vCloud Automation Center Installation Guide
vCloud Automation Center 5.2.1

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:
https://www.vmware.com/support/pubs/

The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
# Table of Contents

1 Overview of vCAC Deployment ......................................................... 1
   Administration Portal Web Site ..................................................... 1
   Reports Web Site ......................................................................... 1
   Model Manager ........................................................................... 2
   vCloud Automation Center Service .............................................. 2
   vCAC Database .......................................................................... 2
   Distributed Execution Managers .................................................. 2
   vCAC Agents .............................................................................. 3
      Virtualization Proxy Agents ..................................................... 3
      Integration Agents .................................................................. 3
      WMI Agent ........................................................................... 3
2 Preparing for vCAC Installation .................................................... 5
   Licensing vCAC for Installation .................................................... 5
   Authorization Store ..................................................................... 5
      File-based Authorization Store ................................................. 5
      SQL-based Authorization Store ................................................ 5
      Active Directory Authorization Store ...................................... 5
   Database Deployment ................................................................. 6
   SSL Configuration ...................................................................... 6
      IIS Certificate Requirement ..................................................... 6
      Adding the Batch Logon Right for vCAC Model Manager Web Service .............................................. 6
      Adding the Service Logon Right for the vCAC Model Manager Web Service .................................... 7
      Security Passphrase ............................................................... 7
   Firewall Configuration ............................................................... 8
   vCAC Installation Profiles .......................................................... 8
      Core vCAC Components .......................................................... 8
      Agents and DEM Workers ....................................................... 9
   Installation Prerequisite Checklist .............................................. 9
      Database Server Requirements ............................................... 9
      Web Server Requirements ..................................................... 10
      vCAC Server Requirements .................................................. 11
      DEM Requirements .............................................................. 11
   vCAC Prerequisite Checker ....................................................... 11
   Users and Credentials Required for Installation ........................ 11
   Users and Credentials Required for vCAC Services ..................... 12
   Installation Planner ................................................................. 12
3 Installing vCAC ..................................................................................... 17
   High-Level Installation Process ................................................................. 17
   Downloading the vCloud Automation Center Installation Package .......... 17
      Installation Package Contents ................................................................. 17
   Installing and Running the vCAC Prerequisite Checker ......................... 19
      Installing and Running the vCAC Prerequisite Checker ....................... 19
   Preparing the Authorization Store............................................................. 20
      Preparing a SQL-based Authorization Store ........................................... 20
      Preparing an Active Directory–based Authorization Store ..................... 20
   Creating the vCAC Database ..................................................................... 21
      Verifying Database Installation Prerequisites ........................................ 21
      Preparing an Empty Database for Installation ....................................... 22
      Creating the vCAC Database by Using the Wizard .................................. 23
      Creating the vCAC Database Manually ................................................ 24
      Creating a SQL-based Authorization Store Manually ............................. 25
   Enabling Database Access from the Manager Service ............................. 25
   Installing vCAC Components ................................................................... 26
      Using Setup.exe to Install vCAC Components ....................................... 26
   Installing vCAC Web Components ............................................................. 27
      Verifying the Web Component Installation Prerequisites ....................... 27
      Installing the vCAC Web Components .................................................. 28
   Installing the Manager Service (vCAC Server) ......................................... 31
      Verifying the Manager Service Installation Prerequisites ..................... 31
      Installing the Manager Service ............................................................. 32
      Configuring the Manager Service ........................................................ 33
   Installing the Distributed Execution Managers ....................................... 35
      Verifying the Distributed Execution Manager Installation Prerequisites .... 35
      Installing the DEM Orchestrator or Worker ......................................... 36
   Preserving the Passphrase Used for Installation ....................................... 37
   Starting the Console ................................................................................. 37
   Installing and Configuring vCAC Components by Using the Command Line ..................................................................................... 38
      Installing vCAC Components by Using the Command Line .................. 38
      Configuring vCAC by Using vCAC-Config.exe ...................................... 39
   Installation Troubleshooting .................................................................... 44
      Installation of Model Manager Data Fails .............................................. 44
      Error Starting Administration Portal Website ....................................... 45
Post-Installation Configuration ................................................................. 45
Specifying a Different SMTP Port ............................................................. 45
Installing in High Availability Mode ....................................................... 46
About Installing the Failover vCAC Server ............................................ 46
About Installing Redundant Distributed Execution Managers ............... 46
About Installing Redundant Web Servers .............................................. 47
Failing Over to the Failover vCAC Server ............................................... 47
Installing vCAC in Web Farm Configuration ........................................... 48
Creating the Session State Database ..................................................... 48

4 Integrating with Provisioning Resources ........................................... 51
DEM Worker Overview ........................................................................... 51
Amazon EC2 Requirements ................................................................. 51
KVM (RHEV) Requirements ................................................................. 51
SCVMM Requirements ......................................................................... 51
vCAC Agent Overview ........................................................................... 53
Planning Your vCAC Proxy Agents ....................................................... 54
Configuring Proxy Agents ..................................................................... 55
Enabling Remote WMI Requests on Windows Machines ..................... 55
Virtual Desktop Integration .................................................................. 55
External Provisioning Integration ......................................................... 56
Using Visual Basic Scripts in Provisioning ........................................... 56
vCAC Agent Relationships .................................................................... 57
vCAC Agent Installation Location and Requirements ........................... 58
Hypervisor Proxy Agent Installation Requirements ................................. 58
WMI Agent Installation Requirements .................................................. 60
VDI Integration Agent Installation Requirements .................................... 61
EPI Agent Installation Requirements .................................................... 62
Preparing Endpoints for vSphere Agents .............................................. 64
Installing a vCAC Agent ........................................................................ 65
Using a Script to Install Multiple Agents .............................................. 72
Modifying Proxy Agent Configurations ............................................... 72

5 Upgrading to vCAC 5.2.1 ................................................................. 75
Supported Upgrade Paths ....................................................................... 75
Verify the Current vCAC Version ......................................................... 75
Create or Import SSL Certificates ....................................................... 75
Allow Machine-Related Operations to Complete .................................. 75
Verify All Data Collections Are Completed and Successful ......................... 75
Record DEM, Agent, and Endpoint Information ........................................ 76
Record All Service User Credentials.......................................................... 77
Uninstall All Customizations...................................................................... 77
Stop All vCAC Services ........................................................................... 78
Back Up Customization Files .................................................................. 78
Back Up vCAC Component Hosts ............................................................... 79
Back Up the AzMan Store.......................................................................... 79
Identify and Back Up the vCAC Database.................................................. 79
Verify Installation Prerequisites............................................................... 80
Upgrading to vCAC 5.2.1 ......................................................................... 80
Stopping All vCAC services ...................................................................... 81
Upgrading vCAC Components ................................................................. 81
Starting All vCAC services......................................................................... 82
Start the Console .................................................................................... 82
Post-Upgrade Steps ................................................................................ 83
Merge Configuration Files ....................................................................... 83
Rebuild WinPE Images ........................................................................... 83

6 Uninstalling and Reinstalling vCAC Components ....................... 85

Uninstalling vCAC Server ....................................................................... 85
Modifying Installed Components ............................................................ 85
About Reinstalling vCAC ......................................................................... 85
Relocating the vCAC Instance ................................................................. 86
Updating vCAC Licenses ......................................................................... 86
Updating Your vCAC License .................................................................. 86

A Installing the Extensibility Toolkits ........................................... 87

Downloading the vCloud Automation Center
Installation Package for Extensibility...................................................... 87
Installation Package Contents ................................................................. 87
Installation Prerequisites ....................................................................... 88
Installing vCloud Automation Center Designer ......................................... 88
Installing the vCloud Automation Center Development Kit ...................... 89
Add vCAC Workflow Activities to Visual Studio ..................................... 90
Updating the CloudUtil Application Configuration ................................ 90
Table of Contents

Uninstalling the Extensibility Toolkits ............................................................91
Upgrading the Extensibility Toolkits ..............................................................92

B Installing the vCAC Self-Service Portal Website .............................. 93
  Downloading the vCAC Self-Service Portal Website............................93
      Installation Package Contents.............................................................93
  Installation Prerequisites .......................................................................93
      Verifying Installation Prerequisites ...................................................94
  Installing the vCAC Self-Service Portal Website ...................................94
  Enabling the Connect Using SSH option for Linux Machines ...............95
  Upgrading or Reinstalling the vCAC Self-Service Portal .....................96
About This Book

This information describes the installation and initial configuration of VMware vCloud Automation Center™ (vCAC) 5.2.1 and its agents. It is intended for system administrators and operators who are responsible for preparing the installation environment and installing vCAC, the required vCAC agents and associated software.

Information on upgrading from vCAC 5.2 to vCAC 5.2.1 is also provided.
Chapter 1 Overview of vCAC Deployment

This information describes the essential elements of vCloud Automation Center. Figure 1 shows the elements and their relationships to each other.

Figure 1 Elements of vCAC

Note: Chapter 2 provides important information about the configurations in which vCAC components can be deployed, including requirements for co-hosting some components.

Administration Portal Web Site

The Administration web site provides access to the vCAC web console at https://web_server_hostname/vCAC. The console provides the user interface to vCAC. The web console communicates with the Model Manager, which provides it with updates from the DEM, proxy agents and database.

Reports Web Site

The reports web site provides access to vCAC reports, available through a link in the vCAC console and at https://web_server_hostname/vCACReports. The reports web site includes reports on the machines managed by the vCAC server, the resources they use, vCAC elements and policies, and other topics.
Model Manager

The Model Manager manages core vCAC and custom models. The Model Manager provides services and utilities for persisting, versioning, securing and distributing the different elements of the model and for communicating with the vCAC portal website and Distributed Execution Managers (DEMs). The Model Manager supports the creation, configuration, and deployment of new models without any code development or compilation. The Model Manager communicates with the database, the DEMs, and the portal website.

The Model Manager is divided into two separately installable components — the Model Manager Web Service and the Model Manager Data component.

Models are used to facilitate the integration of vCAC with external systems and databases and to implement business logic to be executed by a DEM. Models are composed of:

- Secure Multi-Tenancy — Controls that can see what data and who can execute which business logic, leveraging existing authentication and business groupings
- Unified Data Model — Exposes data from the vCAC database and external databases within the model through a secure auto-generated REST API
- Editable Business Logic — Specifies the workflows and activities to be executed
- Execution Policies — Regulate when and where business logic is executed

vCloud Automation Center Service

The vCloud Automation Center service (commonly called the Manager Service) coordinates communication between vCAC agents, the vCAC database, Active Directory and SMTP. The Manager Service communicates with the portal website through the Model Manager. This service requires administrative privileges to run.

The system hosting the Manager Service is typically called the vCAC Server.

vCAC Database

vCAC uses a Microsoft SQL Server database to maintain information about the machines it manages and its own elements and policies. This database is typically created during vCAC installation.

Distributed Execution Managers

A Distributed Execution Manager (DEM) executes the business logic of custom models, interacting with the vCAC database and with external databases and systems as required. DEMs also manage cloud and physical machines for vCAC.

Each DEM instance performs one of two roles: Worker or Orchestrator. The Worker role is responsible for executing workflows, while the Orchestrator role is responsible for monitoring DEM Worker instances, pre-processing workflows for execution, and scheduling workflows.

The DEM Orchestrator performs the following tasks:

- Monitors the status of DEM Workers and ensures that if a Worker instance stops or loses its connection to the Model Manager, its workflows are put back in the queue for another DEM Worker to pick up.
• Manages scheduled workflows by creating new workflow instances at the scheduled time.
• Ensures that only one instance of a particular scheduled workflow is running at a given time.
• Pre-processes workflows before execution, including checking preconditions for workflows (used in the implementation of the “RunOneOnly” feature) and creating the workflow execution history.

Exactly one DEM Orchestrator instance is designated as the active Orchestrator that performs the tasks listed above. The DEM Orchestrator is essential for the execution of workflows and therefore VMware strongly recommends that you install at least one additional Orchestrator instance on a separate machine for failover in the event that there is an issue with the machine on which the DEM Orchestrator is running or the Orchestrator loses its connection to the Model Manager. If a DEM Orchestrator is not the currently active Orchestrator, it monitors the active Orchestrator’s status so that it can take over as the active Orchestrator should the currently active Orchestrator go offline.

**vCAC Agents**

vCAC uses agents to integrate with external systems.

**Virtualization Proxy Agents**

The virtual machines managed by vCAC are created on virtualization hosts. vCAC uses virtualization proxy agents to send commands to and collect data from ESX Server, XenServer, and Hyper-V virtualization hosts and the virtual machines provisioned on them.

A proxy agent:
• Typically requires administrator-level access to the virtualization platform it manages
• Communicates with the Manager Service
• Is installed separately with its own configuration file

**Integration Agents**

Virtual desktop integration (VDI) PowerShell agents allow vCAC to integrate with external virtual desktop systems. Currently, virtual machines provisioned by vCAC can be registered with XenDesktop on a Citrix Desktop Delivery Controller (DDC) and their owners can access the XenDesktop Web Interface from within vCAC.

External provisioning integration (EPI) PowerShell agents allow vCAC to integrate external systems into the machine provisioning process. For example, integration with Citrix Provisioning Server enables provisioning of machines by on-demand disk streaming, and an EPI agent allows you to run Visual Basic scripts as extra steps during the provisioning process.

VDI and EPI agents require administrator-level access to the external systems with which they interact.

**WMI Agent**

The vCAC Windows Management Instrumentation (WMI) agent enables the collection of certain data from Windows machines managed by vCAC.
Chapter 2 Preparing for vCAC Installation

This information guides you through the planning process for your vCloud Automation Center installation and provides a high-level overview of the installation process. Before you install vCAC, you should be aware of the following considerations. Depending on the details of your deployment, some of these may require additional setup or configuration.

Licensing vCAC for Installation

The method of obtaining vCAC licenses is new in vCAC release 5.2.1. Before you can install vCAC 5.2.1, you must obtain the appropriate vCAC licenses from the VMware License Portal. At least one vCAC license is required.

Authorization Store

vCAC uses Windows Authentication and the Windows Authorization Manager (AzMan) to authenticate and authorize users. During installation, you can select an authorization store type:

- File-based
- SQL-based
- Active Directory

Once you select an authorization store type, you cannot change it after installation.

File-based Authorization Store

File-based authorization store is implemented as an XML file on the vCAC Server (Manager Service host). If selected, the vCAC installer automatically creates the authorization file.

This is the simplest type of authorization store and has no prerequisites, which is useful for quick installations for evaluation purposes. However, file-based authorization is supported only if the Manager Service and the Model Manager components are co-hosted.

SQL-based Authorization Store

SQL-based authorization store uses the vCAC database to store authorization information. If selected, the vCAC installer provides an option to automatically create the authorization tables in the database. You can also create the authorization store manually in advance.

Aside from ensuring continuous access from the Manager Service and the Model Manager to the database, there are no prerequisites for this type of authorization store. However, this option is not available if you select SQL-based authentication for the database (rather than Windows authentication).

Active Directory Authorization Store

Active Directory authorization store is implemented using Active Directory (AD), or the Lightweight Directory Services (LDS) component of AD. If selected, you must prepare the authorization store in AD or

**Database Deployment**

When you install vCAC, you can select to connect to the database using SQL-based authentication or Windows authentication. VMware recommends that you deploy a dedicated server running Microsoft SQL Server to host the vCAC database.

The vCAC installer provides three options for creating the vCAC database:

- Automatically
- Manually
- By creating an empty database and using the installer to install the vCAC schema in the existing database

See "Creating the vCAC Database" on page 21 for more information.

**SSL Configuration**

vCAC and its components are installed to use HTTPS as the transport protocol, which ensures secure communication between vCAC components. As a result, before beginning a vCAC installation, you must decide which type of SSL certificate you will use.

VMware recommends that you use a domain certificate from a trusted certificate authority if you are installing vCAC in a distributed or production environment.

**IIS Certificate Requirement**

When you buy a certificate from an authority, the certificate typically does not include a friendly name, which is a name you can use to easily identify the certificate during installation. However, when you import the certificate, you can assign it a friendly name. Refer to the Microsoft documentation on configuring SSL for IIS.

All host names provided during installation must be specified as fully qualified domain names.

**Adding the Batch Logon Right for vCAC Model Manager Web Service**

The vCAC Prerequisite Checker verifies that the identity of the current Windows logon identity is assigned the **Log on as a batch job** right (Windows Local Policy). This right is required for the domain user that you are planning to use as the IIS application pool identity for the Model Manager Web Service.

To add the Log on as a batch job right:

1. From the **Control Panel**, click **System and Security**.
2. Click **Administrative Tools**.
3. Double-click **Local Security Policy**.
4. Expand **Local Policies**, then select **User Rights Assignment**.
5. Double-click **Log on as a batch job**.
6. Click Add User or Group.

7. In Enter the object names to select, type the name of the domain user that you plan to use as the IIS application pool identity for the Model Manager Web Service, and click OK.

8. Click OK.

If you want to assign the Log on as a batch job right to another identity, in the vCAC Prerequisite Checker:

1. Click Settings.

2. In Model Manager Web Application Pool Identity, type the name of the service account you want to use.

3. Rerun the vCAC Prerequisite Checker.

Adding the Service Logon Right for the vCAC Model Manager Web Service

The current Windows logon identity must be assigned the Log on as a service right (Windows Local Policy), which is required to start the Manager Service.

To add the Log on as a service right:

1. From the Control Panel, click System and Security.

2. Click Administrative Tools.


4. Expand Local Policies, then select User Rights Assignment.

5. Double-click Log on as a service.

6. In Enter the object names to select, type the name of the domain user that you plan to use as the IIS application pool identity for the Model Manager Web Service, and click OK.

7. Click OK.

Ensure that the user you added is not assigned the Deny log on as a service right.

Security Passphrase

A passphrase is required to configure vCAC components. A passphrase is a series of words used to create a phrase that generates the encryption key that is used to protect data while at rest in the database. The passphrase used must be the same for a distributed environment. The passphrase is required during an upgrade.

After you install vCAC, the passphrase is stored in the GeneratedPropertyFile file located in C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool. VMware recommends that you move the GeneratedPropertyFile file from the file system to secure media and store it in a secure location.

Follow these guidelines when creating a security passphrase for the first time:

- Use a phrase that is greater than 8 characters and long enough to be hard to guess, but one you will remember
- Include uppercase, lowercase and numeric characters, and symbols
• Avoid using common phrases found in literature or music
• Avoid using words found in the dictionary
• Avoid using your user name, real name, or company name
• Select one that is significantly different from previous passwords or passphrases

**Firewall Configuration**

All vCAC components (including DEMs and agents) and all virtualization hosts (KVM (RHEV), ESX Servers, XenServers, Hyper-V servers) managed by vCAC should be installed on the same network to avoid firewall interference with communication between components.

If firewalls exist between the systems that will host the components of your vCAC installation, you must ensure that the appropriate ports are open between the vCAC hosts. Table 1 describe the ports that must be open.

In addition to the ports listed in Table 1, you must enable Microsoft Distributed Transaction Coordinator Service (MS DTC) communication between all servers in the deployment. The vCAC Prerequisite Checker validates whether MS DTC is running and that the required ports are open.

**Table 1**  TCP Ports used by vCAC

<table>
<thead>
<tr>
<th>Source Component</th>
<th>Target Component</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager Service</td>
<td>SQL Server instance containing vCAC database</td>
<td>MSSQL</td>
<td>1433</td>
</tr>
<tr>
<td>Web components</td>
<td>Manager Service</td>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>SQL Server instance containing vCAC database</td>
<td>MSSQL</td>
<td>1433</td>
</tr>
<tr>
<td>proxy agents</td>
<td>Manager Service</td>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>virtualization host</td>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>guest agents</td>
<td>Manager Service</td>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>DEMs</td>
<td>Manager Service</td>
<td>HTTPS</td>
<td>443</td>
</tr>
</tbody>
</table>

**vCAC Installation Profiles**

This information describes a typical deployment topology for vCAC. For information about hardware recommendations and scalability considerations, refer to the *vCloud Automation Center Reference Architecture*.

