in the migration process.

- Download the VCM SQL Migration Helper Tool from the Download VMware vCenter 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 5.6, 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>
<thead>
<tr>
<th>Version to Migrate</th>
<th>Back up these databases</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware VCM</td>
<td>VCM, VCM_Coll, VCM_UNIX, ReportServer, master, and msdb</td>
</tr>
<tr>
<td>EMC Ionix SCM</td>
<td>SCM, SCM_Coll, SCM_UNIX, ReportServer, master, and msdb</td>
</tr>
<tr>
<td>Configuresoft ECM (versions 4.11.1 to 5.0)</td>
<td>ECM, ECM_Coll, ECM_UNIX, ReportServer, master, and msdb</td>
</tr>
</tbody>
</table>

**Back up Your Files**

Before you migrate an existing VCM environment to VCM 5.6, 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.exe.
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.
12. On the Export Private Key page, select No 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.

The .cer file is now in the location that you specified in the export process.

Migrating VCM

To prepare your environment for VCM 5.6, 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.

Prerequisites

Before you migrate any part of your existing VCM environment to VCM 5.6, you must perform the prerequisites. See "Prerequisites to Migrate VCM" on page 128.

Procedure

- "Migrate Only Your Database " on page 130
  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 131
  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 5.6" on page 132
  Migrate an existing 32-bit Collector to VCM 5.6. A migration to VCM 5.6 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 to VCM 5.6" on page 134
  Migrate an existing 64-bit Collector to VCM 5.6. A migration to VCM 5.6 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-Server Installation" on page 135
  Migrate an existing split installation to a single-tier, two-tier, or three-tier installation configuration for VCM 5.6.

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 5.6. See "Upgrading or Migrating VCM" on page 127.
- Understand the prerequisites to migrate your VCM environment to VCM 5.6. See "Prerequisites to Migrate VCM" on page 128.
- Understand how to attach a SQL server database in SQL Server Management Studio. See the Microsoft MSDN Library.
- Install SQL Server 2008 R2 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 installed.
2. On the prepared machine, start SQL Server Management Studio.
3. Attach the database to SQL Server 2008 R2.
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 5.6. See "Use Installation Manager to Install VCM" on page 117.

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 Configureof ECM.

Previous versions of VMware VCM, EMC Ionix SCM, and Configureof 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 5.6.

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.6. See "Upgrading or Migrating VCM" on page 127
- Perform the prerequisites to migrate your VCM environment to VCM 5.6. See "Prerequisites to Migrate VCM" on page 128.
- Ensure that your environment is functional before you replace it and upgrade to VCM 5.6.

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 operating system on the 64-bit Windows Collector machine.
6. Upgrade VCM to VCM 5.6.

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 149.
- Log in to VCM.

Migrate a 32-bit Environment Running VCM 5.3 or Earlier to VCM 5.6
Migrate an existing 32-bit Collector to VCM 5.6. A migration to VCM 5.6 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 CMFILE$ 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 5.6. See "Upgrading or Migrating VCM" on page 127.
- Perform the prerequisites to migrate your VCM environment to VCM 5.6. See "Prerequisites to Migrate VCM" on page 128.
- 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 2008 R2 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 5.6 installation package on the Download VMware vCenter Configuration Manager Web site or obtain the VCM 5.6 CD.
- Ensure that your environment is functional before you migrate VCM 5.3 or earlier to VCM 5.6.
Procedure

2. Install SQL Server 2008 R2 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.
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 5.6 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 5.6.
    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.

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 149.
- Log in to VCM.

Migrate a 64-bit Environment Running VCM 5.3 or Earlier to VCM 5.6

Migrate an existing 64-bit Collector to VCM 5.6. A migration to VCM 5.6 requires you to prepare new software for your environment and install the required software components.

Use this method as part of the VCM 5.6 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 5.6. 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 5.6. See "Upgrading or Migrating VCM" on page 127.
- Perform the prerequisites to migrate your VCM environment to VCM 5.6. See Prerequisites to Migrate VCM" on page 128.
- 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 2008 R2 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 5.6 installation package on the Download VMware vCenter Configuration Manager Web site or obtain the VCM 5.6 CD.
- Ensure that your environment is functional before you migrate VCM 5.3 or earlier to VCM 5.6.

Procedure

2. Install SQL Server 2008 R2 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.

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_changedowner stored procedure to change the ownership of the databases.

7. Start the VCM 5.6 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 5.6.

    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.


   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 149.
   - Log in to VCM.

Migrate a Split Installation of VCM 5.3 or Earlier to a Single-Server Installation

Migrate an existing split installation to a single-tier, two-tier, or three-tier installation configuration for VCM 5.6.
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 5.6, you can migrate a previous split installation to any of the following configurations.

- **“Single-Tier Server Installation” on page 37**
  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 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 the Windows Server 2008 R2 database server machine, and the VCM Collector and Web components reside on the second Windows Server 2008 R2 machine.

- **“Three-Tier Split Installation” on page 87**
  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 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 5.6. See "Upgrading or Migrating VCM" on page 127.
- Perform the prerequisites to migrate your VCM environment to VCM 5.6. See Prerequisites to Migrate VCM on page 128.
- 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 2008 R2 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 5.6 installation package on the Download VMware vCenter Configuration Manager Web site or obtain the VCM 5.6 CD.
- Ensure that your environment is functional before you migrate VCM 5.3 or earlier to VCM 5.6.
Procedure
2. Install SQL Server 2008 R2 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.
   For a split installation, you must attach the databases from the database Server to SQL Server 2008 R2.
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_changeowner stored procedure to change the ownership of the databases.
7. Start the VCM 5.6 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 5.6.
    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.
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 149.
- Log in to VCM.

How to Recover Your Collector Machine if the Migration is not Successful

If the migration to VCM 5.6 failed, you must perform several steps to recover your VCM Collector machine. Before you attempt another migration to VCM 5.6, 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 130.
- Understand the scenarios to migrate your VCM environment to VCM 5.6. See "Upgrading or Migrating VCM" on page 127.
- Understand the prerequisites to migrate your VCM environment to VCM 5.6. See "Prerequisites to Migrate VCM" on page 128.
- 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 CMFILE$ share.

Upgrading VCM and Components

To prepare your environment for VCM 5.6, you can upgrade VCM, Windows Agents, UNIX or Linux Agents, and VCM Remote Clients.

An upgrade to VCM 5.6 uses an existing VCM Collector installation. Before you migrate any part of your existing VCM environment to VCM 5.6, you must perform several prerequisites.
Prerequisites

- Review and understand the upgrade scenarios. See "Upgrading or Migrating VCM" on page 127.
- Verify that your VCM Collector meets all of the hardware requirements for a 64-bit environment. See "Hardware Requirements for Collector Machines" on page 15.
- 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 19.
- Obtain the installation package from the Download VMware vCenter Configuration Manager Web site or the VCM 5.6 CD.

Procedure

- "Upgrade VCM" on page 139
  An upgrade to VCM 5.6 uses an existing VCM Collector installation. You can upgrade a 64-bit environment that is running VCM 5.3 or earlier to VCM 5.6.
- "Upgrade Existing Windows Agents" on page 140
  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 141
  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 141
  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.
- "Upgrade Virtual Environments Collections" on page 144
  To upgrade vCenter collections, install the VCM 5.4 Agent or later on the Windows machines running vCenter.

Upgrade VCM

An upgrade to VCM 5.6 uses an existing VCM Collector installation. You can upgrade a 64-bit environment that is running VCM 5.3 or earlier to VCM 5.6.

Prerequisites

Perform the prerequisites to upgrade VCM on the Collector. See "Upgrading VCM and Components" on page 138.

Procedure

1. On your Collector machine, upgrade the operating system to Windows Server 2008 R2.
2. Uninstall the 32-bit version of SQL Server Reporting Services (SSRS) 2005.
5. Click Start.
6. Select All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > Reporting Services Configuration Manager.
7. Configure SSRS 2008 to use the existing ReportServer database.
   a. Select the existing ReportServer database.
   b. Configure the Web Service and Report Manager URLs.
   c. Select the Encryption Keys option to delete encrypted content so that the new installation of SSRS can use the existing SSRS database.

8. Run the VCM Installation Manager to upgrade the existing VCM software version to 5.6.

What to do next
Log in to VCM and upgrade your VCM Windows Agents.

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 157.
- 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All machines</td>
<td>Upgrades the Agent on all machines that appear in the list of licensed machines.</td>
</tr>
<tr>
<td>Filtered machines</td>
<td>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.</td>
</tr>
<tr>
<td>Selected machine(s) only</td>
<td>Upgrades the Agent only on selected individual machines.</td>
</tr>
</tbody>
</table>

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.


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.

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 UNIX and Linux platforms. Other UNIX platforms are only supported up to a specific Agent version. For a complete list of UNIX Agents supported on UNIX and Linux platforms, see "Hardware and Operating System Requirements for VCM Managed Machines" on page 157.

Prerequisites

- Identify UNIX machines that are not supported for upgrade to the VCM 5.6 Agent. See "Hardware and Operating System Requirements for VCM Managed Machines" on page 157.

- Understand Red Hat server and workstation licensing for different versions of VCM. See "Red Hat Server and Workstation Licensing" on page 142.


- If you install the VCM Agent on HP-UX 11.11 platforms, install patch PHSS_30966.
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 5.6, physical and virtual machines are licensed as servers or workstations.

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" on page 143.

**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 on the Download VMware vCenter Configuration Manager Web site.

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 "Upgrade Virtual Environments Collections" on page 144.

**Upgrade Virtual Environments Collections**

VCM 5.5 and later includes the ability to collect data directly from instances of vCenter Server, vCloud Director, and vShield Manager. Use this new collections method to collect your virtual environments data and to run actions on vCenter Server, hosts, and guests. See the VCM Administration Guide.

The Agent Proxy configuration is only used to collect the ESX logs and Linux data types form the ESX Service Console OS.

**Upgrade Agent Proxy Machines**

When you upgrade a Collector to VCM 5.6, 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.

**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 page 145
  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 page 146
  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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Machines</td>
<td>Runs the process on all eligible machines.</td>
</tr>
<tr>
<td>Selected Machines Only</td>
<td>Runs the process on all machines listed in the lower pane.</td>
</tr>
<tr>
<td>Filtered Machines</td>
<td>Creates a filter based on the machine name or domain name.</td>
</tr>
<tr>
<td>Arrow buttons</td>
<td>Moves a selected machine name between panes.</td>
</tr>
</tbody>
</table>

6. On the Option page, configure the options and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install From</td>
<td>Selects the name of the Collector used to manage virtual machines.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Sets the schedule to run the action.</td>
</tr>
</tbody>
</table>

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 5.6.
- 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.
Unregister the Previous Version of 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.