**Core vCAC Components**

Table 2 describes a typical server topology for the core vCAC components and the associated installer files.

Chapter 3 provides detailed installation steps for setting up each of these servers.
### Table 2  Core vCAC Components and Installers

<table>
<thead>
<tr>
<th>Server Role</th>
<th>vCAC Components</th>
<th>Installer File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>all servers</td>
<td>Prerequisite Checker</td>
<td>vCAC-PrereqChecker-Setup.exe</td>
</tr>
<tr>
<td></td>
<td>vCAC Database</td>
<td>Setup.exe</td>
</tr>
<tr>
<td></td>
<td>(manual installation)</td>
<td>DBInstall.zip</td>
</tr>
<tr>
<td>Database Server</td>
<td>Model Manager</td>
<td>Setup.exe</td>
</tr>
<tr>
<td></td>
<td>(Web and Data)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Portal Website</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reports Website</td>
<td></td>
</tr>
<tr>
<td>Web Server</td>
<td>Manager Service</td>
<td>Setup.exe</td>
</tr>
<tr>
<td>vCAC Server</td>
<td>DEM Orchestrator</td>
<td>Setup.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Agents and DEM Workers

vCAC Agents and DEM Workers can be installed on the vCAC Server or any other server in your deployment. The number and types of agents varies depending on the provisioning resources in your implementation. Table 3 lists the vCAC component and the associated installer files.

Chapter 4 provides information about planning your vCAC Agents and DEM installations.

### Table 3  vCAC Agent and DEM Installers

<table>
<thead>
<tr>
<th>vCAC Component</th>
<th>Installer File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEM Worker</td>
<td>Setup.exe</td>
</tr>
<tr>
<td>vCAC Agent</td>
<td>Setup.exe</td>
</tr>
</tbody>
</table>

**Note:** VMware recommends that you install and run the Prerequisite Checker (vCAC-PrereqChecker-Setup.exe) before installing the DEM.

### Installation Prerequisite Checklist

This section describes the system configuration requirements for each installation profile that must be in place before you install vCAC. For operating system and high-level environment requirements, see the *vCloud Automation Center Support Matrix*.

### Database Server Requirements

- TCP/IP protocol enabled for MSSQLSERVER
- Microsoft Distributed Transaction Coordinator Service (MS DTC) enabled on all SQL nodes in the system
- No firewalls between Database Server and the Web server or vCAC Server, or ports opened as described in Firewall Configuration
If using SQL Server Express, the SQL Server Browser service must be running.

**Web Server Requirements**

This section includes requirements for both the Web site components and the Model Manager Web Services.

Internet Information Services (IIS) modules:
- WindowsAuthentication
- StaticContent
- DefaultDocument
- ASPNET
- ISAPIExtensions
- ISAPIFilter

IIS Authentication:
- Windows Authentication enabled
- AnonymousAuthentication disabled
- Negotiate Provider enabled
- NTLM Provider enabled
- Windows Authentication Kernel Mode enabled
- Windows Authentication Extended Protection disabled

IIS Windows Process Activation Service roles:
- ConfigurationApi
- NetEnvironment
- ProcessModel
- WcfActivation
- HttpActivation
- NonHttpActivation

Other:
- Microsoft Distributed Transaction Coordinator Service (MS DTC) enabled
- No firewalls between the Web server and the Database Server or vCAC Server, or ports opened as described in Firewall Configuration
- Log on as a batch job right for the domain user that you are planning to use as the IIS application pool identity for the Model Manager Web Service
- Log on as a service right for the domain user that you are planning to use as the IIS application pool identity for the Model Manager Web Service
vCAC Server Requirements

- Microsoft Distributed Transaction Coordinator Service (MS DTC) enabled
- No firewalls between vCAC Server and Database Server or web server, or ports opened as described in Firewall Configuration
- Manager Service’s time should match the database’s time

DEM Requirements

In addition to the following general requirements for Distributed Execution Managers, DEM Worker instances may have additional requirements depending on the provisioning resources that they interact with. For more information on specific requirements for DEM Workers, see Chapter 4.

- .NET Framework 4.5
- Windows PowerShell version 2.0
- SecondaryLogOnService running
- No firewalls between DEM host and vCAC Server, or ports opened as described in Firewall Configuration

vCAC Prerequisite Checker

The vCAC Prerequisite Checker helps you ensure that you have satisfied all installation prerequisites. When you run the vCAC Prerequisite Checker, it lists each system requirement and its status. For each requirement that is not satisfied, the tool provides further information including the recommended actions. VMware strongly recommends that you run the vCAC Prerequisite Checker before installing any of the core vCAC components as described in Chapter 3.

Users and Credentials Required for Installation

Before installing vCAC, add the user under which you plan to execute the vCAC installation programs to the Administrator group on the installation host.

Additionally, the following considerations apply for the credentials that you provide when using the installer to create the vCAC database:

- The user must have the `sysadmin` role in SQL Server to be able to create and alter the size of the database.
- On the vCAC Database Connection Configuration page you have the option to Use Windows Authentication. If you select this option, the installer uses the credentials under which you executed the installer to create the database. If you do not select this option, you can provide the specific credentials to use for database creation.
- On the vCAC Database Configuration page you have the option to Use pre-created empty database. If you select this option, the user credentials that you provide need only have `dbo` privileges for the pre-created database and not the `sysadmin` role.
- If you use the installer to create a SQL-based authorization store (regardless of how you create the vCAC database), the user credentials you provide must have the `sysadmin` role.
Users and Credentials Required for vCAC Services

During vCAC installation, you are prompted to provide user credentials for various vCAC services and components. VMware recommends that you create users specifically for running vCAC services with the minimum required privileges and identify these user credentials before you begin installation. Table 4 describes the required privileges for each service or component.

**Table 4  Required Credentials for vCAC Services**

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum User Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>Domain user with local Administrator privileges on all hosts on which Model Manager Web is installed.</td>
</tr>
<tr>
<td>Reports Website</td>
<td>Domain user.</td>
</tr>
</tbody>
</table>
| Model Manager Web       | Domain user with:  
  - Local Administrator privileges on host on which Model Manager Web is installed  
  **Note:** Full Administrator privileges are not required if the service user has modify privileges for C:\Windows\Temp  
  - **dbo** privileges for the vCAC database |
| Manager Service         | Domain user with:  
  - Local Administrator privileges on host on which Manager Service is installed  
  - Local Administrator privileges on all hosts on which Model Manager Web is installed  
  - **dbo** privileges for the vCAC database  
  To authorize vCAC users in a particular Active Directory Domain, the Manager Service user must belong to the Windows Authorization Access group for that domain. |
| DEM                     | Domain user with:  
  - Local Administrator privileges on all hosts on which Model Manager Web is installed |
| Proxy Agent             | Domain user.                                                                                                                                             |

**Installation Planner**

VMware recommends that you use the following tables to record important information before you install the vCAC components. You are prompted to provide these values at various times in the installation process for different components.

**Authentication Store Information**

- **Store type (circle one):** SQL  AD  XML (not supported in distributed environment)
- **Details:** 

---

---
**SMTP Protocol**

Circle one:  **SSL**  non-SSL

---

**Table 5  License Information**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Automation Center (Desktop)</td>
<td></td>
</tr>
<tr>
<td>vCloud Automation Center (Server)</td>
<td></td>
</tr>
<tr>
<td>vCloud Suite</td>
<td></td>
</tr>
<tr>
<td>vCloud Automation Center Development Kit</td>
<td></td>
</tr>
</tbody>
</table>

**Table 6  Database Information**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Instance name</td>
<td></td>
</tr>
<tr>
<td>Database name</td>
<td></td>
</tr>
<tr>
<td>Database user's credentials</td>
<td></td>
</tr>
<tr>
<td>Database data directory</td>
<td></td>
</tr>
<tr>
<td>Database log directory</td>
<td></td>
</tr>
</tbody>
</table>

**Table 7  Security Information**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security passphrase</td>
<td></td>
</tr>
</tbody>
</table>

**Table 8  Web Site Configuration for HTTPS Port, Certificate, and Virtual Applications**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web site</td>
<td></td>
</tr>
<tr>
<td>HTTPS Port number</td>
<td></td>
</tr>
<tr>
<td>SSL Certificate type</td>
<td></td>
</tr>
<tr>
<td>Suppress certificate mismatch checking (Y/N)</td>
<td></td>
</tr>
<tr>
<td>vCAC IIS Virtual Applications and Applications Pools</td>
<td></td>
</tr>
<tr>
<td>vCAC name</td>
<td></td>
</tr>
<tr>
<td>Report name</td>
<td></td>
</tr>
<tr>
<td>Model Manager name</td>
<td></td>
</tr>
</tbody>
</table>
### Table 9  vCAC Service Account Information

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name in Domain\User format</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>

### Table 10  vCAC AzMan Authorization Store Type Information

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File-based XML (Y/N)</td>
<td></td>
</tr>
<tr>
<td>MSSQL server (Y/N)</td>
<td></td>
</tr>
<tr>
<td>Active Directory (Y/N)</td>
<td></td>
</tr>
<tr>
<td>If creating MSSQL AzMan authorization store, AzMan AD connection string</td>
<td></td>
</tr>
</tbody>
</table>

### Table 11  vCAC Model Manager Information

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name (FQDN)</td>
<td></td>
</tr>
<tr>
<td><strong>Use default log location (Y/N)</strong></td>
<td></td>
</tr>
<tr>
<td>Log directory (or use default)</td>
<td></td>
</tr>
<tr>
<td><strong>SMTP Configuration:</strong></td>
<td></td>
</tr>
<tr>
<td>Enable SSL (Y/N)</td>
<td></td>
</tr>
<tr>
<td>vCAC administration Web site host name</td>
<td></td>
</tr>
<tr>
<td>SMTP server</td>
<td></td>
</tr>
<tr>
<td>From address</td>
<td></td>
</tr>
<tr>
<td><strong>Use anonymous SMTP authorization Y/N</strong></td>
<td></td>
</tr>
<tr>
<td>User name in Domain\User format</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>

**Table 12  vCAC Server Information**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name (FQDN)</td>
<td></td>
</tr>
<tr>
<td><strong>Enable Web farm Support (Y/N)</strong></td>
<td></td>
</tr>
<tr>
<td>Session state database name</td>
<td></td>
</tr>
<tr>
<td>Manager Service log directory</td>
<td></td>
</tr>
<tr>
<td>vCAC Web site log directory</td>
<td></td>
</tr>
</tbody>
</table>

**Table 13  Email Server Information**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP server host name</td>
<td></td>
</tr>
<tr>
<td>SMTP Port</td>
<td></td>
</tr>
<tr>
<td>Email address from which to send notifications</td>
<td></td>
</tr>
<tr>
<td>SMTP server user credentials</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 3 Installing vCAC

This chapter describes the procedures for installing the core vCAC components in a typical deployment topology. It assumes you are familiar with the planning information in Chapter 2.

High-Level Installation Process

The high-level steps for installing the core vCAC components are:

- "Downloading the vCloud Automation Center Installation Package," on page 17
- "Installing and Running the vCAC Prerequisite Checker," on page 19
- "Preparing the Authorization Store," on page 20
- "Creating the vCAC Database," on page 21
- "Installing vCAC Components," on page 26
- "Installing vCAC Web Components," on page 27
- "Installing the Manager Service (vCAC Server)," on page 31
- "Installing the Distributed Execution Managers," on page 35
- "Preserving the Passphrase Used for Installation," on page 37

After you install vCAC and verify your installation, you can configure vCAC to communicate with the provisioning resources in your environment, described in Chapter 4.

Optionally, you can install the extensibility toolkits or the vCAC Self-Service Portal. For information about installing the extensibility toolkits, see Appendix A, Installing the Extensibility Toolkits. For information about installing the Self-Service Portal, see Appendix B, Installing the vCAC Self-Service Portal Website.

Downloading the vCloud Automation Center Installation Package

The vCloud Automation Center installation package contains the installers for all vCAC components and associated support tools.

To download the vCloud Automation Center installation package:

1. Download the zip file for vCloud Automation Center from the VMware downloads page at http://www.vmware.com/download/.
2. Extract the files from the zip archive.

Installation Package Contents

Table 14 describes the contents of the primary vCloud Automation Center installation package.
### Table 14  Installation Package Contents

<table>
<thead>
<tr>
<th>Directory Name</th>
<th>Installer File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>DBInstall.zip</td>
<td>Scripts for manually creating the vCAC database and SQL-based authorization store.</td>
</tr>
<tr>
<td>LinuxGuestAgentPkgs</td>
<td>files located in relevant sub-directories</td>
<td>Used in Red Hat Linux kickstart or SUSE AutoYaST provisioning. For more information, see the <em>vCloud Automation Center Operating Guide</em>.</td>
</tr>
<tr>
<td>Setups</td>
<td>Setup.exe</td>
<td>Installs the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• vCAC agents, including proxy agents, integration agents, and the WMI agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Distributed Execution Manager, including Orchestrator and Worker instances</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The core vCAC components, including the database, administration website, reports website, Model Manager, and Manager Service</td>
</tr>
<tr>
<td></td>
<td>vCAC-WinPEBuilder-Setup.exe</td>
<td>Creates WinPE images. For more information, see the <em>vCloud Automation Center Operating Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>VCACBulkOperationsClient-Installer.msi</td>
<td>Enables an enterprise administrator to perform actions on multiple machines simultaneously. For more information, see the <em>vCloud Automation Center Operating Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>GugentZip.zip</td>
<td>Used in WIM-based and SCCM-based provisioning. For more information, see the <em>vCloud Automation Center Operating Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>GugentZip_x64.zip</td>
<td></td>
</tr>
<tr>
<td>Tools</td>
<td>vCAC-PrereqChecker-Setup.exe</td>
<td>Verifies that the system satisfies all installation prerequisites for vCAC components.</td>
</tr>
<tr>
<td></td>
<td>AzmanUtil.zip</td>
<td>Creates Active Directory-based or SQL-based authorization store.</td>
</tr>
</tbody>
</table>
Installing and Running the vCPC Prerequisite Checker

When you run the vCPC Prerequisite Checker, it lists each system requirement and its status. For each requirement that is not met, the tool provides further information including the recommended actions. VMware strongly recommends that you run the vCPC Prerequisite Checker before installing any of the core vCAC components.

Installing and Running the vCPC Prerequisite Checker

Prerequisites

- Download the vCloud Automation Center installation package.

To install and run the vCPC Prerequisite Checker the first time:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the Tools subdirectory.

2. Right-click vCAC-PrereqChecker-Setup and select Run as administrator.

The first time you install vCAC-PrereqChecker-Setup, it installs and launches the vCPC Prerequisite Checker.

3. From the vCPC Prerequisite Checker you can:

   a. Select the components you want to check before installation and configuration.

   b. (Optional) Use the Settings tab to specify the following configuration settings, if different from the default:

      - From the Web site list, choose the name of the Web site under which you are creating the vCAC Web application.

      - Specify the Database Port for your SQL Server instance.

      - Specify the domain and user name of the account under which to run the Model Manager Web Application Pool.

   c. Click Run Checker.

      The vCPC Prerequisite Checker displays the list of requirements for the selected component and the status of each one.

   d. If any of the requirements do not have a check mark (✓) in the Status column, select that requirement and follow the instructions in the information pane to the right to resolve the problem.

   e. (Optional) Save the vCPC Prerequisite Checker results.

4. Repeat step 3d until all requirements are satisfied.

5. Exit the vCPC Prerequisite Checker.

To run the vCPC Prerequisite Checker after it is installed, you can either:

- Click Start > vCAC Prerequisite Checker

- Click Start > All Programs > VMware > vCAC > vCPC Prerequisite Checker
Preparing the Authorization Store

Depending on the type of AzMan authorization store you select, you may need to do some preparation before running the vCAC installation program.

If you select a file-based authorization store, no preparation is necessary. A file-based store is not recommended for production use.

Preparing a SQL-based Authorization Store

If you select a SQL-based authorization store, you must ensure continuous access to the authorization store by applying the Microsoft hot fix available at: http://support.microsoft.com/kb/975332 to the Manager Service host and all Model Manager Web component hosts.

The installer provides an option to create the authorization store automatically. This option requires that the user running the installer has the sysadmin role in SQL Server. VMware also provides scripts to create the authorization store manually. This must be done after creating the vCAC database. For details, see "Creating a SQL-based Authorization Store Manually," on page 25.

Preparing an Active Directory–based Authorization Store

If you select an Active Directory store, you must prepare an appropriate and accessible store in AD or LDS before beginning installation. VMware provides a tool for creating an AD-based store.

Prerequisites

- Download the vCloud Automation Center installation package.

To create an Active Directory authorization store:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the Tools subdirectory.
2. Extract the AzManUtil.zip archive to a local directory.
3. Execute the application AzManUtil.exe.
4. Click Import.
5. To specify the Source file, click Browse, navigate to the location where you extracted the AzManUtil.zip file, and select the security.xml file.
6. Select Active Directory store.
7. Specify the LDAP connection string including the OU at which you want to create the store, for example, CN=AzManDataStore,OU=vCACAzManStore.
8. Click Import.
9. When the authorization store has been created, exit the AzManUtil application.
10. Grant the Model Manager Web service user administrative access to the AzMan store.
    a. Launch the Authorization Manager administration tool (AzMan.msc).
    b. In the navigation pane, right-click Authorization Manager and select Open Authorization Store.
c. In the Open Authorization Store dialog, select Active Directory or Active Directory Application Model (ADAM).

d. In Store name, type the LDAP connection string that you specified in step 7.

e. Click OK.

f. Right-click the name of the authorization store you just opened and select Properties.

g. On the Security tab, ensure that Administrator is selected under Authorization Manager user role.

h. Click Add.

i. In the Select Users, Computers, or Groups dialog, specify the credentials for the Model Manager Web service user.

j. Click OK twice and exit the Authorization Manager tool.

**Creating the vCAC Database**

The options for creating the vCAC database are:

- Create an empty database and use the vCAC Installation Wizard to install the vCAC schema in the existing database, as described on page 22.
- Use the vCAC Installation Wizard to create the vCAC database, as described on page 23.
- Create the database manually, as described on page 24.

**Note:** Database names must be at least four characters long.

**Verifying Database Installation Prerequisites**

Before creating the vCAC database, use the vCAC Prerequisite Checker to confirm that your database server meets the installation prerequisites.

In addition, if you are using SQL Server Express, the SQL Server Browser service must be running.

To verify vCAC database server prerequisites:

1. If not already installed, install the vCAC Prerequisite Checker, see “Installing and Running the vCAC Prerequisite Checker,” on page 19.

2. If it is already installed, click Start > Prereq Checker.

3. Under Core Install, select Database and clear the check boxes for the other components, including those under Core Upgrade, DEM Install, and vCAC Self-Service Portal Install.

4. If your SQL Server instance is not listening on the default port of 1433, specify the correct port for your instance:
   - Click the Settings tab.
   - In Database Port, specify the port number.

5. Click Run Checker.

The vCAC Prerequisite Checker displays the list of requirements for the selected component and the status of each one.
6. If any of the requirements do not have a green check mark (√) in the Status column, select that requirement and follow the instructions in the information pane to the right to resolve the problem.

7. Repeat step 6 until all requirements are satisfied.

8. Exit the vCAC Prerequisite Checker.

Preventing an Empty Database for Installation

If you choose to install the vCAC schema on an empty database, you must prepare it before you run the vCAC Installation Wizard.

If you are creating the database using the vCAC Installation Wizard or setting up the vCAC database manually, you can skip this procedure and see "Creating the vCAC Database by Using the Wizard," on page 23 or "Creating the vCAC Database Manually," on page 24.

Prerequisites

• Download the vCloud Automation Center installation package.

To prepare an empty database for use with vCAC:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the Database subdirectory.

2. Extract the DBInstall.zip archive to a local directory.

3. Log in to the database host as a user with sufficient rights to create and drop databases (sysadmin privileges) within the SQL Server instance.

4. Edit CreateDatabase.sql and replace all instances of the following variables with the appropriate values:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(DBName)</td>
<td>Name of the database, such as vCAC.</td>
</tr>
<tr>
<td>$(DBDir)</td>
<td>Path to the data directory for the database, excluding the final slash.</td>
</tr>
<tr>
<td>$(LogDir)</td>
<td>Path to the log directory for the database, excluding the final slash.</td>
</tr>
</tbody>
</table>

5. Review the settings in the DB Settings section of CreateDatabase.sql and edit them if desired.

Note: The settings in the script are the recommended settings for the vCAC database. Only ALLOW_SNAPSHOT_ISOLATION ON and READ_COMMITTED_SNAPSHOT ON are required by vCAC.

6. Open SQL Server Management Studio.

7. Click New Query.

A SQL Query window opens in the right-hand pane.

8. On the Query menu, ensure that SQLCMD Mode is selected.

9. Paste the entire modified contents of CreateDatabase.sql into the query window.

10. Click Execute.
Creating the vCAC Database by Using the Wizard

You can use the vCAC Installation Wizard to automatically create the vCAC database or to install the vCAC schema on an existing empty database.

*Note:* The installation host does not need to be the database host. You can run the vCAC Installation Wizard to set up the vCAC database remotely.

**Prerequisites**

- Download the vCloud Automation Center installation package.

To install and configure the vCAC database:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the **Setups** subdirectory.
2. Right-click **Setup.exe** and select **Run as administrator**.
3. On the **Welcome** page, click **Next**.
4. On the **Installation or Upgrade** page, select **New/Repair/Remove**, and click **Start**.
5. On the **End-User License Agreement** page, read the License Agreement, click **I accept the terms in the License Agreement**, then click **Next**.
6. On the **Destination Folder** page, select the folder you want to install to, then click **Next**.
7. On the **Custom Setup** page, select **Database**, and cancel the selection for all other features, then click **Next**.
8. On the **Ready to Install the Program** page, click **Install**.
   The **Wizard Complete** page appears. All of the installation files reside on the destination folder you selected; however, the vCAC database is not configured yet.
9. Optionally, to view the Windows Installer log, select **Show the Windows Installer log**.
10. On the **Wizard Complete** page, click **Finish**.
    The **Welcome to the vCAC Software Configuration Wizard** page appears.
11. On the **Welcome to the vCAC Configuration Wizard** page:
    a. If you plan to use a SQL-based AzMan authorization store, select **Create MSSQL AzMan Authorization store** to create it as part of the initial database configuration. You create the AzMan store once.
    b. Click **Next**.
12. On the **vCAC Database Configuration** page:
    a. In **Database instance**, type the name of the database server.
    b. If you previously prepared an empty database to use for vCAC, select **Use existing empty database** to indicate that the installer should create the vCAC schema in the existing database.
    c. In **Database name**, type the name of the database or use the default name of vCAC.
    d. VMware recommends that you select **Use default data and log directories**. To specify alternative locations for the data and log directories, clear the check box.
e. Select **Use Windows identity of the current logged on user to create the vCAC database and its schema** to use the credentials under which you are running the installer to create the database. Clear the check box to use SQL authentication and provide the credentials with which to connect to the database.

f. Click **Next**.

13. On the **Ready to Configure** page, click **Configure**.

14. When the configuration completes, click **Next**, then **Finish**.

**Creating the vCAC Database Manually**

If you do not want to create the vCAC database using the installer, you can create the database manually. VMware provides a set of scripts for this purpose.

The database scripts assume:

- .NET 4.5 is installed on the SQL Server host
- You are using Windows Authentication (rather than SQL Authentication) to connect to the database

If either of these are not true, edit the **BuildDB.bat** and **DeployVMPS.xml** files and make the needed modifications for your environment before creating the database.

**Prerequisites**

- Download the vCloud Automation Center installation package.

To create the vCAC database using the provided scripts:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the **Database** subdirectory.
2. Extract the **DBInstall.zip** archive to a local directory.
3. Log in to the database host as a user with sufficient rights to create and drop databases (sysadmin role) within the SQL Server instance.
4. Review the database deployment scripts as needed. In particular, review the settings in the **DB Settings** section of **CreateDatabase.sql** and edit them if desired.

**Note:** The settings in the script are the recommended settings for the vCAC database. Only **ALLOW_SNAPSHOT_ISOLATION ON** and **READ_COMMITTED_SNAPSHOT ON** are required by vCAC.

5. Execute the following command with the arguments described in the table:

```bash
BuildDB.bat /p:DBServer=db_server;DBName=db_name;DBDir=db_dir;LogDir=log_dir;ServiceUser=service_user;ReportLogin=web_user
```

<table>
<thead>
<tr>
<th>Argument Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBServer</td>
<td>The SQL Server instance in the format <code>hostname\instance</code> name (or <code>hostname</code> if using the default instance). Default is <code>localhost</code>.</td>
</tr>
<tr>
<td>DBName</td>
<td>Name of the vCAC database. Default is <code>vCAC</code>.</td>
</tr>
</tbody>
</table>
Creating a SQL-based Authorization Store Manually

If you are using a SQL-based authorization store, you can manually create it after creating the vCAC database. The installer also provides an option to create the authorization store automatically.

**Prerequisites**
- Download the vCloud Automation Center installation package.

To create a SQL-based authorization store manually:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the `Database` subdirectory.
2. Extract the `DBInstall.zip` archive to a local directory.
3. Log in to the database host as a user with sufficient rights to create and drop databases (`sysadmin` role) within the SQL Server instance.
4. Execute the `AzManStoreSchema.sql` script:
   a. Open the script in SQL Server Management Studio and examine its contents.
   b. On the **Query** menu, ensure that **SQLCMD Mode** is selected.
   c. Click **Execute**.
5. Repeat step 3 with `AzManStoreExtSP.sql` followed by `AzManStoreData.sql`.

**Enabling Database Access from the Manager Service**

When you install the vCAC database on a separate host from the Manager Service, you must run a script, which is provided with vCAC, on the database to enable the Manager Service to communicate with it. However, you should only run the script if the user name under which the Manager Service will run is not the owner of the vCAC database.

**Note:** If the user name under which the Manager Service will run is the owner of the vCAC database, this script is not required and should not be run.

**Prerequisites**
- Download the vCloud Automation Center installation package.

To enable the Manager Service to communicate with the vCAC database:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the `Database` subdirectory.
2. Extract the **DBInstall.zip** archive to a local directory.
3. Edit **VMPSOpsUser.sql** and replace all instances of **$(ServiceUser)** with the user name under which the vCloud Automation Center service (Manager Service) will run. **Do not** replace **ServiceUser** in the line ending with **WHERE name = N'ServiceUser'**.  
(See "Users and Credentials Required for vCAC Services" in Chapter 2 for information about Manager Service credentials.)
4. Open SQL Server Management Studio.
5. Select the vCAC database (vCAC by default) under **Databases** in the left-hand pane.
6. Click **New Query**.
   A SQL Query window opens in the right-hand pane.
7. Paste the entire modified contents of **VMPSOpsUser.sql** into the query window.
8. Click **Execute**.

### Installing vCAC Components

Setup.exe is used to make a fresh installation of vCAC 5.2.1. It is also used to upgrade vCAC 5.2 to vCAC 5.2.1. The vCAC components installed by Setup.exe include vCAC Server, DEM Orchestrator, DEM workers, and Agents. After you launch Setup.exe, select the component you want to install.

**Note:** If you are installing multiple components in a single host machine, VMware recommends that you install all of the non-server components first, and then install the server on the same machine.

### Using Setup.exe to Install vCAC Components

#### Prerequisites

- Download the vCloud Automation Center installation package.

To install vCAC components:

1. Navigate to the directory where you extracted the zip archive and locate **Setup.exe** in the **Set-ups** directory.
2. Copy **Setup.exe** to the host machine.
3. Right-click **Setup.exe**, and select **Run as administrator**.
4. Click **Next** on the welcome screen.
5. Select **New/Repair/Remove** on the vCAC Installation or Upgrade screen, and click **Start**.
6. Do one of the following:
   - Select **Install vCAC Server** to install vCAC Server, vCAC Database, or vCAC Web Components on the host machine.
   - Select **Install vCAC DEM Orchestrator/Worker** to install the DEM Orchestrator or the DEM Worker on the host machine.
   - Select **Install vCAC Agent** to install an agent on the host machine.
Note: The default port for the vCloud Automation Center server is 443. If the vCloud Automation Center server is installed on a different port and the installation certificate for the DEM Worker does not specify the port where the vCloud Automation Center server is installed, the DEM worker does not start. To prevent this, either install the vCloud Automation Center server using the default port 443, or install the vCloud Automation Center using a port that is different from the default and install the certificate for the DEM Worker specifying that port.

7. Click **Install**.

After installation is complete, click **Finish**. Launch **Setup.exe** on a selected host machine to install another component.

**Installing vCAC Web Components**

The Web components of vCAC include the Administration Website, Reports Website, and the Model Manager. The Model Manager consists of two installable components: Model Manager Web Service and Model Manager Data.

If you do not want to install vCAC within the default Web site, first create a Web site in IIS for use with vCAC, then proceed with the vCAC installation.

**Verifying the Web Component Installation Prerequisites**

To verify the vCAC Web component prerequisites:

1. If not already installed, install the vCAC Prerequisite Checker, see "Installing and Running the vCAC Prerequisite Checker," on page 19.

2. Click **Start > Prereq Checker**.

3. Under **Core Install**, select **Model Manager Web Services** and **Website** and clear the check boxes for the other components, including those under **Core Upgrade**, **DEM Install**, and **vCAC Self-Service Portal Install**.

4. If you are not installing the Web components in the Default Web Site in IIS, specify the Web site to validate:
   - Click the **Settings** tab.
   - From the **Web site** list, choose the name of the Web site under which you are creating the vCAC Web application.

5. If the user credentials under which the Model Manager will run are not the same as the current user:
   - Click the **Settings** tab.
   - In **Model Manager Web Application Pool Identity**, specify the Model Manager user in DOMAIN\username format.

6. Click **Run Checker**.

   The vCAC Prerequisite Checker displays the list of requirements for the selected component and the status of each one.
7. If any of the requirements do not have a green check mark (✓) in the Status column, select that requirement and follow the instructions in the information pane to the right to resolve the problem.

8. Repeat step 7 until all requirements are satisfied.

9. If the vCAC Prerequisite Checker detects that IIS is not installed, you must reregister ASP.NET 4.5 after installing IIS to avoid an error when starting the Administration Website.

   To reregister ASP.NET with IIS, type:

   ```
   C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -iru IISReset
   ```


10. Exit the vCAC Prerequisite Checker.

### Installing the vCAC Web Components

The Web components consist of the Model Manager (Web Service and Data) and both Website components.

    **Note:** All host names specified during the installation process must be fully qualified domain names (FQDN).

**Prerequisites**

- Download the vCloud Automation Center installation package.
- If you have not already reregistered ASP.NET with IIS, type:

  ```
  C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -iru IISReset
  ```


To install the vCAC Web Components:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the **Setups** subdirectory.
2. Right-click **Setup.exe** and select **Run as administrator**.
3. On the **Do you want to allow the following program to make changes to this computer?** dialog box, click **Yes**.
4. On the **Welcome** page, click **Next**.
5. On the **Installation or Upgrade** page, select **New/Repair/Remove**, and click **Next**.
6. Select **Install vCAC Server**, and click **Install**.
7. On the **Welcome** page, click **Next**.
8. On the **End-User License Agreement** page, read the License Agreement, click **I accept the terms in the License Agreement**, then click **Next**.
9. On the Destination Folder page, select the folder you want to install to, then click Next.

10. On the Custom Setup page, select Model Manager Web Service, Model Manager Data, Administration Portal Website, and Reports Website. Cancel the selection for all other features, then click Next.

11. On the Ready to Install the Program page, click Install.

The Wizard Complete page appears. All of the installation files reside on the destination folder you selected; however, vCAC Web Components are not configured yet.

12. (Optional) To view the Windows Installer log, select Show the Windows Installer log.


The Welcome to the vCAC Configuration Wizard page appears.


15. If license keys are not detected, the vCAC License Configuration page appears.

   a. Type a valid vCAC Server license key. You can add all of your license keys at the same time.

   b. If you have a license for the vCloud Automation Center Development Kit and you have not previously added it, add it now. You are not prompted for a license when you install the vCloud Automation Center Development Kit.

12. On the vCAC Database Configuration page:

   a. In Database instance, type the name of the server or click Scan to discover all available servers and select one from the list.

   b. In Database name, type the name of the database (default value is vCAC).

   c. Select Use Windows identity of the currently logged on user to perform configuration tasks that involve database operations to use the credentials under which you are running the installer to connect to the database. Clear the check box to use SQL authentication and provide the credentials with which to connect to the database.

   d. Click Next.

13. On the vCAC Security Information page:

   a. Read the guidelines on the page.

   b. If you already installed components in this environment, type the passphrase that you already created; otherwise, type a new passphrase.

      A passphrase is a series of words used to create a phrase that generates the encryption key that is used to protect data while at rest in the database and for data recovery.

      The passphrase you create during installation must be used across the entire IaaS deployment so that each component has the same encryption keys.

   c. Retype your passphrase to confirm it.

   d. To view the passphrase in text, select Show passphrase.

   **Note:** The passphrase might be required during an upgrade; therefore, you should store it in a secure location or memorize it.

14. On the vCAC Web Site Configuration page:
a. In **Available Web sites**, select **Default Web Site** or another web site from the list.

b. In **Port number**, type an available port number or select 443.

c. Click **Test Binding** to confirm that the port number is available for use.

d. Click **Generate Self-Signed Certificate** if you do not have an available certificate and want to create one.

   If you are installing in a distributed environment, VMware recommends that you use a domain certificate.

   The generated certificate appears in the list of available certificates.

e. In **Available certificates**, select the certificate you want to use.

   • If you imported a certificate after you began the vCAC Configuration Wizard, click **Refresh** so that it appears in the list of available certificates.

   • If you imported a certificate that does not have a friendly name, and it does not appear in the list of available certificates, clear the checkbox for **Display certificates using certificates friendly name** to display the certificate thumbprint.

f. To ensure you selected the correct certificate, click **View selected certificate** to view more information.

g. If you are deploying in a distributed environment and plan to use a single domain certificate for the load balancer (instead of individual certificates for each server in the pool), and the certificate is not a wildcard certificate that also covers the individual servers, select **Suppress mismatch certificate checking**.

h. Click **Next**.

15. On the **vCAC Service Account Configuration** page, specify the user name and password of the service account user who has access the database and is the owner of the selected database, or click **Add Current User**.

16. On the **vCAC AzMan Authorization Store Type** page, select the type of AzMan authorization store you want to use.

   • If you select **File-based XML**, Manager Service and Model Manager Web Service must reside on the same host.

   • If you select **MSSQL Server**, and you do not already have an AzMan authorization store you created manually or during a previous installation, one will be created for you.

   • If you select **Active Directory**, provide the AzMan Active Directory connection string to the authorization store that you previously created.

17. Click **Next**.

18. On the **vCAC Model Manager Configuration** page:

   a. Type the host name of the Model Manager Web Service.

   b. VMware recommends that you select **Use default log location**. To specify an alternative location for the log directory, clear the check box.

   c. Select **Enable SSL** to communicate with the email server using SSL.
d. In vCAC administration Web site host name, specify the fully qualified domain name of the Web server or Web cluster. This information is used to build the base URL for vCAC Console links in notification emails. For example, if you type vCAC-web-cluster.example.com, the base URL for email links is https://vCAC-web-cluster.example.com/vCAC.

e. In SMTP server, specify the host name of the SMTP server.

f. In From address, specify the email address that should appear in the From: address of vCAC notification emails (typically the domain administrator email).

g. If you do not want to use anonymous authentication with the SMTP server, clear Use anonymous SMTP authentication and specify the user credentials with which to authenticate with the SMTP server.

h. Click Next.

19. On the vCAC Web Site Configuration page, leave Enable Web farm support unselected, then click Next.

   This option enables tracking of user session information in a shared session state database. For information about Web farm-based installation, see "Installing vCAC in Web Farm Configuration," on page 48.

20. On the Ready to Configure page, click Configure.

21. At any time while the Configuration Wizard is in process, you can click View configuration log file to view the progress up to the time you opened the log file.

22. When the configuration completes, click Next, then Finish.

For information about setting up additional Web servers, see "About Installing Redundant Web Servers," on page 47.

Installing the Manager Service (vCAC Server)

The Manager Service host is often referred to as the vCAC Server.

If you do not want to install the vCAC application within the Default Web Site, first create a Web site in IIS for use with vCAC, then proceed with the vCAC installation.

Verifying the Manager Service Installation Prerequisites

To verify the Manager Service prerequisites:

1. If not already installed, install the vCAC Prerequisite Checker, see "Installing and Running the vCAC Prerequisite Checker," on page 19.

2. Click Start > Prereq Checker.

3. Under Core Install, select Manager Service and clear the check boxes for the other components, including those under Core Upgrade, DEM Install, and vCAC Self-Service Portal Install.

4. If you are not installing the Manager Service in the Default Web Site in IIS, specify the Web site to validate:

   • Click the Settings tab.
5. Click Run Checker.
   The vCAC Prerequisite Checker displays the list of requirements for the selected component and the status of each one.

6. If any of the requirements do not have a green check mark (✓) in the Status column, select that requirement and follow the instructions in the information pane to the right to resolve the problem.
   If the vCAC Prerequisite Checker detects that IIS is not installed, you must reregister ASP.NET 4.5 after installing IIS to avoid an error when starting the Administration Portal Website. For details, see "Error Starting Administration Portal Website," on page 45.

7. Repeat step 6 until all requirements are satisfied.

8. Exit the vCAC Prerequisite Checker.

Installing the Manager Service

**Note:** All host names specified during the installation process must be fully qualified domain names (FQDN).

**Prerequisites**

- Download the vCloud Automation Center installation package.

**To install the Manager Service:**

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the **Setups** subdirectory.
2. Right-click **Setup.exe** and select **Run as administrator**.
3. On the **Do you want to allow the following program to make changes to this computer?** dialog box, click **Yes**.
4. On the **Welcome** page, click **Next**.
5. On the **Installation or Upgrade** page, select **New/Repair/Remove**, and click **Next**.
6. Select **Install vCAC Server**, and click **Install**.
7. On the **End-User License Agreement** page, read the License Agreement, click **I accept the terms in the License Agreement**, then click **Next**.
8. On the **Destination Folder** page, select the folder you want to install to, then click **Next**.
9. On the **Custom Setup** page, select **Manager Service**. Cancel the selection for all other features, then click **Next**.
10. On the **Ready to Install the Program** page, click **Install**.
    The **Wizard Complete** page appears. All of the installation files reside on the destination folder you selected; however, vCAC Server is not configured yet.
11. To view the Windows Installer log, select **Show the Windows Installer log**.
12. On the **Wizard Complete** page, click **Finish**.
   The **Welcome to the vCAC Configuration Wizard** page appears.

13. To continue to configure vCAC, click **Next** and go to “Configuring the Manager Service”.

14. To cancel, click **Cancel**.

**Configuring the Manager Service**

When configuring the Manager Service, you must have already run Setup.exe and installed the required files, as described in "Installing the Manager Service".

To configure the Manager Service:

1. Click **Start > vCAC Configuration Tool**.
   The configuration tool launches automatically when you complete Setup.exe.