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 \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" on page 147.

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 page 147.
- Locate the procedure to upgrade VCM. See "Upgrading VCM and Components" on page 138.

Procedure

- Upgrade VCM.

What to do next

Register the new vSphere Client VCM Plug-In. See the VCM Administration Guide.
Perform routine maintenance on your VCM configuration management database (CMDB) 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 "Use Installation Manager to Install VCM" on page 117.
- Understand the database recovery models. See "Database Recovery Models" on page 151.

Procedure

1. "Customize VCM and Component-Specific Settings" on page 149
   Customize the general VCM settings and the component-specific settings for your environment.

2. "Configure Database File Growth" on page 151
   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 152
   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 2008 R2" on page 153
   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 CMDB into your Backup and Disaster Recovery Plans" on page 155
   Consider your VCM configuration management 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. On your VCM Collector, 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent - General</td>
<td>Configures the general characteristics of the Windows Agent operation.</td>
</tr>
<tr>
<td>Agent - Thread Priority</td>
<td>Configures priorities for collections while running on managed machines.</td>
</tr>
<tr>
<td>Data Retention</td>
<td>Configures the time to retain each VCM data type in the database.</td>
</tr>
<tr>
<td>Custom Information</td>
<td>Displays the Windows Custom Information script and output types.</td>
</tr>
</tbody>
</table>

4. Click **UNIX** and configure the settings to communicate with the VCM UNIX Agent for your collection types.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent - General</td>
<td>Configures the general characteristics of the UNIX Agent operation.</td>
</tr>
<tr>
<td>Agent - RunAsSuid</td>
<td>Configures data types as RunAsSuid for selected operating systems during Agent operation.</td>
</tr>
<tr>
<td>Agent - Nice</td>
<td>Configures the Nice settings for each data type during Agent operation.</td>
</tr>
<tr>
<td>Data Retention</td>
<td>Configures the time to retain each VCM data type in the database.</td>
</tr>
<tr>
<td>Custom Information Types</td>
<td>Adds custom data types and directives to collect data and parse text files.</td>
</tr>
<tr>
<td>Restricted Path</td>
<td>Configures restricted paths for editing file properties.</td>
</tr>
</tbody>
</table>

5. For the VCM functional areas and the network authority, review and update the component-specific settings for your environment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Extensions</td>
<td>Configures the hardware device and software configuration item settings.</td>
</tr>
<tr>
<td>Integrated Products</td>
<td>Configures settings for the VMware and EMC products that integrate with VCM.</td>
</tr>
<tr>
<td>OS Provisioning</td>
<td>Enables OS provisioning and configures the server connection timeout and user account.</td>
</tr>
<tr>
<td>Scripted Remediation Framework</td>
<td>Sets values for administrative parameters used in remediation scripts.</td>
</tr>
<tr>
<td>VCM for Active Directory</td>
<td>Configures the data retention settings for AD objects and the AD display settings.</td>
</tr>
<tr>
<td>VCM for Virtualization</td>
<td>Configures the data retention settings for vCenter, virtual machine hosts and guests, and the virtual machine logs.</td>
</tr>
<tr>
<td>Network Authority</td>
<td>Configures and manages the available domains, available accounts, and assigned</td>
</tr>
</tbody>
</table>
Configure the database file growth. See "Configure Database File Growth" on page 151.

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 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 2008 R2. In some environments, these default values can result in file fragmentation or reduced performance. The following procedure sets the autogrowth property in each database.

**Prerequisites**

Understand the database recovery models. See "Database Recovery Models" on page 151.
Procedure

1. Click Start.
2. Select All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio.
3. Expand the SQL instance.
4. Expand Databases.
5. Right-click VCM and select Properties.
6. In the left pane, select Files.
7. In the Autogrowth column, click the ellipsis button.
8. Select Enable Autogrowth.
9. 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.
10. In the Maximum File Size area, select Unrestricted File Growth and click OK.
11. 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.

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 page 151.
Procedure
1. Click Start.
2. Select All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio.
3. Expand the SQL instance.
4. Expand Databases.
5. Right-click VCM and select Properties.
6. Click Options.
7. In the Recovery model drop-down, select the recovery model and click OK.

What to do next
Create a maintenance plan for SQL Server 2008 R2. See ‘Create a Maintenance Plan for SQL Server 2008 R2’ on page 153.

Create a Maintenance Plan for SQL Server 2008 R2
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 2008 R2 servers that host the VCM database.

Procedure
1. Click Start.
2. Select All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio.
5. On the Select Plan Properties page, enter a maintenance plan name, select Single schedule for the entire plan or no schedule, and click Change.
6. 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.
7. Click OK to return to the Select Plan Properties page and click Next.
8. On the Select Maintenance Tasks page, select the following maintenance tasks and click Next.
   - Check Database Integrity
   - Rebuild Index
   - Update Statistics
   - Clean Up History
9. On the Select Maintenance Task Order page, order the maintenance tasks and click Next.
10. 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.

11. 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.

12. 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.

13. On the Define History Cleanup Task page, define how the maintenance plan will clean up historical data from the SQL Server 2008 R2 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.

   a. Select Write a report to a text file.
   b. Select a folder for the report and click Next.

15. 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.

16. 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 2008 R2 continues to operate efficiently. To view, save, copy, or send the report, click Report and select an option.
- Use VCM normally.

Incorporate the VCM CMDB into your Backup and Disaster Recovery Plans

Consider your VCM configuration management database as any other SQL database in your environment and incorporate the database into your corporate strategy for backup and disaster recovery.
VCM collects data from Windows and UNIX machines that VCM manages. The VCM Agent is supported on many different machine and operating system types.

**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 Windows or UNIX/Linux, except for HP-UX for Itanium servers.

Machines marked with an asterisk (*) include a pre-VCM 5.2.1 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

<table>
<thead>
<tr>
<th>Agent</th>
<th>Supported Operating System</th>
<th>Supported Hardware Platform</th>
<th>Platforms To Be Upgraded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Microsoft Windows 2003</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows 2003 R2</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft XP Professional (including SP3)</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft XP Professional (SP2 and earlier up to 5.2.1 Agent only)</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td>Supported Operating System</td>
<td>Supported Hardware Platform</td>
<td>Platforms To Be Upgraded</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Microsoft Vista Business (including SP1)</td>
<td>x86 and x64</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Microsoft Vista Ultimate (including SP1)</td>
<td>x86 and x64</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Microsoft Vista Enterprise (including SP1)</td>
<td>x86 and x64</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2008</td>
<td>x86 and x64</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 R2</td>
<td>x86 and x64</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 7 Business</td>
<td>x86 and x64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 7 Ultimate</td>
<td>x86 and x64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 7 Enterprise</td>
<td>x86 and x64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNIX/Linux</td>
<td>AIX 5L 5.3 (up to 5.4.0 Agent only)</td>
<td>RISC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AIX 6L 6.1, AIX 7.1</td>
<td>RISC and PowerPC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Debian 4.0 (Package LSB-Release is required)</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESX 4.1 Update 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11i v1.0 (11.11) (up to 5.4.0 Agent only)</td>
<td>PA-RISC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(If you install the Agent on HPUX 11.11, patch PHSS_30966 is required.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Supported in trusted mode in the default configuration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11i v2.0 (11.23) (up to 5.4.0 Agent only)</td>
<td>Itanium</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11i v2.0 (11.23) (up to 5.4.0 Agent only)</td>
<td>PA-RISC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11i v3.0 (11.31)</td>
<td>Itanium</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11i v3.0 (11.31)</td>
<td>PA-RISC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 3 (ES/AS) including Desktop with Workstation edition (up to 5.4.0 Agent only)</td>
<td>x86</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 4 (ES/AS) including Desktop with Workstation edition</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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 Server, Desktop with Workstation, and Advanced Platform</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Solaris 9 (up to 5.4.0 Agent only)</td>
<td>Sparc and Sparc-V9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Solaris 10 (Certified and verified on Solaris 10 zfs and custom information data class collections on both zfs and vxfs.)</td>
<td>Sparc, Sparc-V9, x86, and x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SUSE Linux Enterprise Server (SLES) 9 (up to 5.4.0 Agent only)</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td>Supported Operating System</td>
<td>Supported Hardware Platform</td>
<td>Platforms To Be Upgraded</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td>SUSE Linux Enterprise Server (SLES) 10–10.4, 11.0–11.1</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td>Mac OS X</td>
<td>Mac OS X 10.5 (up to 5.4.1 Agent only)</td>
<td>Intel and PowerPC</td>
<td></td>
</tr>
<tr>
<td>(Servers and Workstations)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mac OS X 10.6</td>
<td>Intel-based Apple platforms only</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mac OS X 10.7</td>
<td>Intel-based Apple platforms only</td>
<td></td>
</tr>
<tr>
<td>Oracle 9i</td>
<td>Solaris 9</td>
<td>Sparc and Sparc-V9</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Solaris 10</td>
<td>Sparc and Sparc-V9</td>
<td></td>
</tr>
<tr>
<td>Oracle 10g</td>
<td>Solaris 9</td>
<td>Sparc-V9</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Solaris 10</td>
<td>Sparc-V9, x86, and x64</td>
<td></td>
</tr>
<tr>
<td>Active Directory</td>
<td>Microsoft Windows 2000</td>
<td>x86</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows 2003</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows 2003 R2</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows 2008</td>
<td>x86 and x64</td>
<td></td>
</tr>
<tr>
<td>VCM Remote</td>
<td>Supports the same platforms as the Windows Agent.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

**Supported OS Provisioning Target Systems**

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

**Table 15–2. Supported Operating Systems**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>(Server only) 5.0, 5.2, 5.4, 5.5, 5.6, 6.0 32-bit and 64-bit</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>10.3, 32-bit and 64-bit</td>
</tr>
<tr>
<td></td>
<td>11.1, 32-bit and 64-bit</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>64-bit - Std, Ent, Web, DC, StdCore, EntCore, WebCore, DCCore</td>
</tr>
<tr>
<td></td>
<td>SP1 - i386 and 64-bit - Std, Ent, DC, StdCore, EntCore, DCCore</td>
</tr>
<tr>
<td>Windows 7 Pro</td>
<td>i386 and 64-bit</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>R2 SP2 - i386 and 64-bit - Std, Ent</td>
</tr>
</tbody>
</table>

For more information about configuring the OS Provisioning Server for installation, see "Hardware and Software Requirements for the Operating System Provisioning Server" on page 171. Instructions for installing the OS Provisioning Server and using the OS provisioning options in VCM are available in the VCM Administration Guide.

**Software Provisioning Requirements**

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

**Table 15–3. Software Provisioning Operating System and Hardware Requirements**

<table>
<thead>
<tr>
<th>Supported Operating System</th>
<th>Supported Hardware Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 7</td>
<td>x86, x64</td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 R2</td>
<td>x64</td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 SP2</td>
<td>x86, x64</td>
</tr>
<tr>
<td>Windows Vista SP2</td>
<td>x86, x64</td>
</tr>
<tr>
<td>Microsoft Windows XP SP3</td>
<td>x86</td>
</tr>
<tr>
<td>Microsoft Windows XP SP2</td>
<td>x64</td>
</tr>
<tr>
<td>Microsoft Windows Server 2003 R2 SP2</td>
<td>x86, x64</td>
</tr>
<tr>
<td>Microsoft Windows Server 2003 SP2</td>
<td>x86, x64</td>
</tr>
</tbody>
</table>

Your system must meet the requirements for VCM Software Provisioning components and software.
Table 15–4. Software Provisioning Component Requirements

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

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

UNIX and Linux Patch Assessment and Deployment Requirements

VCM 5.6 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 15–5. UNIX/Linux Patch Assessment and Deployment Operating System and Hardware Requirements

<table>
<thead>
<tr>
<th>Supported Operating System</th>
<th>Supported Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX 5.3 (up to 5.4.0 Agent only)</td>
<td>RISC and PowerPC</td>
</tr>
<tr>
<td>AIX 6.1</td>
<td>RISC and PowerPC</td>
</tr>
<tr>
<td>AIX 7.1</td>
<td>RISC and PowerPC</td>
</tr>
<tr>
<td>HP-UX 11i v1.0 (11.11) (up to 5.4.0 Agent only)</td>
<td>PA-RISC</td>
</tr>
<tr>
<td>HP-UX 11i v2.0 (11.23) (up to 5.4.0 Agent only)</td>
<td>Itanium</td>
</tr>
<tr>
<td>HP-UX 11i v2.0 (11.23) (up to 5.4.0 Agent only)</td>
<td>PA-RISC</td>
</tr>
<tr>
<td>HP-UX 11i v3.0 (11.31)</td>
<td>Itanium</td>
</tr>
<tr>
<td>HP-UX 11i v3.0 (11.31)</td>
<td>PA-RISC</td>
</tr>
<tr>
<td>Mac OS X 10.5 (up to 5.4.1 Agent only)</td>
<td>Intel and PowerPC</td>
</tr>
<tr>
<td>Mac OS X 10.6</td>
<td>Intel-based Apple platforms only</td>
</tr>
<tr>
<td>Mac OS X 10.7</td>
<td>Intel-based Apple platforms only</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 3 (ES/AS) including Desktop with Workstation edition (up to 5.4 Agent only)</td>
<td>x86 (includes Intel and AMD architectures, excludes Itanium)</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 4 (ES/AS) including Desktop with Workstation edition</td>
<td>x86 and x64 (includes Intel and AMD architectures, excludes Itanium)</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 6.0, 6.1, 6.2 Server, Desktop with Workstation, and Advanced Platform</td>
<td>x86 and x64 (includes Intel and AMD architectures, excludes Itanium)</td>
</tr>
<tr>
<td>Supported Operating System</td>
<td>Supported Hardware</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Itanium)</td>
<td></td>
</tr>
<tr>
<td>Solaris 9 (up to 5.4.0 Agent only)</td>
<td>Sparc and Sparc-V9</td>
</tr>
<tr>
<td>Solaris 10</td>
<td>Sparc, Sparc-V9, x86, and x64</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES) 9 (up to 5.4.0 Agent only)</td>
<td>x86 and x64 (includes Intel and AMD architectures, excludes Itanium)</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES) 10.0–10.4, 11.0–11.1</td>
<td>x86 and x64 (includes Intel and AMD architectures, excludes Itanium)</td>
</tr>
</tbody>
</table>

VCM 5.6 provides UNIX patch assessment content in a new format for the following operating systems.

- Red Hat RHEL 4, 5, and 6
- SUSE SLES 10.0–10.4 and 11.0–11.1

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

You can collect from the following platforms.

Table 15–6. Supported VMware Infrastructure Platforms

<table>
<thead>
<tr>
<th>Product</th>
<th>Supported Versions</th>
<th>Collection Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server/vSphere</td>
<td>4.x and 5.0 Update 1 for VCM 5.5. 5.0 Update 1a and 5.1 added with VCM 5.5.1.</td>
<td>Managing Agent</td>
</tr>
<tr>
<td>ESXi</td>
<td>Versions supported on the supported vCenter Server versions.</td>
<td>Managing Agent</td>
</tr>
<tr>
<td>ESX</td>
<td>Versions supported on the supported vCenter Server versions.</td>
<td>Managing Agent</td>
</tr>
<tr>
<td>ESX Linux Data Types from the ESX Service Console OS, including ESX Logs</td>
<td>3.5 – 4.x</td>
<td>Agent Proxy</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>1.0.1 (5.5 only), 1.5, and 1.5.1 for VCM 5.5. 5.1 added with VCM 5.5.1.</td>
<td>Managing Agent</td>
</tr>
<tr>
<td>vShield Manager</td>
<td>5.0 for VCM 5.5. 5.1 added with VCM 5.5.1.</td>
<td>Managing Agent</td>
</tr>
</tbody>
</table>

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 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

**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 15–7. FIPS Support for Windows Machines

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>Hardware Platform</th>
<th>FIPS Module Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET</td>
<td>3</td>
<td>.NET</td>
<td>894</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>1</td>
<td>x86</td>
<td>899</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>1</td>
<td>x86 and 64-bit</td>
<td>894</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>1</td>
<td>x86 and 64-bit</td>
<td>893</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>1</td>
<td>x86 and 64-bit</td>
<td>892</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>SP2</td>
<td>x86 and 64-bit</td>
<td>875</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>SP1</td>
<td>x86 and 64-bit</td>
<td>382</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>SP1</td>
<td>x86 and 64-bit</td>
<td>381</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>Gold</td>
<td>x86 and 64-bit</td>
<td>382</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>Gold</td>
<td>x86 and 64-bit</td>
<td>381</td>
</tr>
<tr>
<td>Windows XP</td>
<td>SP2</td>
<td>x86</td>
<td>240</td>
</tr>
<tr>
<td>Windows XP</td>
<td>SP1</td>
<td>x86</td>
<td>238</td>
</tr>
<tr>
<td>Windows XP</td>
<td>Gold</td>
<td>x86</td>
<td>240</td>
</tr>
<tr>
<td>Windows XP</td>
<td>Gold</td>
<td>x86</td>
<td>238</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>All</td>
<td>x86</td>
<td>103</td>
</tr>
<tr>
<td>Windows 2008</td>
<td>1</td>
<td>x86 and 64-bit; Itanium is not supported.</td>
<td>See &quot;Cryptographic RSA Enhanced Validated Modules&quot; on page 165 and &quot;Cryptographic DSS Enhanced Validated Modules&quot; on page 166.</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>RTM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows All</td>
<td>2000</td>
<td>x86</td>
<td>76</td>
</tr>
</tbody>
</table>

### 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 15–8. RSA Enhanced Validated Modules

<table>
<thead>
<tr>
<th>RSAENH Validated Operating Systems</th>
<th>Validated Versions (Links to Security Policy)</th>
<th>FIPS Certificate #</th>
<th>FIPS Version Validated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000</td>
<td>5.0.2150.1</td>
<td>#76</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows 2000 SP1</td>
<td>5.0.2150.1391</td>
<td>#103</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows 2000 SP2</td>
<td>5.0.2195.2228</td>
<td>#103</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows 2000 SP3</td>
<td>5.0.2195.3665</td>
<td>#103</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows XP</td>
<td>5.1.2518.0</td>
<td>#238</td>
<td>140-1</td>
</tr>
<tr>
<td>RSAENH Validated Operating Systems</td>
<td>Validated Versions (Links to Security Policy)</td>
<td>FIPS Certificate #</td>
<td>FIPS Version Validated</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Windows XP SP1</td>
<td>5.1.2600.1029</td>
<td>#238</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows XP SP2</td>
<td>5.1.2600.2161</td>
<td>#238</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows XP Professional SP3</td>
<td>5.1.2600.5507</td>
<td>#989</td>
<td>140-2</td>
</tr>
<tr>
<td>Vista Ultimate Edition</td>
<td>6.0.6000.16386</td>
<td>#893</td>
<td>140-2</td>
</tr>
<tr>
<td>Vista Ultimate Edition SP1</td>
<td>6.0.6001.22202</td>
<td>#1002</td>
<td>140-2</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>6.0.6001.22202</td>
<td>#1010</td>
<td>140-2</td>
</tr>
</tbody>
</table>

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 15–9. DSS Enhanced Validated Modules
<table>
<thead>
<tr>
<th>DSSENH Validated Operating Systems</th>
<th>Validated Versions (Links to Security Policy)</th>
<th>FIPS Certificate #</th>
<th>FIPS Version Validated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000</td>
<td>5.0.2150.1</td>
<td>#76</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows 2000 SP1</td>
<td>5.0.2150.1391</td>
<td>#103</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows 2000 SP2</td>
<td>5.0.2195.2228</td>
<td>#103</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows 2000 SP3</td>
<td>5.0.2195.3665</td>
<td>#103</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows XP</td>
<td>5.1.2518.0</td>
<td>#240</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows XP SP2</td>
<td>5.1.2600.2133</td>
<td>#240</td>
<td>140-1</td>
</tr>
<tr>
<td>Windows XP Professional SP3</td>
<td>5.1.2600.5507</td>
<td>#990</td>
<td>140-2</td>
</tr>
<tr>
<td>Vista Ultimate Edition</td>
<td>6.0.6000.16386</td>
<td>#894</td>
<td>140-2</td>
</tr>
<tr>
<td>Vista Ultimate Edition SP1</td>
<td>6.0.6001.18000</td>
<td>#1003</td>
<td>140-2</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>6.0.6001.18000</td>
<td>#1009</td>
<td>140-2</td>
</tr>
</tbody>
</table>