2. On the **Welcome to the vCAC Configuration Wizard** page, click **Next**.

3. On the **vCAC Database Information** page:
   a. In **Database instance**, type the name of the database instance you typed when you set up your database.
   b. In **Database name**, type the name of the database.
   c. Select **Use Windows identity of the currently logged on user to perform configuration tasks that involve database operations** to use the credentials under which you are running the installer to connect to the database. Clear the check box to use SQL authentication and provide the credentials with which to connect to the database.
   d. Click **Next**.

4. On the **vCAC Security Information** page:
   a. Read the guidelines on the page.
   b. If you already installed components in this environment, type the passphrase you already created; otherwise, type a new passphrase.

   A passphrase is a series of words used to create a phrase that generates the encryption key that is used to protect data while at rest in the database and for data recovery.

   The passphrase you create during installation must be used across the entire vCAC deployment so that each component has the same encryption keys.

   c. Retype to confirm your passphrase.
   d. To view the passphrase in text, select **Show passphrase**.

**Note:** The passphrase might be required during an upgrade; therefore, you should store it in a secure location or memorize it.

5. On the **vCAC Web Site Configuration** page:
   a. In **Available Web sites**, select **Default Web Site** or another web site from the list.
   b. In **Port number**, type a port number or select 443.
   c. Click **Test Binding** to confirm that the port number is available for use.
d. Click **Generate Self-Signed Certificate** only if you:
   - Are not installing in a distributed environment
     If installing in a distributed environment, a domain certificate is required.
   - Do not already have an available certificate and want to create a new one

   The generated certificate appears in the list of available certificates

e. In **Available certificates**, select the certificate you want to use.
   - If you imported a certificate after you began the vCAC Configuration Wizard, click **Refresh** so that it appears in the list of available certificates.
   - If you imported a certificate that does not have a friendly name, and it does not appear in the list of available certificates, clear the checkbox for **Display certificates using certificates friendly name** to display the certificate thumbprint.

f. To ensure you selected the correct certificate, click **View selected certificate** to view more information.

g. If you are deploying in a distributed environment and plan to use a single domain certificate for the load balancer (instead of individual certificates for each server in the pool), and the certificate is not a wildcard certificate that also covers the individual servers, select **Suppress mismatch certificate checking**.

h. Click **Next**.

6. On the **vCAC Service Account Configuration** page, type the user name and password of the service account user who has access the database and is the owner of the selected database, or click **Add Current User**, then click **Next**.

7. On the **vCAC AzMan Authorization Store Type** page, select the type of AzMan authorization store you want to use.
   - If you select **File-based XML**, Manager Service and Model Manager Web Service must reside on the same host.
   - If you select **MSSQL Server**, and you do not already have an AzMan authorization store you created manually or during a previous installation, one will be created for you.
   - If you select **Active Directory**, provide the AzMan Active Directory connection string to the authorization store that you previously created.

8. Click **Next**.

9. On the **vCAC Manager Service Configuration** page:
   a. Type the host name of the Model Manager Web Service. VMware recommends that you click **Test** to force the installer to test connectivity to the Model Manager host before proceeding.
   b. Select **Active node with startup type set to automatic** to start the vCloud Automation Center service automatically when the installation completes.
   c. If you select **Disaster Recovery cold standby node**, the vCloud Automation Center service is installed in Manual startup mode rather than Automatic. Select this option when configuring this Manager Service as a standby node in an HA setup.
d. VMware recommends that you select **Use Default Log Location**. To specify an alternative location for the log directory, clear the check box.

e. Click **Next**.

10. On the **Ready to Configure** page, click **Configure**.

11. At any time while the Configuration Wizard is in process, you can click **View configuration log file** to view the progress up to the time you opened the log file.

12. When the configuration completes, click **Next**, then **Finish**.

For information about setting up additional vCAC servers, see "About Installing the Failover vCAC Server," on page 46.

### Installing the Distributed Execution Managers

The Distributed Execution Manager application can be installed as one of two roles: DEM Orchestrator or DEM Worker. At least one DEM instance must be present for each role.

Only one DEM Orchestrator instance is active at any time. The Orchestrator should be installed on a machine with strong network connectivity to the Model Manager host (typically the same machine as the Manager Service). VMware strongly recommends that you install a second DEM Orchestrator on a different machine for failover.

DEM Workers can be installed on any machine in your deployment architecture. As with the DEM Orchestrator, it is important for DEM Workers to have network connectivity to the Model Manager host. Additional DEM instances can be added for redundancy and scalability, including multiple instances on the same machine.

The installation procedure is the same for both the DEM Orchestrator and Worker roles.

### Verifying the Distributed Execution Manager Installation Prerequisites

To verify the DEM prerequisites:

1. If not already installed, install the vCAC Prerequisite Checker, see "Installing and Running the vCAC Prerequisite Checker," on page 19.

2. Click **Start > Prereq Checker**.

3. Under **DEM Install**, select **Worker and Orchestrator Services** and clear the check boxes for the other components, including those under **Core Install**, **Core Upgrade**, and **vCAC Self-Service Portal Install**.

4. Click **Run Checker**.

   The vCAC Prerequisite Checker displays the list of requirements for the selected component and the status of each one.

5. If any of the requirements do **not** have a check mark (✓) in the Status column, select that requirement and follow the instructions in the information pane to the right to resolve the problem.

6. Repeat step 5 until all requirements are satisfied.

7. Exit the vCAC Prerequisite Checker.
Installing the DEM Orchestrator or Worker

**Prerequisites**

- Download the vCloud Automation Center installation package.

To install the DEM Orchestrator or Workers:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the `Setups` subdirectory.
2. Right-click `Setup.exe` and select **Run as administrator**.
3. On the **Welcome** page, click **Next**.
4. On the **Installation or Upgrade** page, select **New/Repair/Remove**, and click **Next**.
5. Select **Install vCAC DEM orchestrator/worker**, and click **Install**.
6. On the Welcome page, click **Next**.
7. On the **End-User License Agreement** page, read the License Agreement, click **I accept the terms in the License Agreement**, then click **Next**.
8. On the **DEM Instance Configuration** page:
   a. In the **DEM Instance Name** box, provide a name that uniquely identifies this instance in your deployment.
      The DEM instance name must not contain spaces and has a maximum length of 128 characters.
   b. In the **DEM Description** box, provide an optional description for this instance.
   c. Select the role that this instance of the DEM should perform.
      - **Worker Role** — As a worker, the DEM executes workflows.
      - **Orchestrator Role** — As an orchestrator, the DEM oversees the DEM worker’s activities, including scheduling and pre-processing workflows, and checking the DEM’s online status.
   d. Click **Next**.
6. On the **Custom Setup** page, click **Next**.
7. On the **Manager Service and Model Manager Web Service Host Configuration** page:
   a. In the **Manager Service Hostname:Port** box, type the host name of the Manager Service host and the port on which the DEM connects to the Manager Service. The port is typically 443.
   b. In the **Model Manager Service Hostname:Port** box, specify the host name of the Model Manager host and the port on which the Model Manager is listening. The port is typically 443.
   c. Specify the user credentials under which the Model Manager Web service is running.
d. Select **Validate Manager Service service endpoint** to test the connection.
e. Click **Next**.

8. On the Service Configuration page:
   a. Select **Start Distributed Execution Manager Service** to start the DEM service automatically when the installation completes.
   b. Specify the user credentials under which to run the DEM service.
   c. Click **Next**.

9. On the **Ready to Install vCAC DEM** page, click **Install**.

10. At any time while the Configuration Wizard is in process, you can click **View configuration log file** to view the progress up to the time you opened the log file.

**Preserving the Passphrase Used for Installation**

After you install vCAC, the passphrase you entered during the installation is stored in the **Generated-PropertyFile** file located in `C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\`. The passphrase is required during an upgrade, and therefore, you must preserve the passphrase for future use.

VMware recommends that you:

1. Copy **GeneratedPropertyFile** to secure media and store it in a secure location.
2. Delete **GeneratedPropertyFile** from the file system to prevent unauthorized access.

**Starting the Console**

When the database, Web component, Manager Service, and DEM installations are complete, you can verify your installation by starting the vCAC Console.

Before accessing the vCAC Console, verify that the following services are running:

- VMware vCloud Automation Center
- VMware DEM-Orchestrator - *InstanceName*
- VMware DEM-Worker - *InstanceName*

**Note:** Scripting and cookies must be enabled in your browser in order to use the vCAC Console. If you are using Internet Explorer, active scripting must be enabled.

To access the vCAC Console:

1. Launch a Web browser and navigate to **https://vCAC_portal_hostname/vCAC**.
2. When prompted, provide Windows credentials for a user with local administrator privileges on the Manager Service host.
The vCAC Console appears.

All local administrators are granted vCAC administrator access by default. From here, you can complete vCAC setup, including adding users to vCAC. For information about vCAC user role and rights assignments, see the *vCloud Automation Center Operating Guide*.

If your credentials when you open the console are the same as the ones the Manager Service is running under, you may see additional activity groups in the activity pane.

### Installing and Configuring vCAC Components by Using the Command Line

This information provides the procedures you can use to install and configure vCAC components by using the command line.

**Installing vCAC Components by Using the Command Line**

You can install vCAC components from the command line. The examples shown here use the /WAIT option, which can be omitted if you want to return to the command line before the program completes.

To set up command line functionality:

1. Launch `Setup.exe`.
2. When the Installation or Upgrade page appears, click **Cancel**.
3. Open a new command prompt, and create a new directory.
4. Change directories to `%tmp%\vcac-installer\Bin`.
5. Copy all of the files in the Bin directory to the new directory created in step 3.
6. Change directories to the new directory.
7. Run the installer from the command line to install vCAC components.
   
   **Install selected**
   
   ```
   start /WAIT vCAC-Server-Setup /s /w /V"/qn ADDLOCAL=componentname,componentname"
   ```
   
   where `componentname` can be:
   
   ManagerService, ModelManagerWeb, ModelManagerData, Website, ReportWebsite, or Database.
   
   For example, to install the Model Manager Web Service and Model Manager Data, type:
   
   ```
   start /WAIT vCAC-Server-Setup /s /w /V"/qn ADDLOCAL=ModelManagerWeb,ModelManagerData"
   ```
   
   **Install all**
   
   ```
   start /WAIT vCAC-Server-Setup /s /w /V"/qn ADDLOCAL=All"
   ```
   
   The Database, Administration Portal Website, Reports Website, Model Manager Web Service, Model Manager Data, and Manager Service are installed.

### Configuring vCAC by Using vCAC-Config.exe

Before you can configure vCAC by using the vCAC-Config.exe program, you must create a property file, `vCAConfigProperty.xml`, that contains all of the key/pair information required to complete the configuration. You can:

- Use the property file that was created during a previous vCAC configuration
- Edit the sample property file supplied by VMware
- Run the vCAC-Config.exe program by using the `/Gen` option

#### Getting Help for Using vCAC-Config.exe

To see all available options for vCAC-Config.exe, type:

```
vCAC-Config.exe /Help
```

#### Creating the vCACConfigProperty.xml

To create the `vCACConfigProperty.xml` file by running the `Setup.exe` program:

- Run `Setup.exe` to install and configure vCAC.

   The `vCACConfigProperty.xml` file is created in `Program Files (86)\VMware\vCAC\Server\Config-Tool\GeneratedPropertyFile` and contains all of the key/value pairs required to replicate the configuration. A date and time stamp is appended to the file name so that you can identify the correct file.

   You must edit the resulting `vCACConfigProperty.xml` file with the correct license keys, certificate, passphrase, and password for the service user.
To create the vCAConfigProperty.xml file by running the vCAC-Config.exe program:

- Run the vCAC-Config.exe program by using the /Gen option to generate the vCAConfigProperty.xml file for any installable component.

  To create a vCAConfigProperty.xml file for all vCAC components, type:

  `vCAC-Config.exe /Gen`

  The Database, Administration Portal Website, Reports Website, Model Manager Web Service, Model Manager Data, and Manager Service are included in the vCAConfigProperty.xml file.

  To create a vCAConfigProperty.xml file for selected vCAC components, type:

  `vCAC-Config.exe /Gen /F:<componentname,componentname,...>`

  where componentname can be:

  ManagerService, ModelManagerWeb, ModelManagerData, Website, ReportWebsite, or Database.

  For example, to create a vCAConfigProperty.xml file for the Model Manager Web Service and Model Manager Data, type:

  `vCAC-Config.exe /Gen /F:<ModelManagerWeb,ModelManagerData>`

  You must edit the resulting vCAConfigProperty.xml file with the key/value pairs for your configuration, including license keys, certificate, passphrase, and password for the service user.

- Create the vCAConfigProperty.xml file manually:

  a. Go to Program Files (x86)\VMware\vCAC\Server\ConfigTool and locate the sample file named vCAC-ConfigProperty.xml. See "Sample Configuration Key/Value Pair for All vCAC Components" on page 41.

  b. Edit the vCAConfigProperty.xml file by defining the key/value pairs for your configuration.

  c. Rename the file or use the default, vCAConfigProperty.xml.

  d. Place the file in either the default directory, Program Files (x86)\VMware\vCAC\Server\ConfigTool\GeneratedPropertyFile, or another directory.

### Configuring vCAC Components by Using the Command Line

**Prerequisites**

- A property file that defines the key/value pairs for your configuration.

  The default path and file name is Program Files (x86)\VMware\vCAC\Server\ConfigTool\GeneratedPropertyFile\vCAConfigProperty.xml; however, any directory or file name can be specified.

To configure vCAC components as defined in your property file, type:

`vCAC-Config.exe /S /P:<value>\vCAConfigProperty.xml`

where:
• /S is required

• /P:<value> is optional; if /P is not specified, vCAC-Config.exe looks for the property file in the current directory

• <vCACConfigProperty.xml> is the name of the property file

Sample Configuration Key/Value Pair for All vCAC Components

The configuration key/value pairs for all vCAC components are shown in this sample vCACConfigProperty.xml file.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<vCACProperties> -<common>
  <!-- Database instance name. Use hostname\named_instance if not default instance -->
  <DATABASE_INSTANCE>localhost</DATABASE_INSTANCE>
  <!-- Database name to be created -->
  <DATABASE_NAME>vCAC</DATABASE_NAME> </common> -<webServiceCommon>
  <!-- passphrase for ManagerService and or Model Manager Web -->
  <SECURITY_PASSPHRASE>passphrase</SECURITY_PASSPHRASE>
  <!-- Website where vCAC virtual applications will be created under -->
  <WEBSITE_NAME>Default Web Site</WEBSITE_NAME>
  <!-- If HTTPS_FLAG is true then specify https port here -->
  <HTTPS_PORT>443</HTTPS_PORT>
  <!-- Certificate string can be its friendly name or its thumbprint. Leave it empty to use self-signed certificate -->
  <CERTIFICATE/> <SUPPRESS_CERTIFICATE_MISMATCH_FLAG/>
  <!-- Service user in domain\user format. This service user is used to run Manager Service, Website, ReportWebsite and Model Manager Web services -->
  <SERVICE_USER>domain\user</SERVICE_USER>
  <!-- Service user password -->
  <SERVICE_USER_PASSWORD>password</SERVICE_USER_PASSWORD>
  <!-- Model manager web hostname. FQDN is required if Https is used -->
  <MODEL_MANAGER_WEB_HOSTNAME>FQDN</MODEL_MANAGER_WEB_HOSTNAME>
  <!-- Set to true to create AzMan store in Msql. Value: true or false. Not in effect if AzMan store is already created -->
  <CREATE_MSSQL_AZMAN_STORE_FLAG>true</CREATE_MSSQL_AZMAN_STORE_FLAG>
  <!-- AzMan store type. Value: MSSQL, XML (file based), or AD -->
```
<AZMAN_STORE_TYPE>MSSQL</AZMAN_STORE_TYPE>

<!-- Leave it empty if XML or MSSQL. Connection string is required if AzMan store type is AD -->

<AZMAN_CONNECTION_STRING/> </webServiceCommon> -<database>

<!-- Leave it empty to use Mssql default data path. If custom data path is used it must exist first -->

<DATABASE_DATA_PATH/>

<!-- Leave it empty to use Mssql default log path. If custom log path is used it must exist first -->

<DATABASE_LOG_PATH/>

<!-- Set to true to use Windows Identity of the Windows account that runs the configuration tool to perform database operation (database creation, schema creation, Model Manager Data deployment. -->

<!-- If set to true the Windows account must already exist under Security Logon of the Sql server with 'sysadmin' privilege -->

<!-- Set to false to use Sql authentication -->

<WINDOWS_AUTHEN_DATABASE_INSTALL_FLAG>true</WINDOWS_AUTHEN_DATABASE_INSTALL_FLAG>

<!-- Sql user to perform database operation if WINDOWS_AUTHEN_DATABASE_INSTALL_FLAG is set to false -->

<!-- Note: Sql authentication is not supported if AZMAN_STORE_TYPE is MSSQL -->

<DATABASE_INSTALL_SQL_USER/>

<!-- Sql user password -->

<DATABASE_INSTALL_SQL_USER_PASSWORD/>

<!-- Set to true if you wish to use an existing empty vCAC database. Value: true or false -->

<!-- The existing vCAC database must not have any vCAC schema created -->

<preCREATED_DATABASE_FLAG>false</preCREATED_DATABASE_FLAG>

<!-- Set to true to create AzMan store in Msql. Value: true or false. Not in effect if AzMan store is already created -->

<CREATE_MSSQL_AZMAN_STORE_FLAG>true</CREATE_MSSQL_AZMAN_STORE_FLAG> </database> -

<managerService>

<!-- Manager service hostname. Use FQDN if https -->

<!-- Set to true to set service to auto and start once configuration is completed. Value: true or false -->

<MANAGER_SERVICE_SERVICESTART_FLAG>true</MANAGER_SERVICE_SERVICESTART_FLAG>

<!-- Set to false during HA setup so that Manager service Windows service will be set to manual -->

<MANAGER_SERVICE_SERVICESTANDBY_FLAG>false</MANAGER_SERVICE_SERVICESTANDBY_FLAG>

<!-- Multiple license keys can be entered, separated by semicolon (;). It's required during Model manager data deployment -->

<LICENSE_KEYS/>

<!-- Model manager web hostname -->

<MODEL_MANAGER_WEB_HOSTNAME>FQDN</MODEL_MANAGER_WEB_HOSTNAME>

<!-- If HTTPS_FLAG is true then specify https port here -->

<HTTPS_PORT>443</HTTPS_PORT>

<!-- AzMan store type. Value: MSSQL, XML (file based), or AD -->

<AZMAN_STORE_TYPE>MSSQL</AZMAN_STORE_TYPE>

<!-- Leave it empty if XML or MSSQL. Connection string is required if AzMan store type is AD -->

<AZMAN_CONNECTION_STRING/>

<!-- Value: true or false -->

<SMTP_ENABLE_SSL_FLAG>False</SMTP_ENABLE_SSL_FLAG>

<!-- Hostname of the vcAC website. Do not use localhost string in a distributed setup -->

<SMTP_WEBSITE_CONSOLE_HOSTNAME/>

<!-- Smtp server -->

<SMTP_SERVER/>

<!-- Smtp from address -->

<SMTP_FROM_ADDRESS/>

<!-- Set to true to use anonymous smtp. If set to false then smtp user and smtp user password are required -->

<SMTP_ANONYMOUS_AUTHEN_FLAG>True</SMTP_ANONYMOUS_AUTHEN_FLAG>

<!-- Specify smtp user if SMTP_ANONYMOUS_AUTHEN_FLAG is set to false -->

<SMTP_USER/>

<!-- Specify smtp user password if SMTP_ANONYMOUS_AUTHEN_FLAG is set to false -->

<SMTP_PASSWORD/>
<SMTP_USER_PASSWORD/> </modelManagerData> </website>

<!-- Set to true if session state database is used to store user session in a distributed environment. Value: true or false -->

<!-- We recommend users to use sticky-session under the Load Balancer over the use of session state database -->

<!-- If sticky session is used under the LB then set WEBSITE_WEBFARM_FLAG to false -->

<WEBSITE_WEBFARM_FLAG>false</WEBSITE_WEBFARM_FLAG>

<!-- Specify an existing ASPState database. User must create it first -->

<WEBSITE_SESSION_STATE_DATABASE_NAME>ASPState</WEBSITE_SESSION_STATE_DATABASE_NAME>
</website> </vCACProperties>

Installation Troubleshooting

When you execute the Setup.exe file, a log file is generated on the system drive. The path is %SystemDrive%\VMware\VCAC\Server\ConfigTool\Log\VCACConfiguration-date.log, where date indicates the date and time. If you have problems during installation you can consult this log and provide it to VMware support for assistance.

Installation of Model Manager Data Fails

The Model Management Web Service and Model Manager Data should always be configured immediately after creating the vCAC database.

Problem

Installation of the Model Manager Data component fails when configuring the Model Manager components.

Cause

Environmental factors can cause the installation of Model Manager Data to fail, including network problems that cause the operation to time out. Consult the configuration tool log at %SystemDrive%\VMware\VCAC\Server\ConfigTool\Log\VCACConfiguration-date.log to determine the cause.

Solution

1. Uninstall all features.
   a. Log on as a user with administrative privileges to the vCAC host machine.
   b. Click Start > Control Panel > Programs and Features.
   c. Uninstall each feature.
2. In SQL Server, delete the vCAC database that you just created.
3. Verify that all prerequisites were checked and the proper credentials are used.
6. Re-create the vCAC database.
7. Reinstall vCAC components by using Setup.exe.

**Error Starting Administration Portal Website**

The Administration Portal Website fails to load due to an error in IIS.

**Problem**

You see the following error when starting the Administration Portal Website:

```
Could not load type 'System.ServiceModel.Activation.HttpModule' from assembly 'System.ServiceModel, Version=3.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089'.
```

You see the following error in the installation log file:

```
Integrated has a bad module ManagedPipelineHandlee in its module list
Managed handler is used; however, ASP.NET is not installed or is not installed completely
Install ASP.NET if you are using managed handler.
```

**Cause**

There is a conflict between the Microsoft WCF HTTP Activation Feature and ASP.NET 4.5.

**Solution**

Run the following commands to reinstall ASP.NET 4.5:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -iru
IISReset
```


**Post-Installation Configuration**

This section describes additional configuration that may be necessary after installation.