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

The 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 15–10. Windows Agents and Component File Sizes

<table>
<thead>
<tr>
<th>Agent Type</th>
<th>Installed File Size</th>
<th>Data File Size</th>
<th>Projected Data File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCM Agent used as Managing Agent</td>
<td>130–135MB</td>
<td>200MB–1GB</td>
<td>The projected data file sizing information can vary depending on the size of your vCenter Server instances and the number of hosts and guests.</td>
</tr>
<tr>
<td>This default Agent includes Extension for Provisioning and Managing Agent.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Proxy for Virtualization</td>
<td>VCM Agent +40MB</td>
<td>See VCM Agent data file sizes</td>
<td>The projected data file size is determined the same as the default Agent.</td>
</tr>
<tr>
<td>VCM Agent used for Provisioning</td>
<td>130–135MB</td>
<td>10–20MB</td>
<td>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.</td>
</tr>
<tr>
<td>This default Agent includes Extension for Provisioning and Managing Agent.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VCM Agent without Extension for Provisioning</td>
<td>70–76MB</td>
<td>10–20MB</td>
<td>The projected data file size is determined the same as the default Agent.</td>
</tr>
<tr>
<td>Active Directory Agent</td>
<td>VCM Agent +30MB</td>
<td>See VCM Agent data file sizes</td>
<td>The projected data file size is determined the same as the default Agent.</td>
</tr>
<tr>
<td>Agent Type</td>
<td>Installed File Size</td>
<td>Data File Size</td>
<td>Projected Data File Size</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------</td>
<td>----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>VCM Remote Client</td>
<td>VCM Agent +2MB (installs or upgrades Agent)</td>
<td>See VCM Agent data file sizes</td>
<td>The projected data file size is determined the same as the default Agent.</td>
</tr>
<tr>
<td>Patching Agent</td>
<td>VCM Agent +2MB</td>
<td>See VCM Agent data file sizes</td>
<td>The projected data file size is determined the same as the default Agent.</td>
</tr>
<tr>
<td>Package Manager (installed with VCM Agent Extension for Provisioning), which includes the database and cratecache.</td>
<td>Package Manager 4MB Database 140KB Cratecache 0MB</td>
<td>n/a</td>
<td><strong>Package Manager.</strong> The application that installs and removes packages. Size remains fixed. <strong>Database.</strong> Metadata about packages. Increased size based on number of installed packages. For example, installing one package increased the size from 140KB to 141KB. <strong>Cratecache.</strong> 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.</td>
</tr>
<tr>
<td>Package Studio</td>
<td>5MB</td>
<td>n/a</td>
<td>Increased size of the files depends on which *.prj and *.crate files are saved locally.</td>
</tr>
<tr>
<td>Software Repository</td>
<td>5KB</td>
<td>n/a</td>
<td>Increased size of the files is based on the number of packages published to the repository from Package Studio.</td>
</tr>
</tbody>
</table>

### UNIX and Linux Machines

The projected data file sizing information for UNIX and Linux machines information can vary depending on your collection filter set and is determined by collected data types and actions. The size can vary from 10–20 MB 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 15–11. UNIX/Linux Agents File Sizes

<table>
<thead>
<tr>
<th>Agent Type</th>
<th>Installed File Size</th>
<th>Data File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMAgent.5.4.0.AIX.5</td>
<td>60–80MB</td>
<td>5–20MB</td>
</tr>
<tr>
<td>CMAgent.5.4.0.HP-UX.11.ia64</td>
<td>80MB</td>
<td>5–16MB</td>
</tr>
<tr>
<td>CMAgent.5.4.0.HP-UX.11.pa</td>
<td>80MB</td>
<td>5–16MB</td>
</tr>
<tr>
<td>CMAgent.5.4.0.Linux</td>
<td>30–50MB</td>
<td>5–70MB</td>
</tr>
<tr>
<td>CMAgent.5.4.1.Linux</td>
<td>52–72MB</td>
<td>5–70MB</td>
</tr>
<tr>
<td>CMAgent.5.4.0.SunOS</td>
<td>40–50MB</td>
<td>5–30MB</td>
</tr>
<tr>
<td>CMAgent.5.4.0.SunOS.x86.5.10</td>
<td>40–50MB</td>
<td>5–30MB</td>
</tr>
</tbody>
</table>

#### 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 15–12. Mac OS X Agent File Sizes

<table>
<thead>
<tr>
<th>Agent Type</th>
<th>Installed File Size</th>
<th>Data File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMAgent.5.4.1.Darwin</td>
<td>97MB</td>
<td>5–30MB</td>
</tr>
</tbody>
</table>
VCM operating system provisioning supports one instance of VCM with one or more instances of Operating System Provisioning Server (OS Provisioning Server).

Configure the server to meet the requirements.

**Supported OS Provisioning Server Platform**

The OS Provisioning Server can be installed on Red Hat Enterprise Linux version 5.2, 5.4, or 5.5, 32-bit or 64-bit.

**OS Provisioning Server System Requirements**

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

- **Memory:** For physical machines, 4GB RAM is the minimum requirement. 8GB RAM is recommended. For virtual machines, assign 1GB to 4GB to the virtual machine.
- **CPU:** For physical and virtual machines, two or more processors are recommended. The multitasking required to do OS provisioning is better served by a multiprocessor server.
- **Disk Space:** For physical and virtual machines, 100GB minimum disk space to store the OS provisioning application and the repository database. Each imported ISO distribution requires additional space. Use the following sizing information to determine the additional disk space required for each distribution.

<table>
<thead>
<tr>
<th>Base Family</th>
<th>Disk Space (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>3</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL) 5.x</td>
<td>4</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL) 6.0 i386</td>
<td>14</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL) 6.0 x86_64</td>
<td>20</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>3</td>
</tr>
</tbody>
</table>

- **Networking:** For optimal functionality, configure two network interfaces. One interface on the public network, and the second interface on the private provisioning network. Also, as a requirement of the system license policy, the host name of the OS Provisioning Server must resolve to an IP address when pinged. The address can be assigned using DNS or specified in the /etc/hosts file as appropriate for your local network requirements.
OS Provisioning Server Software Requirements

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

**Required Packages**

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

- cURL
- libstdc++.so.5, which is typically installed as part of compat-libstdc++-33
- libstdc++-lib6.2-2, which is typically installed as part of compat-libstdc++-296
- libtool
- kernel: If your Red Hat machine has 2 CPUs and 4 GB memory, install kernel-devel-2.6.18-92.el5. If your machine has 2 CPUs and 8 GB memory, install kernel-PAE-devel-2.6.18-92.el5.
- SQLite, from the group Applications/Databases
- mailcap, from the System Environment/Base
- selinux-policy-devel: Required when installing on RHEL 5.4 and 5.5. SELinux is supported only for RHEL 5.5.

**Disallowed Packages**

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

- fuse
- tftp-server
- system-config-netboot
- stunnel

**OS Provisioning Server Network Requirements**

Configure your network settings to ensure that OS Provisioning Server installs and functions properly.

**Provisioning Network Interface**

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

If you use a separate provisioning network, the provisioning network interface must be associated with the hardware interface named eth1.
Configure the provisioning network interface on the machine you are using as the OS Provisioning Server with a static IP address so that the OS Provisioning Server can act as a DHCP server. The following are the default and preferred values used throughout OS Provisioning Server installation process.

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

## OS Provisioning Network Port Usage

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

### Table 16–1. OS Provisioning Ports

<table>
<thead>
<tr>
<th>Application or Service</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootpd/DHCP</td>
<td>UDP 68</td>
<td>Provides address and server location of PXE configuration files.</td>
</tr>
<tr>
<td>TFTP</td>
<td>UDP 69</td>
<td>Downloads initial PXE/kernel.</td>
</tr>
<tr>
<td>http</td>
<td>TCP 80</td>
<td>Downloads kickstart and package files.</td>
</tr>
<tr>
<td>OS Provisioning Server</td>
<td>21307</td>
<td>Communication with the nodes, including messages and registration requests.</td>
</tr>
<tr>
<td>OS Provisioning Server</td>
<td>40610</td>
<td>Allows nodes to communicate with OS Provisioning Server, including messages and registration requests.</td>
</tr>
<tr>
<td>OS Provisioning Server Repository Server</td>
<td>21307</td>
<td>OS Provisioning Server web service listening for provisioning requests from VCM.</td>
</tr>
<tr>
<td>OS Provisioning Server Hardware Discovery</td>
<td>21309</td>
<td>Used by the hardware discovery program to communicate with the inventory daemon to add new machines into the OS Provisioning Server database.</td>
</tr>
<tr>
<td>VCM Linux Agent</td>
<td>26542</td>
<td>Used for communication between VCM and the VCM Linux Agent.</td>
</tr>
</tbody>
</table>

### Provisioning Network Firewall Configuration

As an alternative to setting the specific ports, as specified above, you can add `-A RH-Firewall-1-INPUT -i eth1 -j ACCEPT` to the `/etc/sysconfig/iptables` firewall configuration file to allow traffic on all ports on the provisioning network.

### Configure the OS Provisioning Server Firewall

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

- Identify the ports for which you must configure the firewall. See "OS Provisioning Server Network Requirements" on page 172.
- Ensure that you do not accidentally lose your iptables changes. In the /etc/sysconfig/iptables-config file, determine whether IPTABLES_SAVE_ON_STOP or IPTABLES_SAVE_ON_RESTART are set to yes.

Procedure

1. On the OS Provisioning Server, log in as root.
2. Change directory to /etc/sysconfig.
3. In the /etc/sysconfig directory, open the iptables file.
4. Add `-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport <port number> -j ACCEPT` to the file to allow communication on the designated port.

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

5. Run the service iptables restart command to restart the iptables service.
The Operating System (OS) Provisioning Server is a repository of imported OS distributions. It manages the installation of the distributions on target machines. The installation of the distributions is part of the OS provisioning function in VCM, which identifies machines that can be provisioned and initiates the OS provisioning on the target machines.

You install and configure the OS Provisioning Server on one or more Red Hat servers. After configuring the servers, you import the operating system ISO files. The database manages the metadata about the OS distributions and the ISO files are saved in the OS Provisioning Server repository. After you import the distributions, the server performs the installation process, which is managed in VCM. For provisioning machines instructions about Getting Started with Operating System Provisioning, see the VCM Administration Guide.

Upgrade your OS Provisioning Server from version 5.4.1 to version 5.5. Your repository database is preserved, but you must create a new Windows Boot Image. See "Upgrade the OS Provisioning Server to 5.5" on page 187.

When the OS Provisioning Server is installed and configured, consult the VCM Backup and Disaster Recovery Guide and create a backup plan for your server and files.

**Restricted Network Environment**

To maintain security during the OS provisioning process, install and run your OS Provisioning Server in a private or restricted network. When you provision target machines, you connect the machines to this private network. See VCM Security Guide.

**Install and Configure the OS Provisioning Server**

You install the OS Provisioning Server and configure the components used to manage your operating system distributions. After you configure the components, you import the distributions and use VCM to install them on target machines.

**Prerequisites**

Ensure that your target OS Provisioning Server meets all the hardware and software requirements. See the VCM Installation Guide.
Procedure

1. "Install the Operating System Provisioning Server" on page 176
   Using the supplied media or media images, install the OS Provisioning Server and run the command to create the distribution repository.

2. "Configure DHCP" on page 178
   When you configure a private, isolated network that is used specifically for provisioning, the OS Provisioning Server uses the DHCP server it installed to provide addresses and network boot information to nodes connected to the network.

3. "Configure TFTP" on page 179
   The OS Provisioning Server provides TFTP services that run on the provisioning network. You must configure the TFTP server to listen on the private OS provisioning network interface.

4. "Create a Windows Boot Image" on page 180
   Create a Windows boot image and copy it to the OS Provisioning Server. You create the image on a Windows 2008 or Windows 7 machine, and copy the files to the OS Provisioning Server.

5. "Copy the VCM Certificate to the OS Provisioning Server for Linux Provisioning" on page 181
   If you use the OS Provisioning Server to install Linux distributions, you must copy the VCM certificate file to the OS Provisioning Server to ensure the certificate is included with the Agent when OS Provisioning Server creates the configured session prior to provisioning.

Install the Operating System Provisioning Server

Using the supplied media or media images, install the OS Provisioning Server and run the command to create the distribution repository.

VCM OS provisioning supports a single instance of VCM with a multiple instances of the OS Provisioning Server.

Prerequisites

- Install VCM. See "Use Installation Manager to Install VCM" on page 117.
- Ensure the target machine meets the prerequisites. See Hardware and Software Requirements for the Operating System Provisioning Server.
- Determine whether you are installing the OS Provisioning Server as an attended or unattended installation. To run an unattended installation, use the ./autoinstall -a y command. This procedure is based on an attended installation.

Procedure

1. On the target machine, log in as root.

2. Mount the VCM-OS-Provisioning-Server-<version number>.iso by attaching or mounting the image.
   When you mount the image, do not use the no exec option.

3. Type cd /<path to mounted OS Provisioning Server.iso> to change the directory to the location of the image.

4. Run the ./INSTALL-ME command to install the server.

5. In the Nixinstaller window, click Next.

6. Click Continue.
7. Click **Close** when the installation finishes.

8. In the Nixstaller window, click **Finish**.

9. Run the service **FastScale status** command to verify that the installation finished.

   A successful installation displays the following results. PID values vary.
   
   rsyslogd (pid 3335) is running...
   fsmesgd (pid 3517) is running...
   fsrepod (pid 3683) is running...
   fsadmin (pid 12618) is running...
   dhcpd is stopped
   tftpd (pid 12057) is running
   fsjobd (pid 4237) is running...
   fshinvd (pid 4249) is stopped...

   An unsuccessful installation displays **FastScale: unrecognized service** or **several services are not running.** Review the logs to determine possible problems.

10. Run **ospctrl --configure --createrepo**.

    If the firewall is enabled, add the **--firewall** option.

    If you are installing on a RHEL 5.5 and SELinux is enabled, add the **--selinux** option. SELinux is supported only for RHEL 5.5.

    As part of the installation script, provide Linux passwords for the following accounts.

    | User Name | Account type                      |
    |-----------|-----------------------------------|
    | fsadmin   | OS Provisioning Repository administrator |
    | vcmuser   | Account used to connect to VCM    |
    | fastscal  | Apache administrator              |

11. Reboot the OS Provisioning Server to ensure that all related services are started in the correct order.

12. Run the service **FastScale status** command to verify the OS Provisioning Server services after reboot.

    A successful installation displays the services and their PIDs as running.

**What to do next**

- Configure your DHCP server for provisioning. See "**Configure DHCP**" on page 178.

- (Optional) Add the OS Provisioning Server maintenance commands to the root user’s path. The OS Provisioning Server modifies the default shell profiles by adding `/opt/FastScale/sbin` to the root account. When the user is root, the maintenance commands in `/opt/FastScale/sbin` are available in the default path, and they are available when the profile is reloaded.

**Uninstall the OS Provisioning Server**

Uninstalling the OS Provisioning Server removes the provisioning application from the machine on which it is installed. You must mount the OS Provisioning Server media and run the uninstall command.
CAUTION  The uninstall process removes the application and deletes all the data in the database.

Procedure

1. On the OS Provisioning Server, log in as root.
2. Mount the OS Provisioning Server ISO by attaching or mounting the image.
3. Type `cd /<path to OS Provisioning Server.iso>` to change the directory to the location of the image.
4. Run the `.UNINSTALL-ME` command to uninstall the application.
5. Type yes.

The uninstall process completes and generates a log. See the example log.

```
[Thu Jul 22 08:57:06 IST 2012] UNINSTALL-ME: Starting uninstallation of VCM OS Provisioning Server...
[Thu Jul 22 08:57:08 IST 2012] UNINSTALL-ME: FastScale service is running
Shutting down FSnetfs: [ OK ]
Shutting down FSsyslog: [ OK ]
Shutting down FSmesgd: [ OK ]
Shutting down FSdhcpd: [ OK ]
..........
[Thu Jul 22 09:00:44 IST 2012] UNINSTALL-ME: Uninstallation complete!
```

Configure DHCP

When you configure a private, isolated network that is used specifically for provisioning, the OS Provisioning Server uses the DHCP server it installed to provide addresses and network boot information to nodes connected to the network.

Prerequisites

Determine whether you are using a private network (recommended) or shared network (supported, but not recommended). If you are provisioning systems on a shared network, you probably have a DHCP server on the network. Disable the OS Provisioning Server's DHCP server and configure your regular DHCP server to provide network boot information for machines to be provisioned. See "Configure a DHCP Server Other Than the OS Provisioning Server" on page 179.
Procedure

1. Open `/opt/FastScale/etc/dhcpd.conf`.
2. Configure the settings for your environment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>subnet</td>
<td>The IP address subnet of the private network interface. Default value is 10.11.12.0.</td>
</tr>
<tr>
<td>netmask</td>
<td>The netmask of the subnet. Default value is 255.255.255.0.</td>
</tr>
<tr>
<td>range</td>
<td>The range of allocated IP addresses for the provisioned nodes. Default value is 10.11.12.100–10.11.12.200.</td>
</tr>
<tr>
<td>broadcast-address</td>
<td>The broadcast address on the subnet. Default value is 10.11.12.255.</td>
</tr>
<tr>
<td>next-server</td>
<td>The IP address of the private network interface. Default value is 10.11.12.1.</td>
</tr>
</tbody>
</table>

What to do next

Configure your TFTP server to work with the provisioning environment. See "Configure TFTP" on page 179.

Configure a DHCP Server Other Than the OS Provisioning Server

To configure your system to work with a DHCP server other than the one on the OS Provisioning Server, you turn off the OS Provisioning Server DHCP server and configure your corporate DHCP server to connect to the OS Provisioning Server after nodes connect and NetBoot (PXE) starts. The nodes download the boot kernel from the OS Provisioning Server through TFTP.

Procedure

1. On the OS Provisioning Server, log in as root.
2. Open `/etc/sysconfig/FSdhcpd`.
3. Change `DHCPD_CONF=/opt/FastScale/etc/dhcpd.conf` to `DHCPD_CONF=/opt/FastScale/etc/dhcpd.conf.none`

   This change prevents the DHCP from resetting after a reboot.
4. Run the `/opt/FastScale/etc/init.d/FSdhcpd stop` command.
5. On the corporate DHCP server, update `dhcpd.conf` to add these options:
   
   ```
   allow bootp;
   allow booting;
   next-server <IP address of the OS Provisioning Server>;
   ```

Configure TFTP

The OS Provisioning Server provides TFTP services that run on the provisioning network. You must configure the TFTP server to listen on the private OS provisioning network interface.
Prerequisites
Configure your DHCP server. See "Configure DHCP" on page 178.

Procedure
1. On the OS Provisioning Server, log in as root.
2. Run ospctrl --showconfig.
   The following results verify that the TFTP and Apache services are running.
   - TFTP - Configured on * - Running
   - Apache - Configured on * - Running
3. Run ospctrl --configure --privateip <IP Address>.
   The configuration process runs. The IP address is 10.11.12.1.
   - Shutting down FStftpd: [ OK ]
   - Starting FStftpd: [ OK ]
   - TFTP - Configured on 10.11.12.1 - Running
   - Shutting down FSadmin: [ OK ]
   - Starting FSadmin: [ OK ]
   - Apache - Configured on 10.11.12.1 - Running
4. Run ospctrl --showconfig.
   The following text appears when the TFTP and Apache services are running.
   - TFTP - Configured on 10.11.12.1 - Running
   - Apache - Configured on 10.11.12.1 - Running

What to do next
To install Windows distributions on target machines, you must create a Windows boot image and copy it to the OS Provisioning Server. See "Create a Windows Boot Image" on page 180.

Create a Windows Boot Image
Create a Windows boot image and copy it to the OS Provisioning Server. You create the image on a Windows 2008 or Windows 7 machine, and copy the files to the OS Provisioning Server.

Prerequisites
- Verify that the Windows Automated Install Kit (WAIK) 3.0 is installed on the Windows machine on which you are creating the boot image.
- Verify that the Windows machine on which you are creating the image, which is usually the VCM Collector, can access the OS Provisioning Server on the network.
- On Windows 2008 machines, you run the command line options in this procedure as Administrator.
Procedure

1. On the OS Provisioning Server, copy /opt/FastScale/deployment to a directory on the Windows machines on which you are creating the boot image.
   
   For example, c:\Program Files\osp.
2. Right-click the Command Prompt icon and select Run as administrator.
3. From the Windows command line, change the directory to the location where you copied the deployment files.
   