**Specifying a Different SMTP Port**

If the SMTP server you specified during installation is not on port 25 (for example, if you use SMTP over SSL), you need to configure vCAC to use the correct port.

To change the SMTP port:

1. Log into the vCAC Console as a vCAC Administrator.
2. Click **vCAC Administrator > Global Properties**.
3. Update the value of the **SMTP Port** property.
   a. Click the pencil icon next to the name of the property.
   b. Specify the SMTP port on the server specified in the **SMTP Server** property.
   c. Click the **Save** button.
4. Restart the vCloud Automation Center service.

**Installing in High Availability Mode**

vCAC can be installed and configured in high availability (HA) mode, in which clustered instances of the vCAC Server provide a failover capability.

In this high availability configuration, components are deployed in the following manner:

- The Manager Service is installed on two hosts behind a load balancer: the primary vCAC Server and a failover vCAC Server to be activated in the event of a failure on the primary.
- A failover instance of the DEM Orchestrator is installed on a different host from the primary Orchestrator and redundant DEM Worker instances are installed.
- Web components are installed on multiple hosts behind a load balancer.

**Note:** Installing the vCAC Web components and Manager Service on the same machine is not supported in a high availability configuration. If you have a use case that requires such a configuration, contact VMware support.

**About Installing the Failover vCAC Server**

Installing the failover vCAC Server follows the same procedure as installing the primary vCAC Server with the following differences:

- On the Server Configuration page:
  a. Clear the check box for **Active node with startup type set to automatic** and select **Disaster Recovery cold standby node**.
  b. Type the Manager Service credentials you provided when installing the primary server.

**Note:** Any changes made to the `ManagerService.exe.config` file after installation must be made to the files on both the failover and the primary vCAC servers.

When using multiple vCAC instances for high availability, install identical sets of identically configured agents on each vCAC server. For information about installing vCAC Agents, see Chapter 4.

**About Installing Redundant Distributed Execution Managers**

Exactly one DEM Orchestrator instance is designated as the active Orchestrator. VMware strongly recommends that you install at least one additional Orchestrator instance on a separate machine for failover in the event that there is an issue with the machine on which the DEM Orchestrator is running or the Orchestrator loses its connection to the Model Manager. If a DEM Orchestrator is not the currently active Orchestrator, it monitors the active Orchestrator’s status so that it can take over as the active Orchestrator should the currently active Orchestrator go offline.

If you have any workflows that require prerequisites for the DEM Worker instance that need to execute them, ensure that you have more than one Worker that is capable of executing any given workflow for redundancy.
About Installing Redundant Web Servers

VMware recommends that you install redundant Web servers behind a load balancer with session affinity (sticky sessions). If you do not want to enable session affinity on your load balancer, you can install the Web components in Web farm configuration, which uses a session state database to track session information across requests. For information about using a session state database, see "Installing vCAC in Web Farm Configuration," on page 48.

When installing additional Web servers:

- Do not select Model Manager Data. This component should only be installed on one server in your deployment.

- If you are using a SQL-based authorization store, do not select Create MSSQL AzMan authorization store on the AzMan Authorization Store Type page; the store was created when you installed the first Web server with the Model Manager Data component.

- To prevent a lookback from occurring when the website queries the local repository through the load balancer, users should configure the Website to look for the repository by using the fully qualified domain name of the local machine.

Failing Over to the Failover vCAC Server

In the event of a system failure on the Manager Service host, follow these steps to fail over to the secondary server:

1. If the primary vCAC Server is still running:
   b. Stop any vCloud Automation Center Agent services, then stop all VMware DEM services and vCloud Automation Center services.
   c. Change the Startup Type of the vCloud Automation Center service from Automatic to Manual.

   **Note:** If the primary server is not running, be sure to change the vCloud Automation Center service to manual startup once it is back up.

2. Deactivate the primary server on the load balancer.
3. Activate the failover vCAC Server on the load balancer.
4. On the failover server, select Start, right-click Command Prompt and select Run as administrator. In the command window, issue the command iisreset.
5. Restart the vCAC services on the failover server.
   b. Start the vCloud Automation Center service, the Distributed Execution Manager services and any vCloud Automation Center Agent services (see Chapter 4).
   c. Change the Startup Type of the vCloud Automation Center service from Manual to Automatic.
Installing vCAC in Web Farm Configuration

The Enable Web farm support option in the vCAC installer enables the vCAC Web servers to use a shared session state database. In this configuration, the session state database is used to track session information regardless of load balancer settings for session affinity. For performance reasons, VMware recommends that you use a load balancer with session affinity to manage sessions across Web servers instead of deploying a session state database.

If you want to use a database to track Web server sessions, the high-level process is:

4. Install the Web components in a Web farm configuration by selecting Web Farm Support on the vCAC Web Site Configuration page. See "Installing vCAC Web Components" on page 27.
5. Install the Manager Service. See "Installing the Manager Service (vCAC Server)" on page 31.
6. Install the Distributed Execution Managers. See "Installing the Distributed Execution Managers" on page 35.

Note: For successful operation of vCAC, the Web site machine key must be the same across all Web servers in a Web server cluster. See http://msdn.microsoft.com/en-us/library/ff649308.aspx.

Creating the Session State Database

You can use a SQL Server database to store ASP.NET session state across the Web servers in the cluster throughout a user visit. This database should be created in the SQL Server instance containing the vCAC database before the Web components of a Web farm configuration are installed.

Note: For performance reasons, VMware recommends that you use a load balancer with session affinity to track user sessions instead of a session state database.

Prerequisites

- Download the vCloud Automation Center installation package.

To create a session state database for use with vCAC:

1. Open a command prompt.
2. Create the session state database using the `aspnet_regsql.exe` command, for example:

   `aspnet_regsql.exe -S databaseinstance -E -ssadd -sstype p -d databasename`

   where `databaseinstance` is either `localhost` or the database server and instance name in the format `server\instance` and `databasename` is the name of the session state database, which is optional. The default name for the database if you omit the `-d` argument is `ASPState`.

   For more information about the ASP.NET SQL Server Registration Tool (`aspnet_regsql.exe`), see the Microsoft documentation: http://msdn.microsoft.com/en-us/library/ms229862(v=vs.80).aspx.
3. If the user under which the Manager Service will run is not the owner of the session state database, you must run a script to grant that user access to the session state database.

   a. Navigate to the directory where you extracted the installation zip archive, then navigate to the **Database** subdirectory.

   b. Extract the **DBInstall.zip** archive to a local directory.

   c. Edit **GrantAspSessionStateUserPermission.sql** and replace all instances of **$(ServiceUser)** in the script with the user name under which the vCloud Automation Center service (Manager Service) will run. (For information about Manager Service credentials, see "Users and Credentials Required for vCAC Services"). Do not replace **ServiceUser** in the line ending with **WHERE name = N'ServiceUser'**.

   d. Open SQL Server Management Studio.

   e. Select the session state database under **Databases** in the left-hand pane.

   f. Click **New Query**.

      A SQL Query window opens in the right-hand pane.

   g. Paste the entire modified contents of **GrantAspSessionStateUserPermission.sql** into the query window.

   h. Click **Execute**.
Chapter 4 Integrating with Provisioning Resources

vCAC uses two primary mechanisms to communicate with external systems, such as provisioning resources, and the machines that it manages: Distributed Execution Managers (specifically, DEM Workers), and various Agents. Both DEM Workers and Agents may have specific requirements depending on the system with which it is intended to integrate.

DEM Worker Overview

DEM Workers manage cloud, physical, and some virtual machines depending on the hypervisor management platform. This information describes requirements for specific provisioning platforms. If not all DEM Workers in your vCAC instance satisfy the requirements for a specific provisioning type, you can use skills to restrict specific workflows to DEM instances that satisfy the requirements. For details about working with skills, see the vCloud Automation Center Operating Guide.

For information about general DEM prerequisites, see “Preparing for vCAC Installation” on page 5. For information about installing DEM Workers, see Chapter 3.

Amazon EC2 Requirements

vCAC communicates with and collects data from an Amazon EC2 account using the Internet. Therefore, if you intend to use Amazon EC2 provisioning for cloud machines, there are two DEM-related requirements:

- Hosts on which DEMs are installed must have access to the Internet; if there is a firewall, HTTPS traffic must be allowed to and from aws.amazon.com, as well as the URLs representing all the EC2 regions your AWS accounts have access to, for example ec2.us-east-1.amazonaws.com for the US East region. Each URL resolves to a range of IP addresses, so you may need to use a tool such as the one available at http://www.networksolutions.com/whois to list and configure these IP addresses.

- If Internet access from the DEM host is through a proxy server, the DEM service must be running under credentials that can authenticate to the proxy server. For information about connecting to Amazon Web Services through a proxy server, see the vCloud Automation Center Operating Guide.

KVM (RHEV) Requirements

For information about KVM requirements, see the vCloud Automation Center KVM (RHEV) Integration Guide.

SCVMM Requirements

Any DEM Worker used to manage virtual machines through SCVMM must be installed on a host on which the SCVMM Console is installed. In addition:

- The DEM must have access to the SCVMM PowerShell module installed with the console.

- The MS PowerShell Execution Policy must be set to “RemoteSigned” or “Unrestricted.”
For information on PowerShell Execution Policy issue one of the following commands at Power-Shell command prompt:

```
help about_signing
help Set-ExecutionPolicy
```

- If all DEM Workers within the vCAC instance are not on compute resources meeting these requirements, Skills must be used to direct all SCVMM-related workflows to those that are. For information about using skills to associate workflows with DEM instances, see the vCloud Automation Center Extensibility Guide.

The following additional requirements apply to SCVMM:

- Each SCVMM instance must be joined to the domain containing the vCAC server.
- The credentials used to manage the endpoint representing an SCVMM instance must have Administrator privileges on the SCVMM server. These credentials must also have Administrator privileges on the Hyper-V servers within the instance.
- Hyper-V servers within an SCVMM instance to be managed by vCAC must be Windows 2008 Servers with Hyper-V installed. The processor must be equipped with the necessary virtualization extensions. .NET Framework 4.5 must be installed and Windows Management Instrumentation (WMI) must be enabled.
- To provision machines on an SCVMM compute resource, a user must be added in at least one security role within the SCVMM instance, for example the Self-Service role.

## Configuring the DEM to Connect to SCVMM on a Nonstandard Installation Path

By default the DEM Worker configuration file (`DynamicOps.DEM.exe.config`) points to the standard installation path of the SCVMM Console: `{ProgramFiles}\Microsoft System Center 2012\Virtual Machine Manager\bin`.

If the SCVMM Console has been installed in another location, the configuration file of the DEM Worker (located in `%SystemDrive%\Program Files (x86)\VMware\vCAC\Distributed Execution Manager\<InstanceName>\DynamicOps.DEM.exe.config) must be updated to change the default path in the `assemblyLoadConfiguration` section to point to the new folder:

```
<assemblyLoadConfiguration>
<assemblies>

<!-- List of required assemblies for Scvmm -->

<add name="Errors" path="{ProgramFiles}\Microsoft System Center 2012\Virtual Machine Manager\bin" />

[...] 
</assemblies>
</assemblyLoadConfiguration>
```

After updating the DEM configuration file, restart the DEM to apply the changes.
Virtual Provisioning on SCVMM

When setting up a virtual machine template in SCVMM, a Guest OS Profile can be added directly to a Windows template using SCVMM Console. See “Preparing for Virtual Provisioning by Cloning” in the vCloud Automation Center Operating Guide for more information on Windows and Linux template configuration.

Some restrictions apply to SCVMM template and hardware profile names. Specifically, these names cannot start with the following words:

- TemporaryTemplate
- Temporary Template
- TemporaryProfile
- Temporary Profile
- Profile

Because of naming conventions that SCVMM and VMware use for temporary templates and hardware profiles, these words are ignored during data collection.

A compute resource running under SCVMM can have multiple paths in the placement section that are collected and exposed to be assigned in a reservation.

On a Hyper-V cluster under SCVMM management, data collection is for Shared Volumes only since a work load can only be provisioned on a shared resource of a cluster.

- View the SCVMM Console, then right-click your Hyper-V cluster to select properties. Browse to the Shared Volumes section to view the storage properties.

When running data collection on Standalone hosts for storage used in the reservation, vCAC collects the default virtual machine paths. This can be configured through SCVMM Console under the Placement section.

- View the SCVMM Console, then right-click your Hyper-V standalone host to select properties. Browse to the Placement section to view the storage properties.

vCAC Agent Overview

vCAC server relies on four types of agents:

- Hypervisor proxy agents
- Windows Management Instrumentation (WMI) agents
- Virtual desktop infrastructure (VDI) integration agents
- External provisioning infrastructure (EPI) integration agents

These agents are all installed using the same procedure, as described later in this chapter.
Planning Your vCAC Proxy Agents

The vCAC Server uses proxy agents to communicate with virtualization platforms such as vCenter Server instances, Citrix XenServers, and Microsoft Hyper-V servers, to discover available work, fetch host information, and report completed work items and host status changes.

Once a vCAC server proxy agent is managing a virtualization host, the vCAC Server can collect data about that host, including its characteristics, the physical memory and storage it provides, and the amount of these resources that are in use, and any unmanaged virtual machines (provisioned outside vCAC server) that exist on the host.

A single instance of vCAC server can support multiple XenServers, Hyper-V servers and vCenter Server instances. The proxy agent that manages each host must have certain privileges on it. Therefore the number of proxy agents you install depends on the number needed to ensure that at least one will have the required access to each of the hosts you want to add to vCAC server. On this basis, one uniquely named proxy agent must be installed for:

- Each vSphere endpoint representing all discoverable ESX Servers within a single vCenter Server instance
- Each set of credentials used by the agent to access one or more XenServers
- Each set of credentials used by the agent to access one or more Hyper-V servers

You may want to fully prepare the credentials the agents will need before installing the agents. For vSphere agents, you need to create a vSphere endpoint containing these credentials as well as installing the agent. For Xen and Hyper-V agents, you need to install enough agents to cover all of the required credentials. For example, if you add half of your Hyper-V hosts to one domain and half to another, and within each domain prepare a set of administrator-level credentials for the proxy agents to use, you will need to install two Hyper-V agents—one for each domain. You will also need to collect the configuration information for each agent—the entities to be managed and the credentials required to manage them—before installing the agents. For these reasons, you will likely find it very helpful to prepare ahead of time a plan of the agents you need including the instances and hosts to be managed and the credentials to be used. An example is shown in the following table.

Table 15   Proxy Agent Installation Table

<table>
<thead>
<tr>
<th>vCAC Server</th>
<th>Agent Type</th>
<th>Agent Name</th>
<th>Service Username</th>
<th>vCenter Server URL or Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcac-1</td>
<td>vSphere</td>
<td>vsphere20</td>
<td>vc20</td>
<td><a href="https://vsphere-20/sdk">https://vsphere-20/sdk</a></td>
</tr>
<tr>
<td></td>
<td>vSphere</td>
<td>vsphere27</td>
<td>vc27</td>
<td><a href="https://vsphere-27/sdk">https://vsphere-27/sdk</a></td>
</tr>
<tr>
<td>vcac-2</td>
<td>Hyper-V</td>
<td>hv1</td>
<td>hv1</td>
<td>hv-217 through hv-225</td>
</tr>
<tr>
<td></td>
<td>Xen</td>
<td>xen1</td>
<td>xen1</td>
<td>xen-11, xen-17, xen-25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>xen2</td>
<td>xen2</td>
<td>xen-14, xen-19, xen-20-22</td>
</tr>
</tbody>
</table>

Note: If you installed clustered instances of vCAC for high availability, as described in Chapter 3, install identical sets of agents on the primary and failover vCAC servers.
Configuring Proxy Agents

The way in which a proxy agent is configured for the virtualization hosts it manages depends on the type of host involved.

- A vSphere proxy agent is configured when installed for a vSphere endpoint specifying the location of the vCenter Server instance it is to manage and the credentials it will use to do so. The endpoint, which is created using the vCAC Administrator > Endpoints activity in the vCAC console (as described in the vCloud Automation Center Operating Guide) must exist and contain valid information before the agent is installed (or at least before the agent service is started). Use your agent list to create the needed endpoints and then install the corresponding vSphere agents.

- A Xen or Hyper-V proxy agent is installed with only the credentials used to gain access to the hosts it will manage and not the names of the host themselves. For this reason, each Xen and Hyper-V agent must be configured for each XenServer or Hyper-V host it is to manage. This is done using the vCAC Administrator > Agent Configuration activity in the vCAC console, as described in the vCloud Automation Center Operating Guide, and can be done after the agent is installed and running. Once a host is configured using this function and placed in an enterprise group, data collection begins automatically. Use your agent list to install the needed Xen and Hyper-V agents and then configure the agents for the corresponding hosts.

Enabling Remote WMI Requests on Windows Machines

A Windows Management Instrumentation (WMI) agent is required to collect certain data from a Windows machine managed by vCAC, for example the Active Directory status of a machine’s vCAC owner. To ensure successful management of Windows machines, you must enable all WMI agents to collect data from Windows machines.

To enable the WMI agent to collect this data from Windows machines:

1. In each domain to which Windows virtual machines provisioned and managed by vCAC may be joined, create an Active Directory group and add to it the service credentials of the WMI agents that may need to execute remote WMI requests on the provisioned machines.

2. Enable remote WMI requests for the Active Directory group(s) containing the agent credentials on each Windows machine provisioned. Procedures for this are discussed in Chapter 2 of the vCloud Automation Center Operating Guide.