   For example, c:\Program Files\osp\deployment.
4. From the Windows command line, run bin\osp --osphome="c:<Path to OSP files> --deploymenturl=<OS Provisioning Server Private IP Address> --waik=<Path to WAIK>".

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>osphome</td>
<td>The path to the files copied from the OS Provisioning Server. For example, c:\Program Files\osp\deployment. If you run the command from the directory, you can use --osphome=.</td>
</tr>
<tr>
<td>deploymenturl</td>
<td>The OS Provisioning Server's Private Interface IP Address. The default configuration is 10.11.12.1.</td>
</tr>
<tr>
<td>waik</td>
<td>Path to the Windows AIK files. For example, &quot;c:\Program Files (x86) \Windows AIK&quot;.</td>
</tr>
</tbody>
</table>

5. When the preinstallation environment and boot configuration are created, copy the directories from the Windows AIK machine to the OS Provisioning Server.

<table>
<thead>
<tr>
<th>From Windows AIK Machine</th>
<th>To OS Provisioning Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>[path]\deployment\output\Boot</td>
<td>/FSboot/</td>
</tr>
<tr>
<td>[path]\deployment\output\windows\amd64\winpe.wim</td>
<td>/FSboot/windows/amd64/</td>
</tr>
<tr>
<td>[path]\deployment\output\windows\x86\winpe.wim</td>
<td>/FSboot/windows/x86/</td>
</tr>
</tbody>
</table>

What to do next

Copy the VCM certificate to the OS Provisioning Server to ensure the successful installation of your Linux distributions. See "Copy the VCM Certificate to the OS Provisioning Server for Linux Provisioning" on page 181.

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

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

Prerequisites

Ensure that you have access to the VMware_VCM_Enterprise_Certificate_*_.pem file in the \Program Files (x86)\VMware\VCM\CollectorData folder on the VCM Collector.
Copy the VCM certificate, VMware_VCM_Enterprise_Certificate_*.pem, to the OS Provisioning Server/opt/FastScale/var/fsadmin/basic/ directory.

What to do next

Import operating system distributions into your repositories. See "Import Distributions into the OS Provisioning Server Repository" on page 182.

Import Distributions into the OS Provisioning Server Repository

To install operating system distributions on target machines, you must import the distributions into the OS Provisioning Server repository.

For supported operating systems, see "Hardware and Operating System Requirements for VCM Managed Machines" on page 157.

Prerequisites

Confirm that you installed OS Provisioning Server and configured all the options. See "Install and Configure the OS Provisioning Server" on page 175.

Procedure

1. "Create Directories for Windows Distributions" on page 182.

Some Windows operating system distribution files are issued on multiple disks. Because of the dependencies within the packages, you must create a single directory for multiple Windows operating system disks before you import Windows distributions.

2. "Import Windows Distributions" on page 183.

Windows distributions are the operating system installation files that you import into the OS Provisioning Server repository. After importing the distribution, you use VCM provisioning actions to install the operating system on target machines.

3. "Import Linux Distributions" on page 185.

Linux distributions are the operating system installation files that you import into the OS Provisioning Server repository. After importing the distribution, use VCM provisioning actions to install the operating system on target machines. You can import standard and customized operating system distributions.

Create Directories for Windows Distributions

Some Windows operating system distribution files are issued on multiple disks. Because of the dependencies within the packages, you must create a single directory for multiple Windows operating system disks before you import Windows distributions.

Procedure

1. On the OS Provisioning Server, use the mkdir -p /tmp/<directory name> command to create a directory to contain the imported files from multiple source files.

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

2. Insert the first CD in the drive and run the cp -R /media/cdrom/<source directory name> /tmp/<directory name> command.
For example, cp -R /media/cdrom/Win2003-R2-SP2-Standard /tmp/Win2003-R2-SP2-
Standard-Disk1.

3. Replace the first CD with the second CD and run the cp -R /media/cdrom/<source directory
name> /tmp/<directory name> command.

For example, cp -R /media/cdrom/Win2003-R2-SP2-Standard /tmp/Win2003-R2-SP2-
Standard-Disk2.

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

What to do next
Import Windows distributions into your repository. See "Import Windows Distributions" on page 183.

Import Windows Distributions

Windows distributions are the operating system installation files that you import into the OS Provisioning
Server repository. After importing the distribution, you use VCM provisioning actions to install the
operating system on target machines.

You can import standard and customized ISO images. When you import a standard image, you type the
required metadata. If the import process detects a custom image, you must select specific values for the
platform, distribution, and build type.

When you mount the images, do not use -t iso9660. If you use -t iso9660, some automounted
media will not import. If the import process reports a fingerprint error message, you must unmount the
directory and manually mount it using the -t udf rather than the -t iso9660 option.

Prerequisites

- Verify that the distributions you are importing do not include spaces in the filenames. Before you
  import, remove the spaces or replace them with underscores.

- Confirm that the current OS Provisioning Server IP address is correct for your production
  environment. You cannot change the OS Provisioning Server IP address at a later time. If the initial IP
  address of the OS Provisioning Server after install is not the address you intend for it to have when it is
  put into production, you must change its address, and change related DHCP and TFTP configurations,
  before you import any OS distributions. If you change the OS Provisioning Server IP address after you
  imported the distributions, you must re-import the distributions with the new address. You must also
  recreate the Windows boot image with the new IP address.

- Determine whether you are importing a single ISO image or multiple images from a directory. The
  basicimport command uses a -i option to specify an ISO file and a -d option to specify the directory.
  For information about Using the basicimport Command Options, see the VCM Administration Guide.

- If you are importing multdistribution .iso files, create directories and copy the files to the directories.
  See "Create Directories for Windows Distributions" on page 182.

Procedure

1. On the OS Provisioning Server, log in as vcmuser.

2. Mount the ISO by attaching to the media image or mounting the image.

   For Windows 2008 and Windows 7, use -t udf mount type and do not include any spaces in the path.

   For all other Windows operating systems, use loopback. For example, $ sudo mount -o loop
   /<iso_file.iso> /<mount point>.
3. Run the `sudo basicimport -d /mnt/<directory name> -l <OS Provisioning Server private IP address or provisioning network IP address>` command.
   
   For example, `sudo basicimport -d /mnt/Win2k3SE-R2-SP2-i386 -l 10.11.12.1`.
   
   If you created a `/tmp/` directory for a multi-CD distribution, include the path. For example, `/tmp/<directory name>`, or `/tmp/Win2003-R2-SP2-Standard`.
   
   For subsequent imports, you can run the command without the `-l` option.

4. Type the Family Name.
   
   For example, `Windows`. You must provide a unique family name to import different operating systems in the same family. No other family can exist with the same combination of name, version, and architecture values.

5. Type the Family Version.
   
   For example, `2008R2`.

6. Type the Family Architecture.
   
   For example, either `i386` or `x86_64`.

7. Type the Provenance.
   
   For example, `CD`, `hotfix`, or `SP`.

8. For Windows 2008 R2, Windows 7, and Windows 2003 only, type the Build Type.
   
   For example, either `volume` or `retail`.
   
   If you importing a standard ISO, the distribution is imported. If the ISO is customized, you must provide additional information about the distribution that is used when installing the operating system.

9. In the OS platform list, select 1. Microsoft Windows.

10. In the OS distributions list, select the number that most closely corresponds to the operating system you are importing.

    1. Microsoft Windows Server 2008 R2
    2. Microsoft Windows Server 2008 SP2
    3. Microsoft Windows Server 2008 SP1
    4. Microsoft Windows 7
    5. Microsoft Windows 2003, Enterprise Edition R2 SP2

   If you select the incorrect distribution, you can import the distribution, but you cannot install it.

11. Type the Build Type, either `retail` or `volume`.

    The distribution is imported.

What to do next

Import Linux distributions into the OS Provisioning Server repository. See the VCM Administration Guide.
Import Linux Distributions

Linux distributions are the operating system installation files that you import into the OS Provisioning Server repository. After importing the distribution, use VCM provisioning actions to install the operating system on target machines. You can import standard and customized operating system distributions.

You can import standard and customized ISO images. When you import a standard image, you type the required metadata during the import process. If the import process detects a custom image, you must select specific values for the platform and distribution.

Use this procedure to import Linux distributions. For SUSE distributions that are issued on multiple DVDs, you use only the first disk and import the distribution using this procedure.

Prerequisites

- Verify that the distributions you are importing do not include spaces in the filenames. Before you import, remove the spaces or replace them with underscores.

- Confirm that the current OS Provisioning Server IP address is correct for your production environment. You cannot change the OS Provisioning Server IP address at a later time. If the initial IP address of the OS Provisioning Server after install is not the address you intend for it to have when it is put into production, you must change its address, and change related DHCP and TFTP configurations, before you import any OS distributions. If you change the OS Provisioning Server IP address after you imported the distributions, you must re-import the distributions with the new address.

- Determine whether you are importing a single ISO image or multiple images from a directory. The basicimport command uses a -i option to specify an ISO file and a -d option to specify the directory. For information about Using the basicimport Command Options, see the VCM Administration Guide.

Procedure

1. On the OS Provisioning Server, log in as vcmuser.

2. Mount the ISO by attaching to the media image or mounting the image.
   
   For all Linux operating systems, use loopback. For example, `sudo mount -o loop <iso_file.iso> /<mount point>`.

3. Run the `sudo basicimport -i <distribution name>.iso -l <OS Provisioning Server private IP address or provisioning network IP address>` command.
   
   For example, `sudo basicimport -i rhel-server-6.0-x86_64-dvd.iso -l 10.11.12.1`.
   
   For subsequent imports, you can run the command without the -l option.

4. Type the Family Name.
   
   For example, `rhel`. You must provide a unique family name to import different operating systems in the same family. No other family can exist with the same combination of name, version, and architecture values.

5. Type the Family Version.
   
   For example, `6.0`.

6. Type the Family Architecture.
   
   For example, either `i386` or `x86_64`.

7. Type the Provenance.
   
   For example, `CD`, `hotfix`, or `SP`. 

VMware, Inc. 185
If you are importing a standard ISO, the distribution is imported. If the ISO is customized, you must provide additional information about the distribution that is used when installing the operating system.

8. In the OS distributions list, select the number that most closely corresponds to the operating system you are importing.

1. RedHat Enterprise Linux 6
2. RedHat Enterprise Linux 5.6
3. RedHat Enterprise Linux 5.5
4. RedHat Enterprise Linux 5.4
5. RedHat Enterprise Linux 5.2
6. RedHat Enterprise Linux 5.0
7. Suse Linux Enterprise 11.1
8. Suse Linux Enterprise 10.3

If you select the incorrect distribution, you can import the distribution, but you cannot install it. The distribution is imported.

What to do next
Use VCM to install your distributions on target machines. See the VCM Administration Guide.

Using the basicimport Command Options

You use the basicimport command-line options to import Windows or Linux distributions into the OS Provisioning Server repository.

Table 17–1. basicimport Command Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-h</code></td>
<td>Help. Displays and describes the basicimport options.</td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Directory. Path to the media source directory. This option is required when you import OS distributions issued on more than one media item, such as multiple DVDs.</td>
</tr>
<tr>
<td><code>-i</code></td>
<td>ISO file. Path and image name for the distribution. Used with importing distributions issued on one media source, such as a Red Hat distribution on a single DVD.</td>
</tr>
<tr>
<td><code>-l</code></td>
<td>Deployment IP address of the OS Provisioning Server.</td>
</tr>
<tr>
<td><code>-n</code></td>
<td>Family name. For example, Linux or Windows.</td>
</tr>
<tr>
<td><code>-v</code></td>
<td>Family version. For example, 6.0 or 2008r2sp2.</td>
</tr>
<tr>
<td><code>-a</code></td>
<td>Family Architecture. For example, i386 or x86_64.</td>
</tr>
<tr>
<td><code>-p</code></td>
<td>Provenance. Distribution source. For example, CD, hotfix, or SP.</td>
</tr>
<tr>
<td><code>-t</code></td>
<td>ISO build type. For example, retail or volume. Applies only to Windows Server 2008 R2, Windows 7, and Windows Server 2003.</td>
</tr>
</tbody>
</table>
Working with Custom Linux ISO Distributions

The OS Provisioning Server in VCM allows you to import custom Red Hat and SUSE ISO images into the repository and then to install the custom distributions on target machines.

To support standard and custom ISO images, OS Provisioning Server includes required package lists for each supported ISO. If your custom ISO is missing any of the packages specified in the list, or is missing any of the dependencies specified by the required packages, you can import the ISO into the repository, but the installation of a distribution lacking a required or dependency package might fail.

To provide you with the flexibility to use OS provisioning to install your custom distribution, you have two options.

- Add the missing required packages back into the ISO and re-import it into the repository. Run the Provision wizard again to create a new configured session with the updated distribution. The installation of the distribution on the target machines will proceed without an error and the required list remains as it was provided in the OS Provisioning Server.
- Modify the required package list by removing the package names from the list. The installation of the distribution on the target machines will proceed without an error unless there are missing dependency packages.

The required package lists, whether you are using them for reference, as in the first option, or are modifying them, as in the second option, are located on the OS Provisioning Server.

- **Red Hat:** /FSboot/repository/linux/<RHEL version>.
  
  For example, /FSboot/repository/linux/RHEL6.0server-x86_64/packages

- **SLES 10.3:** /opt/FastScale/var/fsadmin/jobs/SLES10.0_sp3.basic.php

- **SLES 11.1:** /opt/FastScale/var/fsadmin/jobs/SLES11.0_sp1.basic.php

For error messages due to missing packages, see the VCM Troubleshooting Guide.

Upgrade the OS Provisioning Server to 5.5

Upgrade your OS Provisioning Server from version 5.4.1 to version 5.5. Your repository database is preserved, but you must create a new Windows Boot Image.

Prerequisites

Ensure that there are no outstanding provisioning actions. The Provisionable Machines data grid should not include any target machines that must be installed before you upgrade. In VCM, click Administration and select Machines Manager > OS Provisioning > Provisionable Machines and review the OS Provisioning Status column. If you find target machines that are not yet fully provisioned, complete the provisioning process, license, install the VCM Agent, and collect data from the target machines. This action ensures that the machines continue as managed machines.

Procedure

1. On the OS Provisioning Server machine, log in as root.
2. Mount the VCM-OS-Provisioning-Server-<version number>.iso by attaching or mounting the image.

   When you mount the image, do not use the no exec option.

3. Type cd /<path to mounted OS Provisioning Server.iso> to change the directory to the
location of the image.

4. Run the ./UPGRADE-ME command to install server.

5. In the Nixstaller window, click **Next**.

6. Click **Continue**.

7. Click **Close** when the installation finishes.

8. In the Nixstaller window, click **Finish**.

9. Run the service **FastScale status** command to verify that the installation finished.

   A successful installation displays the following results. PID values vary.
   
   rsyslogd (pid 3335) is running...
   fsmesgd (pid 3517) is running...
   fsrepol (pid 3683) is running...
   fsadmin (pid 12618) is running...
   dhcpd is stopped
   tftpd (pid 12057) is running
   fsjobd (pid 4237) is running...
   fshinvd (pid 4249) is stopped...

   An unsuccessful installation displays **FastScale: unrecognized service or several services are not running. Review the logs to determine possible problems.**

10. Reboot the OS Provisioning Server to ensure that all related services are started in the correct order.

11. Run the service **FastScale status** command to verify the OS Provisioning Server services after reboot.

    A successful installation displays the services and their PIDs as running.

**What to do next**

Create a new Windows boot image. See "Create a Windows Boot Image" on page 180.
Managing the OS Provisioning Server System Logs

The OS Provisioning Server log files are located in the /opt/FastScale/logs and /var/log directories. You must monitor the space used and truncate the files if they begin to consume more disk space on the server than you have space to store.

**Table 17–2. Log File Locations**

<table>
<thead>
<tr>
<th>Directory</th>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/FastScale/logs</td>
<td>fsadmin.err</td>
<td>Messages from the Apache Web server.</td>
</tr>
<tr>
<td></td>
<td>fsadmin.log</td>
<td>Lists internal commands from the Apache Web server.</td>
</tr>
<tr>
<td></td>
<td>FSjobd.log</td>
<td>Messages generated during the job build process.</td>
</tr>
<tr>
<td></td>
<td>FSmesgd.log</td>
<td>Messages generated by the message daemon.</td>
</tr>
<tr>
<td></td>
<td>FSnetfs.log</td>
<td>Messages from the FSnetfs service.</td>
</tr>
<tr>
<td></td>
<td>FSrepod.log</td>
<td>Messages generated by the repository database server.</td>
</tr>
<tr>
<td></td>
<td>php.log</td>
<td>Messages from the php interpreter used by the Web server and the jobs build program.</td>
</tr>
<tr>
<td>/var/log</td>
<td>messages</td>
<td>Messages from dhcpd and tftpd services generated during hardware discovery and operating system deployment to target machines.</td>
</tr>
</tbody>
</table>
ospctrl Command Options

Use the ospctrl command-line options to configure your TFTP and Apache services with the OS provisioning private IP address and to back up and restore the OS Provisioning Server repository and distribution files.

Table 17–3. ospctrl Command Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help</td>
<td>Displays and describes the ospctrl options.</td>
</tr>
<tr>
<td>--configure --privateip &lt;IPAddress&gt;</td>
<td>Configures the TFTP server and the Apache server with the private provisioning network IP address.</td>
</tr>
<tr>
<td>--configure --selinux</td>
<td>If SELinux is enabled, compiles the policies of OS Provisioning Server and then inserts the policies into the running kernel. The action also relabels OS Provisioning Server objects.</td>
</tr>
<tr>
<td>--configure --firewall</td>
<td>Makes the OS Provisioning Server services trusted by enabling the appropriate ports to communicate with outside networks for the purpose of operating system provisioning.</td>
</tr>
<tr>
<td>--configure --creatrepo</td>
<td>Creates data for OS Provisioning Server and prompts you to change default passwords of OS Provisioning Server.</td>
</tr>
<tr>
<td>--configure --creatrepo --nopasswd</td>
<td>Creates data for OS Provisioning Server and with the default passwords rather than prompting you to change the passwords.</td>
</tr>
<tr>
<td>--deconfigure</td>
<td>Resets the TFTP server and the Apache server to the default values.</td>
</tr>
<tr>
<td>--showconfig</td>
<td>Displays the current state of the TFTP and Apache servers, including the configured private IP address.</td>
</tr>
<tr>
<td>--backup --dirpath=&lt;path to backup directory&gt;</td>
<td>Backs up the repository and the OS distributions to the specified --dirpath location.</td>
</tr>
<tr>
<td>--restore --dirpath=&lt;path to backup directory&gt;</td>
<td>Restores the repository and the OS distributions from the specified --dirpath backup location.</td>
</tr>
</tbody>
</table>
Index