Virtual Desktop Integration

vCAC uses virtual desktop integration (VDI) PowerShell agents to register the machines it provisions with external desktop management systems and to communicate with those systems. The VDI integration agent currently supports registration of machines with XenDesktop and provides the owners of registered machines with a direct connection to XenDesktop Web Interface from the vCAC Console. A VDI agent can be installed as a dedicated agent to interact with a single Desktop Delivery Controller or as a general agent that can interact with multiple DDCs. You can combine dedicated and general agents as needed given your particular configuration, throughput, availability and load balancing considerations.
External Provisioning Integration

External provisioning integration (EPI) PowerShell agents allow vCAC to integrate external provisioning technologies into its machine provisioning process. The EPI integration agent currently supports integration of vCAC with Citrix Provisioning Server, which provides on-demand streaming of the disk images from which machines boot and run.

An EPI agent can be installed as a dedicated agent to interact with a single external provisioning server or as a general agent that can interact with multiple external provisioning servers of the same type. (Only the former configuration is supported for Citrix Provisioning Server.) You can combine dedicated and general agents as needed given your particular configuration, throughput, availability and load balancing considerations.

Using Visual Basic Scripts in Provisioning

vCAC allows you to specify Visual Basic (VB) scripts to be run outside vCAC as additional steps in the provisioning process, before or after provisioning a machine. You can also run a script when unprovisioning (destroying) a machine. The desired script(s) are specified in the blueprint from which machines will be provisioned. Such scripts have access to all the custom properties associated with the machine and can even update their values; the next step in the workflow then has access to these new values. For example, you could use a script to generate certificates or security tokens before provisioning and then use them in provisioning the machine. (See the vCloud Automation Center Operating Guide for information about custom properties.)

To enable VB scripts in provisioning, you must install a specific type of EPI agent and place the scripts you want to use on the system on which the agent is installed.

When executing a VB script, the EPI agent passes all machine custom properties as arguments to the script. To return updated property values to vCAC, you must place these properties in a dictionary and call a function provided by vCAC.

A sample VB script that you can use as a template is included in the scripts subdirectory of the EPI agent installation directory. This script contains a header to load all arguments into a dictionary, a body in which you can include your function(s) and a footer to return updated custom properties values to vCAC.

See the vCloud Automation Center Operating Guide for more information about adding VB scripts to the provisioning process.

Note: You can install multiple EPI/VBScripts agents on multiple servers and provision using a specific agent and the Visual Basic scripts on that agent’s host, but not using the vCAC agent installer and the provisioning procedures described in the vCloud Automation Center Operating Guide. If you have a need for this capability, contact VMware customer support.
**vCAC Agent Relationships**

vCAC agents and their relationships to vCAC, virtualization platforms, and other external systems are shown in the following diagram. Each blue double arrow in the diagram represents a proxy agent; for example, the arrow labeled hvC represents the proxy agent communicating with Hyper-V servers C1 and C2, both accessed using credentials C.

The diagram also shows VDI and EPI agents (in green) and the servers with which they interact. The WMI agent is not shown. Cloud and physical provisioning infrastructure are also not shown in this diagram.

**Figure 2** vCAC Agents for vCenter Server, XenServer and Hyper-V Plus VDI and EPI

---

**Note:** vCAC does not support multiple machines with the same name within a single vCenter Server instance, XenServer or Hyper-V server. This can occur if a single instance or provisioning host is being managed by multiple instances of vCAC through multiple agents, as each instance will validate new names only against the names of machines it is managing, not against names of those managed by other instances. You can prevent this problem by customizing each instance of vCAC to validate machine names against DNS and/or Active Directory; see Chapter 5 of the *vCloud Automation Center Operating Guide* for more information.
vCAC Agent Installation Location and Requirements

vCAC agents are typically installed on the same host as the vCAC server they communicate with (with the exception of EPI agents interacting with Citrix Provisioning Server 5.1, as described below). If an agent is installed on another host, the network configuration must be such that the agent can communicate with the vCAC server host.


Each agent is installed under a unique name in its own directory, Agents\agentname, under the vCAC install directory (typically %SystemDrive%\Program Files (x86)\VMware\vCAC), with its configuration stored in the file VRMAgent.exe.config in that directory.

Hypervisor Proxy Agent Installation Requirements

Hypervisor proxy agent installation requires that you provide the following:

- Credentials under which to run the agent service; these must have administrative access to the installation host (typically the vCAC server host).
- If a Xen agent or Hyper-V agent, one set of administrator-level credentials for all XenServer or Hyper-V instances on the hosts to be managed by the agent.

Note: By default, Hyper-V is not configured for remote management. A vCAC Hyper-V proxy agent cannot communicate with a Hyper-V server unless remote management has been enabled. To configure Hyper-V for remote management, see http://technet.microsoft.com/en-us/library/cc794756.aspx or other Microsoft documentation.

- If a vSphere agent, the URL of the vCenter Server instance and credentials for the instance, which must have permission to modify custom attributes.

In some cases, the use of an administrator-level account for this purpose may conflict with established policy or practice. The following table shows the detailed permissions the vSphere agent account must have to enable the agent to manage a vCenter Server instance for vCAC.

Note: When creating the endpoint representing the vCenter Server instance to be managed by a vSphere agent, you can choose to have the agent use the credentials the service is running under to interact with vCenter Server. See "Preparing Endpoints for vSphere Agents" for more information.

Be sure to disable or reconfigure any third-party software that might automatically change the power state of virtual machines outside of vCAC. Such changes can interfere with vCAC's management of the machine's lifecycle and cause errors.
<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>VirtualCenter 2.5</th>
<th>vCenter Server 4.0/4.1/5.0/5.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Manage Custom Attributes</td>
<td>Manage Custom Attributes</td>
</tr>
<tr>
<td></td>
<td>Set Custom Attribute</td>
<td>Set Custom Attribute</td>
</tr>
<tr>
<td>Folder</td>
<td>Create Folder</td>
<td>Create Folder</td>
</tr>
<tr>
<td></td>
<td>Delete Folder</td>
<td>Delete Folder</td>
</tr>
<tr>
<td>Datastore</td>
<td>Browse Datastore</td>
<td>Browse Datastore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Allocate Space</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Inventory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td>Create from existing</td>
</tr>
<tr>
<td></td>
<td>Move</td>
<td>Create New</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Move</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remove</td>
</tr>
<tr>
<td></td>
<td>Interaction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power On</td>
<td>Power On</td>
</tr>
<tr>
<td></td>
<td>Power Off</td>
<td>Power Off</td>
</tr>
<tr>
<td></td>
<td>Suspend</td>
<td>Suspend</td>
</tr>
<tr>
<td></td>
<td>Reset</td>
<td>Reset</td>
</tr>
<tr>
<td></td>
<td>Device Connection</td>
<td>Device Connection</td>
</tr>
<tr>
<td></td>
<td>Configure CD Media</td>
<td>Configure CD Media</td>
</tr>
<tr>
<td></td>
<td>Tools Install</td>
<td>Tools Install</td>
</tr>
</tbody>
</table>
WMI Agent Installation Requirements

Typically, one WMI agent is installed for each vCAC instance. WMI agent installation requires that you provide credentials with administrative access to the installation host (typically the vCAC server host).

The credentials under which you install the WMI agent must also have the right to execute remote WMI requests on Windows machines managed by vCAC. See "Enabling Remote WMI Requests on Windows Machines", earlier in this chapter, for more information.
VDI Integration Agent Installation Requirements

The following requirements apply to VDI Agents:

- XenDesktop DDC servers to be integrated with vCAC must be running XenDesktop 4 or later. When installing a VDI agent for XenDesktop you must choose whether to install for XenDesktop 4 or XenDesktop 5; see "Installing a vCAC Agent".

  **Note:** A XenDesktop 4 VDI agent cannot be installed on a 64-bit host, such as a Windows Server 2008 R2 system. If the vCAC server is a 64-bit host, install any XenDesktop 4 VDI agents on other hosts in an appropriate network configuration.

- The credentials under which the agent will run must have administrative access to all XenDesktop DDC servers with which it will interact.

- A general VDI agent can interact with multiple servers. If installing one dedicated agent per server for load balancing or authorization reasons, you must provide the name of the XenDesktop DDC server when installing the agent. A dedicated agent can handle only registration requests directed to the server specified in its configuration.

- The following software must be installed on the installation host prior to agent installation:
  - **Microsoft PowerShell.** The version required depends on the installation host's operating system and may have been installed with that operating system. Visit [http://support.microsoft.com](http://support.microsoft.com) for more information.
  - **Citrix XenDesktop SDK.** The version depends on which version of XenDesktop you have installed. The SDK for XenDesktop 5 or 5.5 is included on the XenDesktop installation disc. For XenDesktop 4, version 2.1.2327 is required; you can download this software from these locations:
    - [http://support.citrix.com/article/CTX118973](http://support.citrix.com/article/CTX118973)
    - [http://support.citrix.com/servlet/KbServlet/download/18540-102-19308/XdsControllerSDK-2_1_2327-E.zip](http://support.citrix.com/servlet/KbServlet/download/18540-102-19308/XdsControllerSDK-2_1_2327-E.zip)
  - MS PowerShell Execution Policy must be set to "RemoteSigned" or "Unrestricted."

    For information on PowerShell Execution Policy issue one of the following commands at PowerShell command prompt:
    ```
    help about_signing
    help Set-ExecutionPolicy
    ```

    - In XenDesktop 5.x, the name given to the XenServer Host on your XenDesktop 5.x server must match the UUID of the Xen Pool in XenCenter. If no XenPool is configured, it must match the UUID of the XenServer itself.
      a. In Citrix XenCenter, select your XenPool or standalone XenServer and click the **General** tab. Record the UUID.
      b. When adding your XenServer Pool or standalone host to XenDesktop, type the UUID that was recorded in the previous step for the **Connection name**.
Each XenDesktop 5 DDC server with which you intend to register machines must be configured as follows:

- The group/catalog type must be **Existing** for use with vCAC.
- The name of a vCenter Server host on a DDC server must match the name of the vCenter Server instance as entered in the vCAC vSphere endpoint, **without** the domain. For example, if the address in the endpoint is **https://virtual-center27.domain/sdk** , the host’s name on the DDC server must be set to **virtual-center27**.
- If XenDesktop will be used with Citrix Provisioning Server, PVS 5.6 or higher must be in use.

Each XenDesktop 4 DDC server with which you intend to register machines must be configured as follows:

- The group type must be **Assigned > Pre-Assigned** for use with vCAC.
- Citrix MFCOM can be registered for each DDC server. This is not typically required but you may want to forestall errors during XenDesktop registration of provisioned machines by using the following procedure. Details are available at [http://support.citrix.com/article/CTX120649](http://support.citrix.com/article/CTX120649).
  a. Log into the host as a user with administrative access. Open a command window and change to the directory **C:\Program files\Citrix\Desktop Delivery Controller\PowerShell**.
  b. Type:

        mfreq.exe DDC_server_name

    where DDC_server_name is the fully-qualified hostname of each XenDesktop DDC server with which you intend to register machines.

**EPI Agent Installation Requirements**

EPI agents can be used to integrate vCAC with Citrix Provisioning Server and to enable the use of Visual Basic scripts in the provisioning process.

**EPI Agent for Citrix Provisioning Server Installation Requirements**

The following requirements apply to installing an EPI agent to interact with Citrix Provisioning Server:

- For Citrix Provisioning Services (PVS) 5.1 instances, the EPI agent must be installed on the PVS host. For PVS 5.6 instances, the EPI agent can be installed on the same host or a remote host.
- You must apply one of the following hot patches to Citrix Provisioning Services.
  For PVS 5.1, see:
  - [http://support.citrix.com/article/CTX125103](http://support.citrix.com/article/CTX125103)
  For PVS 5.6, see:
  - [http://support.citrix.com/article/CTX128245](http://support.citrix.com/article/CTX128245)
• Although an EPI agent can generally interact with multiple servers, Citrix Provisioning Server requires a dedicated EPI agent. You must install one EPI agent for each Citrix Provisioning Server instance, providing the name of the server hosting it. The credentials under which the agent will run must have administrative access to the Citrix Provisioning Server instance.

• On a XenDesktop 5 DDC server, Citrix PVS 5.6 or higher must be installed and used with XenDesktop.

• The following software must be installed on the installation host prior to agent installation:

  **Citrix Provisioning Services SDK.** The following versions of the SDK must be installed depending on the PVS version installed.

  **Table 17    Citrix Provisioning Services SDK Versions**

<table>
<thead>
<tr>
<th>PVS Version</th>
<th>SDK Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>5.1.0.2933</td>
</tr>
<tr>
<td>5.6</td>
<td>5.6.0.1028</td>
</tr>
<tr>
<td>5.6 SP1</td>
<td>5.6.1.1045</td>
</tr>
<tr>
<td>5.6 SP2</td>
<td>5.6.2.1313</td>
</tr>
<tr>
<td>6.0</td>
<td>6.0.0.1026</td>
</tr>
</tbody>
</table>

**Microsoft PowerShell.** The version required depends on the installation host’s operating system and may have been installed with that operating system. Visit [http://support.microsoft.com](http://support.microsoft.com) for more information.

You must also ensure that the PowerShell Snap-In is installed. The following instructions are quoted from the PowerShell Programmer’s Guide available at [http://support.citrix.com/article/CTX121334](http://support.citrix.com/article/CTX121334):

• The PowerShell snap-in (McliPSSnapIn.dll) can be installed using the Provisioning Server Console install.

• If the snap-in later needs to be registered in PowerShell, this can be manually done by executing the following command at a DOS command prompt, in the directory containing McliPSSnapIn.dll:

  ```bash
  %systemroot%\Microsoft.NET\Framework\v2.0.50727\installutil.exe  \
  McliPSSnapIn.dll
  
  You must be in the Citrix Provisioning Server directory in which the snap-in is located.

• Another way to register the snap-in is by running this command at the PowerShell command prompt:

  ```powershell
  $installutil = $env:systemroot + '\Microsoft.NET\Framework\v2.0.50727\installutil.exe' &$installutil \ McliPSSnapIn.dll
  ```

  **Note:** On a 64-bit installation host, substitute `\Microsoft.Net\Framework64` for `\Microsoft.Net\Framework` in the above commands.

• MS PowerShell Execution Policy must be set to “RemoteSigned” or “Unrestricted.”
For information on PowerShell Execution Policy issue one of the following commands at PowerShell command prompt:

```
help about_signing
help Set-ExecutionPolicy
```

**EPI Agent for Visual Basic Scripting Installation Requirements**

The following requirements apply to installing an EPI agent to enable the use of Visual Basic scripts in the provisioning process:

- The credentials under which the agent will run must have administrative access to the installation host.
- Microsoft PowerShell must be installed on the installation host prior to agent installation: The version required depends on the installation host’s operating system and may have been installed with that operating system. Visit [http://support.microsoft.com](http://support.microsoft.com) for more information.
- MS PowerShell Execution Policy must be set to “RemoteSigned” or “Unrestricted.”

For information on PowerShell Execution Policy issue one of the following commands at PowerShell command prompt:

```
help about_signing
help Set-ExecutionPolicy
```

**Preparing Endpoints for vSphere Agents**

A vSphere agent is configured during installation for an endpoint containing information about the vCenter Server instance it is to manage. Because this endpoint must exist and contain valid information before the agent service is started, you have two options:

- Create all needed endpoints first, using the vCAC console and the instructions provided in Chapter 3 of the *vCloud Automation Center Operating Guide*, then install and start the corresponding vSphere agents.
- Install the needed vSphere agents without starting them, then create the corresponding endpoints, then start the agents.

If you want to create the endpoints before installing agents, you must use the vCAC console in the vCAC administrator role. Start the console (as described in Chapter 3) either as a member of the local Administrators group or as a user who has been given the vCAC administrator role by a member of the group. Details are provided in the *vCloud Automation Center Operating Guide*, but the following is a very brief summary of the procedure for creating a generic endpoint.

1. Select **vCAC Administrator > Endpoints**.
2. Move the pointer over the **New Endpoint** link at the right-hand end of the title bar and choose **vSphere** from the hover menu to display the New Endpoint - vSphere page.
3. Enter the endpoint name (typically this indicates the vCenter Server instance the endpoint is for) and a more detailed description and enter the URL of the vCenter Server instance (for example **https://vsphereA/sdk**),
4. Click the button next to **Credentials** to display the Credentials grid.
5. Click the New Credentials link at the right-hand end of the title bar. Enter credentials for the vCenter Server instance the agent will manage, along with a useful name and a more detailed description. (See "Hypervisor Proxy Agent Installation Requirements" for information about vCenter Server permissions required for vSphere agents.) Alternatively, you can choose to have the vSphere agent interact with vCenter Server using the credentials under which the which the agent service will be running (you provide these during agent installation). To do so, select the predefined credentials Integrated for the endpoint.

   Click the Save button to save the credentials. Select them and click OK to return to the New Endpoint page.

6. Click the Save button.

7. Repeat this procedure for all the needed endpoints.

Installing a vCAC Agent

Prerequisites

- Download the vCloud Automation Center installation package.

To install a vCAC proxy, WMI, VDI or EPI agent:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the Setups subdirectory.
2. Right-click vCAC-Agent-Setup.exe and select Run as administrator.
3. On the Welcome page, click Next.
4. On the End-User License Agreement page, read the License Agreement, click I accept the terms in the License Agreement, then click Next.

   Note: If the vCAC agent installer detects existing vCAC agents installed on the host, it provides you with the option to upgrade those agents to the current version of vCAC. See Chapter 6 for procedures for upgrading vCAC and vCAC agents.

5. On the Agent Name page:
   a. In the Agent name box, provide a unique name for the agent.
   b. In the vCloud Automation Center Hostname:Port box, specify the host name and port of the vCAC Server. The default port is 443.
   c. In the Model Manager Web Service Hostname:Port box, specify the host name and port of the Model Manager server. The default port is 443.

   Note: Maintain a careful record of each proxy agent’s name, the credentials entered for it and the virtualization platform instance it is intended for so that when a Hyper-V or XenServer host is added to the agent configuration the administrator performing the operation has this information readily available.

   Agent names must not be duplicated unless the agent configurations are identical.
6. On the Agent Selection page, select the type of agent you want to install. You can change the default installation location for the agent (%SystemDrive%\Program Files (x86)\VMware\vCAC Agents) by using the Browse button.

Select Test for a test agent that will not interact with any virtualization platform or other entity.

The procedure for configuring the agent differs depending on the agent type.

For a vSphere Agent

- On the Service Configuration page, indicate whether you want to register and start the agent service as part of installation. Both are required for the proxy agent to function, but if you have not prepared a valid endpoint for the agent, do not select Start Agent Service; you must create the endpoint before starting the agent. (Starting the agent if the endpoint does not exist or does not have valid information generates repeated error messages until the service is stopped.)

On the same page, enter the credentials to be used by the agent service. See "Hypervisor Proxy Agent Installation Requirements" for a detailed discussion of permissions required for vSphere agent credentials.

**Note:** If you selected or will select the predefined Integrated credentials for the vSphere endpoint you are going to specify on the vSphere Endpoint Configuration page (see "Preparing Endpoints for vSphere Agents"), the credentials you enter for the agent service must have the permissions listed in "Hypervisor Proxy Agent Installation Requirements" for the vCenter Server instance specified in the endpoint.

Throughout this procedure, when you specify a domain user you must enter the username in domain format, for example ENGINEERING\jsmith.

Do not select Use Local System Account for a vSphere agent.
You can also choose whether to change the location for the agent logs. You may want to do this, for example, to place the log files on a dedicated partition separate from the one hosting the operating system. This prevents the increase in space devoted to log files from affecting the operating system or vCAC. To change from the default location, uncheck **Use Default Log Location** and enter the log file location you want in the **Agent Log Location** box.

- On the vSphere Agent Configuration page, enter the credentials you entered for the Model Manager Web service on the Model Manager Configuration page when installing vCAC. The agent installer validates the combination of Model Manager Web host and service credentials; if they are valid, you can continue with installation. If an error is returned, you must determine the correct combination of repository host and credentials before proceeding.
• On the vSphere Endpoint Configuration page, enter the name of the generic endpoint you prepared containing the URL of the vCenter Server instance and appropriate credentials for the instance.

Remember, if you have not yet created a valid endpoint, you should not start the agent service. Return to the Service Configuration page unselect **Start Agent Service**. After you have created the endpoint you configured for the agent, you can start the agent service by selecting **Start > Administrative Tools > Services** and then starting the vCloud Automation Center Agent – *agentname* service.)

**Note:** The agent installer cannot validate the virtualization platform credentials contained in the endpoint. If this information is entered incorrectly, the agent is not able to log into the instance and the error is recorded in the log file in the agent directory (%SystemDrive%\Program Files (x86)\VMware\vCAC Agents\*agentname*). After you correct the endpoint data, the agent automatically picks up the new credentials.

For a Xen or Hyper-V Agent
On the Agent Configuration page enter credentials that provide administrator-level access to XenServer or Hyper-V on all hosts that will be managed by the agent.

Note: A Hyper-V proxy agent installed on a Hyper-V server will connect to the local instance of Hyper-V using the service credentials it is running under as entered on the Service Configuration page described below, not the credentials entered on the Agent Configuration page.

The agent installer cannot validate the virtualization platform credentials you enter. If the information is entered incorrectly for a Hyper-V or Xen agent, the agent will not discover the intended host when configured for one (see the vCloud Automation Center Operating Guide). See "Modifying Proxy Agent Configurations", below, for instructions for correcting the credentials.

For a VDI PowerShell Agent

- On the Agent Configuration page, select the type of virtual desktop infrastructure (currently locked to XenDesktop) and choose XenDesktop 4 or XenDesktop 5 (see "VDI Integration Agent Installation Requirements" for important information). Then enter the name of a XenDesktop DDC server at the VDI Server prompt or leave the field blank to let the agent interact with multiple servers. The server with which a VDI agent interacts depends on the value of a required custom property in the blueprint from which you provision virtual machines with XenDesktop integration, VDI.Server.Name (see the vCloud Automation Center Operating Guide). Therefore,

  - If you install a dedicated VDI agent by specifying a server name during installation, only machines whose VDI.Server.Name property specifies exactly the same server name as that configured for the agent can be registered with or provisioned by that server.

  - If you install a general VDI agent by not specifying a server name during installation, a machine can be registered with or provisioned by any server specified in its VDI.Server.Name property (assuming the agent can contact that server).
**Note:** A XenDesktop 4 VDI agent cannot be installed on a 64-bit host, such as a Windows Server 2008 R2 system. If the vCAC server is a 64-bit host, install any XenDesktop 4 VDI agents on other hosts in an appropriate network configuration.

The agent installer checks to see whether the Citrix XenDesktop SDK version required for the agent version you selected is installed on the installation host; if it is not, you are alerted and informed of what is required, but the agent installation continues.

**For an EPI PowerShell Agent**

- On the Agent Configuration page, select a type of **CitrixProvisioning** or **VBScripts**. For EPI/CitrixProvisioning, you must specify a server name at the **EPI Server** prompt, as you must install a dedicated EPI agent for each Citrix Provisioning Server instance you want vCAC to interact with. The blueprint you create for provisioning with Citrix Provisioning Server must specify the name of a server for which an EPI/CitrixProvisioning agent is configured in the EPI.Server.Name custom property (see the **vCloud Automation Center Operating Guide**). Do not enter a server name for an EPI/VBScripts agent.

**Note:** To interact with a Citrix Provisioning Server 5.1 instance, an EPI agent must be installed on the CPS host. For PVS 5.6 instances or higher, it can be installed on the same host or a different host.

When you select **CitrixProvisioning**, the agent installer checks to see whether the required Citrix Provisioning SDK version (see "EPI Agent Installation Requirements") is installed on the installation host; if it is not, you are alerted and informed of what is required, but the agent installation continues.

If you install multiple general EPI/VBScripts agents using the vCAC agent installer, the agent is chosen at random when a blueprint calls a Visual Basic script, so you must install the same scripts on the servers hosting all such agents or results will be inconsistent.

For more information on provisioning machines with VDI integration and EPI integration, including installing an EPI agent for provisioning with BMC BladeLogic or HP Software Automation (formerly Opsware SAS), see the **vCloud Automation Center Operating Guide**.

**For a Guest, WMI or Test Agent**

- The installer directly skips to the Service Configuration page.
7. For all agents types except vSphere, the Service Configuration page follows agent configuration.

On this page, indicate whether you want to register and start the agent service as part of installation. Both are required for the proxy agent to function. If you want to delay starting the service for any reason, you can easily start it manually later. (Select Start > Administrative Tools > Services and then start the vCloud Automation Center Agent – agentname service.)

On the same page, enter the credentials to be used by the agent service. As noted, this user must have administrative access to the machine the agent is being installed on. For VDI agents, the user must have administrative access to all VDI servers with which the agent will interact. For EPI/CitrixProvisioning agents, the user must have administrative access to Citrix Provisioning Server on the host it is installed on.

You can select Use Local System Account to run the agent service under the Local System account. If you do, you do not need to enter service credentials.

**Note:** The agent installer cannot validate the agent service credentials you enter. If this information is entered incorrectly or is not valid, installation fails.

A Hyper-V proxy agent installed on a Hyper-V server will connect to the local instance of Hyper-V using the service credentials entered on this page, not the credentials entered previously on the Agent Configuration page. Therefore these credentials must have administrator level access to the local Hyper-V instance as well as to the local host.

As noted in Enabling Remote WMI Requests earlier in this chapter, service credentials for proxy agents and WMI agents must belong to an Active Directory group in each domain to which provisioned virtual machines may be joined. This allows the credentials to be enabled for remote WMI requests on those machines. For this reason, if you choose to run a proxy or WMI agent under the Local System account, the installation host must belong to all such domains and be added to the remote WMI request Active Directory group.
This page allows you to change the location for the agent service logs. You may want to do this, for example, to place the log files on a dedicated partition separate from the one hosting the operating system. This prevents the increase in space devoted to log files from affecting the operating system or vCAC. To change from the default location, uncheck Use Default Log Location and enter the log file location you want at the bottom of the page.

8. On the Ready to Install page, click Install.

When installation is complete and vSphere proxy agent service is started, all ESX Server hosts in the vCenter Server instance specified by the endpoint the agent is configured for are automatically discovered. Remember that you must configure XenServer and Hyper-V hosts for the hosts they are to manage (using vCAC Administrator > Agent Configuration in the vCAC console, as described in the vCloud Automation Center Operating Guide) before information about them can be collected by vCAC.

Using a Script to Install Multiple Agents

By using the VrmAgentInstaller.msi file, which can be extracted from the agent installer vCAC-Agent-Setup.exe, you can use a script to execute "silent" agent installations with no manual interaction required. The following is an example of such a script, installing a vSphere agent called VC-1, configured for the endpoint VC1Endpoint. The italicized values in the script refer to the input required when manually installing an agent, as described in the last section. TRANSFORMS keeps track of the agent instances.

To install another vSphere agent named VC-2 with endpoint VC2Endpoint on the same host, you would create another script with those values and TRANSFORMS set to AgentInstanceId02. A series of such scripts could be executed by a shell script to install as many agents as desired.