3
32-bit environment migrations 130
6
64-bit environments supported 117
A
account
database server 57, 82, 109
Kerberos, database server 57, 82, 109
accounts
clustered servers 49, 70, 96
administrator rights 24
agent 24, 27
communication settings 150
disk sizing 167
EXE installer 35
folder 27
hardware 157
software provisioning 160
MSI installer 35
non-English Windows platforms 13
OS platform support 13
patch assessment 161
platforms supported 141
software
software provisioning 160
UNIX/Linux upgrade 142-143
upgrade for UNIX/Linux 141
upgrading 140
agent certificates 34
agent installed status 27
agent machines for new content architecture 162
Agent Proxy
FIPS 166
hardware requirements 164
OS requirements 164
virtualization 163
agent proxy machine upgrade 144-145
agent proxy machine upgrade manually 146
agent service account for SQL Server 49, 70, 96
application services account 26
architecture, new patch assessment content 162
ASP Role Service 43, 72, 113
ASP.NET Client System Web version 43, 72, 113
ASP.NET Role Service 43, 72, 113
attributes for certificates 33
authenticate server to client 33
authentication with HTTP/HTTPS 57, 82, 108
autogrowth for database 151
avoid loss of data
back up certificates 129
back up databases 129
back up files 129
B
back up
certificates 129
databases 129
files and reports 129
back up key to encrypted file 54, 77, 103
backup and disaster recovery plan 155
basic authentication with HTTP/HTTPS 57, 82, 108
basicimport
provisioning, operating system 186
best practices guides 17
boot image, Windows
provisioning, operating system 180
browser compatibility 25
C
certificates 33
back up 129
collector 34
tool 34
Installation Manager generated 33
certificates for agents 34
certificates, copy
provisioning, operating system 181
channel throughput with SQLIO 125
Cloud Infrastructure 163
clustered servers account types 49, 70, 96
collect virtual environment data 163
collection scripts use PowerShell 159
collector
certificates 34
collector services account 26
communication certificates 33
communication settings for agents 149
compatibility of browser 25
component-specific settings 149
Component Services DCOM Config console 26
component settings 149
computer name matches SQL Server 48
computer names, SQL Server 68, 94
configurations
database file growth 151
configure
agent communication settings 149
collector components 40, 59, 62, 84, 88, 112
CPU for VCM on virtual machine 30
database file growth 151
database recovery settings 152
disk for VCM on virtual machine 30
IIS 52
Kerberos on database server 57, 82, 108
memory for VCM on virtual machine 31
provisioning, operating system 175-176
SQL Server 121
SQL Server processor settings 122
SSRS 55, 79, 105
SSRS, two-tier 77, 104
Web components 40, 50, 62, 72, 88, 97
Web Service URL 56, 80, 106
content architecture for patch assessment 162
CPU requirements
VCM on virtual machine 30
Cryptographic DSS Enhanced Modules 166
Cryptographic RSA Enhanced Modules 165
Cryptographic Service Providers 164
customize VCM 149
D
dashboard errors in SSRS 54, 77, 103
data collections in virtual environments 144
data file sizing
Mac OS X machines 169
UNIX and Linux machines 168
Windows machines 167
database
back up 129
backup and disaster recovery plan 155
file growth 151
history cleanup 154
index rebuild setting 154
integrity check 153
recovery models 151
recovery settings 152
settings for SQL Server 121
SQL Server 55, 79, 106
update statistics 154
database server
AD account for Kerberos 57, 82, 109
configure Kerberos 57, 82, 108
DCOM
enable 42
default network authority account 25
default port 1433 44, 65, 91
DHCP
provisioning, operating system 178-179
disaster recovery plan 155
disk configuration requirements 17
disk interface and drive performance 124
disk IO for SQL Server 122
disk space sizing for agent machines 167
disk space requirements
collector 15
VCM on virtual machine 30
DSS Enhanced Validated Modules 166
E
encryption keys 56, 80, 106
Enhanced Key Usage extensions 34
enhanced security mode for IE 44, 65, 91
enterprise certificates 34
environment size 15, 19
environment variable 27
establish
administration rights 24
SQL Server administrator rights 50, 71, 97
TLS connection 34
ESX Service Console OS 163
evaluation version of SQL Server 19, 45, 66, 92
F
Federal Information Processing Standards 164
file growth for database 151
file size for agents
Mac OS X 169
UNIX/Linux 168
Windows 167
FIPS 164
Agent Proxy 166
Windows hardware 164
Firefox 25
firewall
OS Provisioning server 173
Foundation Checker 23
G
guides for best practices 17
H
hardware
agent 157
collector 15
managed machines 157
software provisioning 160
virtualization 164
history cleanup for database 154
hyperthreading 122
I
IE enhanced security mode 44, 65, 91
IIS
64-bit 87
configuring 52, 74, 99
ISAPI Extensions 54, 76, 101
impact of environment sizing 19
import distributions
provisioning, operating system 182
Windows directories 182
import Windows
provisioning, operating system 183
importing
provisioning, operating system 183
basicimport 186
index rebuild setting for database 154
install
provisioning, operating system 175-176
SSRS 77, 104
install VCM on virtual machine 29
installation
check prerequisites 15, 19
configurations 19, 22
maintenance 149
preparing 21
prerequisites 15, 19
requirements 13
VCM 117
N
NET Framework 43, 71, 112
installed versions 43, 71, 112
status 43, 72, 113
network authority account 25
new content architecture 162
non-clustered servers account types 49, 70, 96
non-English Windows platforms 13
O
OpenSSL FIPS 166
operating system locale settings 42
operating system requirements 157
FIPS 164
OS Provisioning 160
Software Provisioning 160
OS Provisioning server 38
osctrl commands
provisioning, operating system 190
overview of installation configurations 19
P
patch assessment
agent machines 161
new content architecture 162
performance of SQL Server 121
permissions
SQL Server agent service account 49, 70, 96
VCM Remote virtual directory 120
personal certificate store 33
personal system store 34
physical requirements for Agent Proxy 164
planning VCM maintenance 153
platforms
for Cloud Infrastructure 163
UNIX/Linux agent support 141
PLS files for UNIX/Linux patch assessment 161
plug-in files for vSphere Client VCM Plug-in 147
ports
1433 44, 65, 91
split installation requirements 117
PowerShell for collection scripts 159
prepare for installation 21, 118
prerequisites
check for installation 15, 19
installation 19, 23
single-tier installation 39
three-tier installation 88
to migrate VCM 130
two-tier installation 62
prerequisites for migration 128
procedure
single-tier installation 40
three-tier installation 88
two-tier installation 62
processor settings for SQL Server 122
properties
SQL Server 47, 67, 93
provisioning, operating system
certificates, copy 181
configure 175
configure 176
custom Linux distributions 187
index
DHCP 178-179

distributions importing 182

firewall 173

import

Windows 183

import Linux/ESX 185

import, create Windows directories 182

importing

basicimport 186

install 175-176

logs 189

network 172

osctrl commands 190

requirements 171

server platform 171

server requirements 171

software 172

supported platforms 160

system requirements 171

TFTP 180

uninstall 177

upgrade 187

Windows boot image 180

public key infrastructure 33

R

RAID levels for SQL Server 122

recover collector 138

recovery models for database 151

recovery plan 155

recovery settings

configure 152

register

vSphere Client VCM Plug-in 147

remote desktop session host 42, 64, 90

disable in three-tier install 90

disable in two-tier install 64

Remote Desktop Session Host 42

remote package

UNIX/Linux agent upgrade 143

repair

uninstall, troubleshooting 118

replace 32-bit environment 131

Report Manager URL confirmation 56, 80, 107

reports generation 40, 54, 77, 103-104

requirements

Agent Proxy 163-164

collector software and OS 19

disk configuration 17

installation 13

managed machines 157

Managing Agent 163

operating system 157

OS Provisioning server 171

software sizing impacts 19

split installation ports 117

UNIX/Linux agent machines 161

UNIX/Linux patch deployment 162

VCM CPU on virtual machine 30

VCM disk space on virtual machine 30

VCM memory on virtual machine 31

VCM on virtual machine 29

resource for VCM on virtual machine 29

RSA Enhanced Validated Modules 165

RSA machine key 119

S

scripts for collection use PowerShell 159

secure certificates 33

Security Guide for VCM certificates 33

system prerequisites 23

security mode for IE 44, 65, 91

security policy 119

server

provisioning, operating system 171

server authentication 33

Service Console OS for ESX 163

services account

for collector 26

Servics Management console 26

settings

database recovery 152

settings to customize components 149

single-tier installation 22, 37

components 37

configuration 39

prerequisites 39

procedure 40

size of environment 15

sizing worksheets 15, 17

software

collector 19

managed machines 157

software provisioning 160

software provisioning 160

split install 37, 61, 87

split installation 22

migration 136

SQL Server

administrator rights 50, 71, 97

agent service account 49, 70, 96

computer name 48

computer names 68, 94

configure 121

database 55, 79, 106

database settings 121

disk IO configuration 122

evaluation version 19, 45, 66, 92

installing 64-bit 45, 65, 91

maintenance plan 153

performance 121

processor settings 122

properties 47, 67, 93

RAID levels 122

SQL Server Reporting Service (SSRS)

backup keys 77, 103

SQL XML 87

SQLIO for IO channel throughput 125

SQLXML version 28, 60, 85, 112

SSRS

back up keys 54, 77, 103

configure 55, 79, 105
dashboard errors 54, 77, 103
generate reports 40, 54, 77, 103-104
user permissions errors 54, 77, 103
Web service errors 54, 77, 103
status of agent installed 27
supported agent machines 157
supported platforms
	provisioning, operating system 160
sysadmin 25, 49, 70, 96
system checks 23
system prerequisites 23
T
TFTP
	provisioning, operating system 180
three-tier split installation 22, 87
	prerequisites 88
	n procedure 88
throughput with SQLIO 125
TLS 119
	server authentication 33
trust

certificate 34
	chain 34
	two-tier installation
	procedure 62
two-tier split installation 22, 61
prerequisites 62
U
uninstall
	provisioning, operating system 177
troubleshooting 118
uninstall agent 24, 27
MSI installer 27
UNIX/Linux agent
	communication settings 150
data file sizing 168

machine patch assessment 161
platform support 141
upgrade 141
upgrade local package 142
upgrade remote package 143
unregister vSphere Client VCM Plug-in 147
update statistics for database 154
upgrade
agent proxy machine 144-145
agent proxy machine manually 146
agents 138
failed, troubleshooting 118
provisioning, operating system 187
UNIX/Linux agent 141
UNIX/Linux agent local package 142
UNIX/Linux agent remote package 143
VCM 20, 138-139
VCM Remote client 141
virtual environments 144
vSphere Client VCM Plug-in 147
Windows agents 140
upgrading 127
URL for Report Manager 56, 80, 107
URL for Web Service 56, 80, 106
user permissions errors for SSRS 54, 77, 103
V
center Server 144, 163
cCloud Director 144, 163
VCM

component-specific settings 149
database backup 129
database recovery models 151
supports 64-bit environments 117
supports three-tier installations 22, 117
upgrade 139
VCM installation 117
on virtual machine 29
VCM maintenance plan 153
VCM Remote

t virtual directory 120
VCM Remote client
upgrade 141
VCM Security Guide

certificates 33
	system prerequisites 23
VCM upgrade and migration 20
version
	SQLXML 60, 85, 112
virtual directory
	VCM Remote 120
virtual directory permissions 120
virtual environments

data collection 144, 163
upgrade 144
virtual machine VCM installation 29
virtual requirements for Agent Proxy 164
virtualization
	Agent Proxy 163
	hardware 164
VMware Cloud Infrastructure 163
vShield Manager 144, 163
vSphere Client VCM Plug-in 147
upgrade 147
W
WCF ISAPI extensions 54, 76, 101
WCl uses PowerShell 159
Web service errors for SSRS 54, 77, 103
windir environment variable 27
Windows

FIPS 164

Windows agent

communication settings 150
data file sizing 167
upgrade 140
Windows agent data file sizing 167
Windows boot image
provisioning, operating system 180
Windows directories
provisioning, operating system import 182
Windows import
provisioning, operating system 183
Windows Server 2008 R2 41, 63, 89
worksheets for sizing environment 15, 17
X
X.509 RFC standard 34