```bash
msiexec /i "VrmAgentInstaller.msi" /qb /norestart /l* Install-Agent.log AGENT_TYPE=vSphere AGENT_NAME=VC-1 VRM_SERVER_NAME=manager_service_host SERVICE_USER_NAME=agent_service_username SERVICE_USER_PASSWORD=agent_service_password REPOSITORY_USER=manager_service_username REPOSITORY_USER_PASSWORD=manager_service_password VSPHERE_AGENT_REPOSITORY_HOSTNAME=model_manager_web_host ADDLOCAL=Core-Agents,vSphereAgent VSPHERE_AGENT_ENDPOINT=VC1Endpoint MSINEWINSTANCE=1 TRANSFORMS=:AgentInstanceId01
```

Modifying Proxy Agent Configurations

At some time following the installation of a vCAC proxy agent, you may need to modify an agent configuration setting you specified during installation. In particular, if the credentials provided for a XenServer or Hyper-V server are entered incorrectly, the proxy agent will not be able to connect to the virtualization platform; in this case you would need to update the agent configuration with the correct credentials. (When this happens the failed login attempt is recorded in the log file in the agent directory.)

The installation configurations are encrypted in the agent configuration file. However, a proxy agent configuration utility can be used to make such modifications. The utility also allows you to change vCAC’s machine deletion policy for the virtualization platform with which the agent communicates.

To display the current agent configuration (except the password you provided during install) using the utility, log into the vCAC Server as a user with administrator-level credentials and change to the directory %SystemDrive%\Program Files (x86)\VMware\vCAC Agents\agent_name, where agent_name is the directory containing the proxy agent, which is also the name under which the agent was installed (see the previous procedure, "Installing a vCAC Agent"). Then issue the command
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get

For a vSphere agent, the output of the command looks like this:

managementEndpointName: vc227endpoint

doDeletes: True

For a Hyper-V or Xen agent:

Username: XS49admin

To change one of the configuration properties, issues the command

DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set property value

where property is one of the following:

<table>
<thead>
<tr>
<th>Table 18</th>
<th>Proxy Agent Configuration Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>property</td>
<td>descriptionz</td>
</tr>
<tr>
<td>managementEndpointName</td>
<td>The name of the generic endpoint for which the agent was configured at installation. Changing this property renames the generic endpoint within vCAC, rather than changing endpoints. (vSphere agents only.)</td>
</tr>
<tr>
<td>doDeletes</td>
<td>Determines whether machines are deleted from vCenter Server when destroyed in vCAC, or instead moved to the VRMDeleted folder. (vSphere agents only)</td>
</tr>
<tr>
<td>username</td>
<td>The username representing administrator-level credentials for the XenServer or Hyper-V server the agent communicates with. (XenServer and Hyper-V agents only.)</td>
</tr>
<tr>
<td>password</td>
<td>The password for the above username. (XenServer and Hyper-V agents only.)</td>
</tr>
</tbody>
</table>

If you omit value, the utility prompts you for the new value. This is useful for entering passwords because your entry for this property is not echoed to the screen.

For example, to change the administrator level credentials for the virtualization platform specified during the agent install, issue these commands:

DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith

DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password

Please enter the value for password:

Please confirm the value for password:

To cause vCAC to place machines in a vCenter Server folder called VRMDeleted when they are destroyed in vCAC, instead of immediately deleting them in vCenter Server (the default), issue this command:

DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes false

To switch vCAC back to the original behavior, immediate deletion, issue this command:

DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes true

After changing an agent’s configuration, restart the agent service by by selecting Start > Administrative Tools > Services and then restarting the vCloud Automation Center Agent – agentname service.)
**Note:** The `DynamicOps.Vrm.VRMencrypt.exe` command can be used to change the configuration of proxy agents only.
Chapter 5 Upgrading to vCAC 5.2.1

This chapter provides the necessary information required to upgrade to vCAC 5.2.1.

Supported Upgrade Paths

This guide describes how to upgrade a VMware vCloud Automation Center 5.2 or a VMware vCloud Automation Center 5.2 with applied hotfixes implementation to vCAC 5.2.1 To upgrade from earlier versions, first upgrade to vCAC 5.2.

Verify the Current vCAC Version

Verify the version of the currently installed vCAC instance by selecting the About link in the upper right of the vCAC console. The version displayed must be 5.2 or 5.2 with any installed hotfix.

Create or Import SSL Certificates

In release 5.2.1, vCAC and all its components are installed to use HTTPS as the transport protocol, which ensures secure communication between vCAC components.

As a result, before beginning a vCAC migration, you must decide which type of SSL certificate to use. See "SSL Configuration" on page 6 for more information about certificate requirements.

Note: After migration, the Repository, vCAC, and vCACReports applications in IIS have Require SSL selected.

Allow Machine-Related Operations to Complete

Ensure that all machine provisioning, reprovisioning, and disposing operations are completed and that no further machine-related operations are initiated until upgrade is complete. All workflows should be completed or canceled. Additionally, all pending requests must be resolved prior to migration, such as Lease Extension requests, Approvals, and Reclamation requests.

Verify All Data Collections Are Completed and Successful

For endpoint data collection:

1. Log in to the vCAC Console as a vCAC administrator.
2. Click vCAC Administrator > Endpoints.
3. For all physical endpoints, and any cloud or virtual endpoint that uses the DEM instead of a proxy agent to communicate with the provisioning platform (Amazon EC2, SCVMM, or vCloud Director), point to the name of the endpoint and click Data Collection.
4. Verify that the status of the most recent data collection is succeeded.
• If the data collection has been **requested**, wait for it to complete.
• If the data collection status is **failed**, consult the logs to resolve the issue, then click **Start** to initiate data collection.

For compute resource data collection:
1. Log in to the vCAC Console as an enterprise administrator.
2. Click **Enterprise Administrator > Compute Resources**.
3. For each compute resource in the list, point to the name of the compute resource, and click **Data Collection**.
4. For each type of data collection, verify that the status is **Succeeded**.
• If the data collection status is **In Progress**, wait for it to complete.
• If the data collection status is Failed, consult the logs to resolve the issue, then click **Request Now** to initiate data collection.
5. If your hosts belong to multiple enterprise groups with different administrators, repeat the above steps for each enterprise administrator.

**Record DEM, Agent, and Endpoint Information**

Record the configuration settings for all DEMs and Agents for later use. When you install version 5.2.1 of the DEMs and agents, you must provide the previous configuration settings.

To view the names and hosts of existing DEMs:
1. Log in to the vCAC Console as a vCAC administrator.
2. Click **vCAC Administrator > Distributed Execution Status**.
3. For each Distributed Execution Manager, note the following information:
   • Name
   • Host name (Machine)
   • Role
   • Skills, if any

To view the names of existing vCAC agents:
1. Log on to the vCAC Server.
2. Navigate to the agent installation location, typically `%SystemDrive%\Program Files (x86)\DynamicOps\DCAC Agents`.
3. For each subdirectory in this folder:
   a. Note the directory name. This is the agent's instance name.
   b. Navigate to the agent directory, open a command prompt, and type:
      
      DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get

  c. Record the value for **managementEndpointName**.
4. Repeat these steps for all hosts where agents are installed.
Record All Service User Credentials

VMware recommends that you use the same service user credentials for release 5.2.1 as for your existing implementation. Because this information may not be preserved when migrating to release 5.2.1, you should record it before you begin the migration process.

To determine the vCAC service user credentials:

1. Log on to the vCAC Server as a user with full administrative access.
3. Note the value under Log On As for the following services:
   - Each VMware vCloud Automation Center Agent – agentname service
   - Each VMware DEM-role - instancename service (DynamicOps Cloud Automation Center DEM if upgrading from DCAC 4.5)
   - The VMware vCloud Automation Center service (DynamicOps Cloud Automation Center if upgrading from DCAC 4.5) — Manager Service host only
   - Repeat these steps for any other host on which agents or DEMs may be installed.
4. To obtain the username for the Report Service, select Application Pools within IIS and make a note of the Identity shown for DcacReportAppPool, as shown in Figure 3.

Figure 3 DCACReport Service Username

Uninstall All Customizations

Uninstall all customizations made with the vCAC extensibility toolkits. For details, see the vCloud Automation Center Extensibility Guide.
If your implementation includes customizations supplied by VMware, contact your Professional Services team for assistance.

**Stop All vCAC Services**

Before you create backups of your existing implementation, stop all vCAC services.

When stopping services, first stop all services on all DEM and agent hosts other than the vCAC Server (Manager Service host), then stop the services on the vCAC Server.

To stop the vCAC services:

1. Log on as a user with full administrative access.
2. Select **Start > Administrative Tools > Services**.
3. Stop:
   - Each VMware vCloud Automation Center Agent – *agentname* service
   - Each VMware DEM-Worker - *instancename* service; wait 90 seconds and then stop each VMware DEM-Orchestrator - *instancename* service
   - The VMware vCloud Automation Center service — Manager Service host only

**Note:** Wait at least two minutes after stopping all vCAC services before continuing, to allow time for any current workflow instances to terminate.

4. Confirm that all workflows have stopped.
   a. Log in to the vCAC Console as a vCAC administrator.
   b. Click **vCAC Administrator > Distributed Execution Status**.
   c. Verify that the **Workflows Executing** value for all DEM workers is 0.

**Back Up Customization Files**

Before proceeding with migration, make a backup of the following files and store them in a safe place:

1. Application configuration files, including:
   a. **ManagerService.exe.config**, located in `%SystemDrive%\Program Files (x86)\DynamicOps\DCAC Server`
   b. **DynamicOps.DEM.exe.config**, located in `%SystemDrive%\Program Files (x86)\DynamicOps\Distributed Execution Manager\instance_name`
   c. **VRMAgent.exe.config**, located in `%SystemDrive%\Program Files (x86)\DynamicOps\Agents\instance_name`

2. Email templates located in `%SystemDrive%\Program Files (x86)\DynamicOps\DCAC Server\Templates`

3. Workflow configuration XML files located in `%SystemDrive%\Program Files (x86)\DynamicOps\DCAC Server\ExternalWorkflow\xmlldb`
Back Up vCAC Component Hosts

VMware recommends that you make a snapshot or a full backup of each vCAC component host (other than a standalone database host) for use in the unlikely event of a failed upgrade that does not roll back correctly. This includes systems hosting the Manager Service and Model Manager Data and the web components, if they are separate. In Web farm configuration, back up each host in the web cluster. In high availability mode, back up both Manager Service hosts.

Back Up the AzMan Store

Record your AzMan store settings and, if necessary, create a backup of your AzMan store prior to migrating.

To back up your AzMan store:

1. Open the ManagerService.exe.config file, located in %SystemDrive%\Program Files (x86)\DynamicOps\DCAC Server.
2. Search for authorizationStore.
3. Record the value of the authorizationStore attribute.
   - If the value begins with msxml://, back up the XML file in that location and store it in a safe place.
   - If the file begins with msldap://, back up your Active Directory–based authorization store. See the Microsoft documentation for details.
   - If the file begins with mssql://, you have a SQL-based authorization store and do not need to back it up separately. (It is backed up as part of backing up the vCAC database.)

Identify and Back Up the vCAC Database

To identify and back up the current vCAC database:

1. Log into the vCAC Server as a user with full administrative access.
2. Record the name and location of the current vCAC database. By default, the name is DCAC and the location is localhost, but these may have been specified differently during installation.

   **Note:** To confirm the name and location of the vCAC database, search the file ManagerService.exe.config in the vCAC server installation directory (typically %SystemDrive%\Program Files (x86)\DynamicOps\DCAC Server) for Initial Catalog= ... which shows the name of the vCAC database, and Data Source= ... which shows the server it is located on.

3. Make a backup of the current vCAC database in SQL Server, verifying that the backup completes successfully.

   **Caution:** Do not proceed without backing up the database.

   *Store the database files in a secure location where they cannot be accidentally destroyed.*
Verify Installation Prerequisites

Verify that release 5.2.1 installation requirements, as described in Chapter 2, are met on each host on which you will be upgrading a vCAC component by running the vCAC Prerequisite Checker.

**Note:** In addition to the requirements listed in the vCAC Prerequisite Checker, you must also ensure that Microsoft .NET Framework 4.5 is installed on all hosts.

**Prerequisites**

- Download the vCloud Automation Center installation package.

To verify prerequisites before upgrading vCAC:

1. Install the vCAC Prerequisite Checker.
   a. Navigate to the directory where you extracted the installation zip archive, then navigate to the **Tools** subdirectory.
   b. Right-click **vCAC-PrereqChecker-Setup** and select **Run as administrator**.

   The first time you install vCAC-PrereqChecker-Setup, it installs and launches the vCAC Prerequisite Checker.

2. Under **Core Install**, select the components that you are migrating on the current host.

3. If you are migrating a DEM instance, select **DEM** under **Core Upgrade**.

4. If you are not installing the Web components in the Default Web Site in IIS, specify the Web site to validate:
   a. Click the **Settings** tab.
   b. From the **Web site** drop-down list, choose the name of the Web site under which you are creating the vCAC web application.

6. Click **Run Checker**.

   The Prerequisite Checker displays the list of requirements for the selected component and the status of each one.

7. If any of the requirements do not have a green check mark (✓) in the Status column, select that requirement and follow the instructions in the information pane to the right to resolve the problem.

8. Repeat Step 7 until all requirements are satisfied.

9. Exit the Prerequisite Checker.

Upgrading to vCAC 5.2.1

Follow this process to upgrade your deployment:

1. Stop all vCAC services in your deployment.

2. Run **Setup.exe** to upgrade your installed vCAC components on each host machine.

3. Start all vCAC services beginning with the vCAC server. Do not start any other vCAC services until the vCAC server is started.
Stopping All vCAC services

Use Windows Component Services to stop all vCAC services on each machine that hosts vCAC components:

1. Click **Start > Control Panel > Administrative Tools**.
2. Double-click **Component Services**.
3. Right-click each vCAC service under Services (Local), select **Stop**, and wait for the service to stop.

Upgrading vCAC Components

Use the following procedure to upgrade all vCAC components in your deployment. If your vCAC components are installed on more than one host machine, run Setup.exe on each machine.

**Note**: If you are upgrading multiple components in a single host machine, VMware recommends that you upgrade all of the non-server components first, and then upgrade the server on the same machine. Alternately, you can uninstall all vCAC components from the machine and then reinstall the components.

**Prerequisites**

- Download the vCloud Automation Center installation package.

To upgrade installation using Setup.exe:

1. Navigate to the directory where you extracted the zip archive, then navigate to the **Setups** subdirectory.
2. Copy Setup.exe to the host machine.
3. Right-click **Setup.exe**, and select **Run as administrator**.
4. On the Welcome screen, click **Next**.
   The Welcome screen lists all of the components on the host machine to be upgraded. Click **Next**.
5. Review the end user license agreement on the License Agreement screen, select **I accept the terms in the license agreement**, and click **Next**.
6. Supply the requested information on the Detected Components screen:
   - Enter administrative credentials for the host machine under Model Manager Administrator Account.
   - Enter the database instance and name under Mssql Server Information for the vCAC 5.2 instance that you are upgrading.
   Click **Next**.
7. Review the information on the Ready to Configure screen, and click **Next**.
   The upgrade process displays on the Start Configuration screen.
8. Click **Next** after the upgrade process finishes.
9. Decide whether to start vCAC services automatically on the final page. If you have vCAC components installed on other machines, wait until all components are updated before starting services. Click Finish.

10. Verify the new version by launching the vCAC console and checking the About page. If upgrading from vCAC 5.2 to vCAC 5.2.1 is successful, the version displayed is 5.2.4 Build 101.

**Starting All vCAC services**

After all of the vCAC components are upgraded, use Windows Component Services to start all vCAC services on each machine that hosts vCAC components.

| Note: | Start the services in the following order: 1. vCAC server, 2. DEMs, 3. Agents.

1. Click Start > Control Panel > Administrative Tools.
2. Double-click Component Services.
3. Right-click each vCAC service under Services (Local), select Start, and wait for the service to start.

**Start the Console**

After all services are running, verify that your upgrade was successful by starting the vCAC Console.

To access the vCAC Console:

1. If you are using Internet Explorer, clear your browser cache prior to accessing the vCAC Console for the first time after upgrade.

   **Note:** The following instructions are for Internet Explorer 9. The steps may be different for earlier versions of IE.

   a. From the Tools menu, select Safety > Delete browsing history.
   b. In the Delete Browsing History dialog box, select Temporary Internet files.
   c. If the vCAC Console is in your Favorites list, clear the selection for Preserve Favorites Web site data.
   d. Click Delete.

      When the files are deleted, the “Internet Explorer has finished deleting the selected browsing history.” notification appears.

2. Navigate to: https://vCAC_portal_hostname/vCAC.
3. When prompted, provide your Windows credentials.
   The vCAC Console appears.
4. Before you begin to use vCAC, you must verify that your licenses are correct:
   a. In the vCAC Console, select vCAC Administrator > License Info.
   b. Verify that the license information is correct and make changes as required.
Post-Upgrade Steps

This section describes post-upgrade tasks that you must complete before the updated instance is considered fully operational.

Merge Configuration Files

If you made changes to any application configuration files, workflow configuration files, or email templates, merge your changes into the 5.1.2 version of the files.

**Caution:** Do not overwrite the 5.2 configuration files with your pre-upgrade files. You must manually merge your changes. If you require assistance, contact VMware support.

Rebuild WinPE Images

If you use vCAC for WIM-based provisioning, you must uninstall the 5.2 WinPEBuilder utility, install the 5.2.1 WinPEBuilder utility, and regenerate your WinPE images after upgrading to release 5.2.1.

To uninstall the 5.2 WinPEBuilder utility:

1. Log on as a user with administrative privileges to the vCAC host machine.
2. Click Start > Control Panel > Programs and Features.
3. Uninstall the WinPEBuilder utility.

**Prerequisites**

- Download the vCloud Automation Center installation package.
- Obtain and install Windows Automated Installation Kit.

To install the 5.2.1 WinPEBuilder utility:

1. Navigate to the directory where you extracted the zip archive, and locate vCAC-WinPEBuilder-Setup.exe in the Setups directory.
2. Copy vCAC-WinPEBuilder-Setup.exe to the host machine.
3. Right-click vCAC-WinPEBuilder-Setup.exe, and select Run as administrator.
4. On the Do you want to allow the following program to make changes to this computer dialog box, click Yes.
5. On the Welcome screen, click Next.
6. On the Custom Setup screen, click Next.
   The Installing vCAC PE Builder 2008 screen shows the installation status.
8. On the Completed screen, click Finish.

To rebuild WinPE images:

1. Update the guest agent in your WinPE image using one of the following methods:
   - After installing the 5.2.1 WinPEBuilder utility, generate a new ISO file.
• Insert the 5.2.1 guest agent executable into a WinPE image created using another method. For details about generating WinPE images for use with vCAC, see the *vCloud Automation Center Operating Guide*.

2. Optionally, update existing blueprints and build profiles to remove the `VirtualMachine.Admin.EncryptPasswords` property. This property has no effect if you are using a 5.2 WinPE image.
Chapter 6 Uninstalling and Reinstalling vCAC Components

This information contains procedures for uninstalling and reinstalling vCAC and related activities.

Uninstalling vCAC Server

If you have changed any vCAC configuration files, you may want to save these files before uninstalling vCAC in case you reinstall vCAC and want to restore your configuration.

To uninstall vCAC:

1. Log on as a user with administrative privileges.
2. Click Start > Control Panel > Programs > Uninstall a program.
3. Select VMware vCloud Automation Center Server and click Uninstall.

Modifying Installed Components

You can add or remove selected vCAC components by using the command line.

To add or remove selected vCAC components:

1. Navigate to the directory where you extracted the zip archive and locate Setup.exe in the Set-ups directory.
2. Copy Setup.exe to the host machine.
3. Right-click Setup.exe, and select Run as administrator.
4. Click Next on the welcome screen.
5. Select New/Repair/Remove on the vCAC Installation or Upgrade screen, and click Start.
6. Select the components you want to add or remove.
   Depending on your selections, a series of confirmation dialog boxes appear.

About Reinstalling vCAC

Before you reinstall the same version of vCAC that you have previously uninstalled:

- Delete HTTPS binding in IIS
- Delete the database or use a new database name
- Reuse the previous certificate or create a new one

For information about upgrading to a new version of vCAC, see Chapter 6.
Relocating the vCAC Instance

This section describes how to relocate vCAC components after the initial installation.

**Note:** In the event that you need to relocate your vCAC database to another server some time after installation and initial use, contact VMware support.

If the vCAC Server (the Manager Service host) is moved to a new Active Directory domain, authorization problems are likely to result. The best practice is to use the procedure in Creating the vCAC Database Manually to install a new vCAC instance in the desired domain using the existing vCAC database, rather than moving the existing vCAC Server to a new domain. In brief,

1. Gather and preserve information about existing modifications to the Manager Service configuration on the vCAC server, typically by preserving the existing `ManagerService.exe.config` file in `%SystemDrive%\Program Files x86\VMware\vCAC\Server` (or the vCAC server install directory if different); see the *vCloud Automation Center Operating Guide* for more information.
2. Gather information about all vCAC agent configurations (see Chapter 4) so that these can be applied to the new vCAC server and agents.
3. Install vCAC in the new domain with the existing database as described in Chapter 3.
4. Update the Manager Service configuration to match the existing vCAC server, typically by copying the preserved `ManagerService.exe.config` file to the vCAC install directory, and restart the VMware vCloud Automation Center service.
5. Install agents to match the all the agents in the existing vCAC installation; see Chapter 4 for more information.
6. Verify that the new vCAC installation functions properly, then uninstall the old vCAC agents and server.

Updating vCAC Licenses

When you reinstall vCAC components, you can use the same license key you used during installation. Please contact VMware Customer Support for all license-related queries and problems.

Updating Your vCAC License

You must provide a valid vCAC license key when installing vCAC.

To update your license:

1. Log in to the vCAC Console as a vCAC administrator.
2. Select **vCAC Administrator > License Info**.
3. Click **Add License**.
   
   The **Add License** dialog appears.
4. In **License key**, type a valid license key.
5. Click **OK**.

If the new license is not valid, a warning banner appears stating the reason for vCAC administrators, Enterprise Administrators and PGMs that machines can no longer be provisioned within your site. After you replace the invalid license, operation is restored.
Appendix A Installing the Extensibility Toolkits

The VMware extensibility toolkits consist of vCAC Designer and the vCloud Automation Center Development Kit (vCAC Development Kit).

With vCloud Automation Center Designer, you can customize workflows provided in the Model Manager and also associate workflows with DEM workers using skills. For an additional license, the vCAC Development Kit provides advanced extensibility tools, including the Workflow Generator Visual Studio plugin that enables you to create your own custom workflows and install them in the Model Manager.

Downloading the vCloud Automation Center Installation Package for Extensibility

The vCloud Automation Center installation package for extensibility contains the installers for the vCAC extensibility toolkits.

To download the vCloud Automation Center installation package for extensibility:

1. Download the zip file for vCloud Automation Center extensibility or the vCloud Automation Center Development Kit from the VMware downloads page at http://www.vmware.com/download/.
2. Extract the files from the zip archive.

Installation Package Contents

Table 19 describes the two installer options for the extensibility toolkits. Choose only one of the following depending on your situation:

Table 19 Installer Options for Extensibility Toolkits

<table>
<thead>
<tr>
<th>Installation package</th>
<th>Installer Executable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCAC-521-Extensibility.zip</td>
<td>DesignCenter-Setup.exe</td>
<td>Does not require an additional license. Installs vCloud Automation Center Designer and basic CloudUtil commands.</td>
</tr>
<tr>
<td>vCAC-521-DK-Installation.zip</td>
<td>CDK-Setup.exe</td>
<td>Requires a vCAC Development Kit license. Installs vCloud Automation Center Designer, the full set of CloudUtil commands and the Workflow Generator plugin.</td>
</tr>
</tbody>
</table>

In addition, the installation package for extensibility includes the installer for the vCAC Self-Service Portal. For information about this component, see Appendix B "Installing the vCAC Self-Service Portal Website".
Installation Prerequisites

The extensibility toolkits are typically installed on a development machine rather than a server. This section describes the system configuration requirements that must be in place before you install the extensibility toolkits. For operating system and high-level environment requirements, see the vCloud Automation Center Support Matrix.

- .NET Framework 4.5 must be installed.
- The vCAC Designer or vCAC Development Kit host must have network access to the Model Manager host (specifically, the Model Manager Web component).
- To support the Workflow Generator Visual Studio plugin (vCAC Development Kit only), Visual Studio 2010 or 2012 must be installed.

Installing vCloud Automation Center Designer

Prerequisites

- Download the vCloud Automation Center installation package for extensibility.

To install vCAC Designer:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the Setups subdirectory.
2. Right-click DesignCenter-Setup.exe and select Run as administrator.

   **Note:** When installing on a Windows XP system, right-click DesignCenter-Setup.exe and select Run as, then either select Current user and clear the selection for Protect my computer and data from unauthorized program activity, or select The following user and enter the credentials with administrator access to the system.

3. On the Welcome page, click Next.
4. On the End-User License Agreement page, read the License Agreement, click I accept the terms in the License Agreement, then click Next.
5. On the Custom Setup page, click Next.
6. On the Model Manager Web Service Host Name page:
   a. Specify the fully qualified domain name and port of the system hosting the Model Manager Web instance that you want the extensibility tools to interact with.
   b. Specify the user credentials under which the Model Manager is running.
   c. Click Next.

   The installer validates the combination of Model Manager host and credentials by attempting to access to the Model Manager; if it succeeds, you can continue with installation. If an error is returned, you must determine the correct combination of Model Manager host and credentials before proceeding.
7. On the Ready to Install page, click Install.
Installing the vCloud Automation Center Development Kit

The vCAC Development Kit installation includes vCloud Automation Center Designer.

Prerequisites

- Download the vCloud Automation Center installation package for the vCAC Development Kit.
- If you previously installed the vCloud Automation Center Designer without the vCAC Development Kit, first uninstall the vCloud Automation Center Designer, then proceed with the vCAC Development Kit installation.

To install vCAC Designer and the vCAC Development Kit:

1. Navigate to the directory where you extracted the installation zip archive, then navigate to the Setups subdirectory.
2. Right-click CDK-Setup.exe and select Run as administrator.

   **Note:** When installing on a Windows XP system, right-click DesignCenter-Setup.exe and select Run as, then either select **Current user** and clear the selection for **Protect my computer and data from unauthorized program activity**, or select **The following user** and enter the credentials with administrator access to the system.

3. On the Welcome page, click Next.
4. If you previously installed the vCloud Automation Center Designer without installing the vCAC Development Kit, and you did not uninstall it before installing the vCAC Development Kit:
   a. click Remove on the Change or remove installation page.
   b. Click Remove.
   c. Click Finish, return to step 1, then skip step 4.
5. On the Custom Setup page, select vCAC Designer to install the vCloud Automation Center Designer console and the extended CloudUtil command-line tool. Select Visual Studio 2010 or 2012 Addin to also install the Workflow Generator Visual Studio plug-in.

   **Note:** The Visual Studio 2010 or 2012 Addin option cannot be selected if the installer determines that Visual Studio is not installed. If both Visual Studio 2010 and Visual Studio 2012 are installed, the Addin is installed for Visual Studio 2012.

6. Click Next.
7. On the Model Manager Web Service Host Name page:
   a. Specify the fully qualified domain name and port of the system hosting the Model Manager Web instance that you want the extensibility tools to interact with.
   b. Specify the user credentials under which the Model Manager is running.
   c. Click Next.
The installer validates the combination of Model Manager host and credentials by attempting to access to the Model Manager; if it succeeds, you can continue with installation. If an error is returned, you must determine the correct combination of Model Manager host and credentials before proceeding.

8. On the Ready to Install page, click Install.

9. To enable the full functionality of the vCAC Development Kit, you must provide a vCAC Development Kit license key. If you did not enter the license key during the Model Manager installation and you did not added the license key in the vCAC console, you must:
   a. Log in to the vCAC Console as a vCAC administrator.
   b. Select vCAC Administrator > License Info.
   c. Click Add License.
   d. The Add License dialog appears.
   e. In License key, type a valid license key.
   f. Click OK.

Add vCAC Workflow Activities to Visual Studio

After installing the vCAC Developer Kit, you may want to add the vCAC workflow activities to the Visual Studio toolbox to use in custom workflows.

**Note:** The vCenter Orchestrator activities cannot be imported into Visual Studio. You must use vCAC Designer to access the activities that invoke vCenter Orchestrator workflows.

To add the vCAC activities to the toolbox:

1. Create a new Visual Studio project or open an existing project.
2. Ensure that the Toolbox is displayed. If it is hidden, open it.
3. Right-click in the Toolbox and select Add Tab.
4. Specify a name for the new tab, such as vCAC.
5. With the vCAC tab selected, select Tools > Choose Toolbox Items.
6. Browse to %SystemDrive%\Program Files x86\VMware\vCAC\Design Center\Addin\Templates\version\DynamicOps.Cdk.Activities.dll and click OK.
8. Click OK.

Updating the CloudUtil Application Configuration

The CloudUtil application configuration file, CloudUtil.exe.config, contains connection information for the Model Manager and databases that support any custom models you create with the vCloud Automation Center Development Kit.
To update the CloudUtil application configuration:

1. Navigate to the vCloud Automation Center Designer installation directory, where the CloudUtil.exe executable is located. (In a typical installation, this is %SystemDrive%\Program Files x86\VMware\vCAC\Design Center.)

2. Edit the file CloudUtil.exe.config.

3. Within the appSettings element, you can define properties by adding an entry in the following format:

   `<add key="keyName" value="keyValue" />`

The valid properties for CloudUtil are as follows:

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>repositoryAddress</td>
<td>The default root URI of the Model Manager. The initial value is set</td>
</tr>
<tr>
<td></td>
<td>based on the value for the Model Manager Web host name specified</td>
</tr>
<tr>
<td></td>
<td>in the installer.</td>
</tr>
<tr>
<td>Default Sql User</td>
<td>The default SQL user name to use to authenticate to the SQL</td>
</tr>
<tr>
<td></td>
<td>instance where the data specified by custom model resides.</td>
</tr>
<tr>
<td>Default Sql Password</td>
<td>The default SQL password to use to authenticate to the SQL</td>
</tr>
<tr>
<td></td>
<td>instance where the data specified by custom model resides.</td>
</tr>
</tbody>
</table>

4. You can also update the log location. By default, CloudUtil logs are located in %APPDATA%\VMware\vCloud Automation Center Designer\Logs\CloudUtil_All.log. You can change this by editing the following line:

   `<loggingConfiguration name="Logging Application Block" tracingEnabled="true" defaultCategory="Error" logWarningsWhenNoCategoriesMatch="false">`

   `<add name="LogFileListener" ... fileName="%APPDATA%\VMware\vCloud Automation Center Designer\Logs\CloudUtil_All.log" ... />`

   ...  

   `</loggingConfiguration>`

5. Save and close the file.

**Uninstalling the Extensibility Toolkits**

You can uninstall the extensibility toolkits using the Windows Control Panel. The following steps are for Windows 7 or Windows Server 2008 R2; they may differ slightly depending on your version of Windows.

To uninstall the extensibility toolkits:

1. Click **Start > Control Panel**.
2. Click **Uninstall a program**.
3. From the list of installed programs, select **VMware vCloud Automation Center Designer** (the name is the same regardless of whether you have installed the full vCAC Development Kit).

4. Click **Uninstall**.

Alternatively, you can run the installation program, **DesignCenter-Setup.exe** or **CDK-Setup.exe**, on the machine on which the extensibility toolkit is installed. The installer detects that you have an existing vCAC Designer or vCloud Automation Center Development Kit installation and you can click **Remove** to uninstall the toolkit.

## Upgrading the Extensibility Toolkits

If you have upgraded your vCloud Automation Center installation, you must upgrade your extensibility toolkits to maintain compatibility with your upgraded vCAC instance.

To upgrade the extensibility toolkits:

1. Uninstall the previous version of the **VMware vCloud Automation Center Designer** program.
2. Delete each user’s cache, which can be found at `%SystemDrive%\Users\username\AppData\Roaming\VMware\vCloud Automation Center Designer\AssemblyCache`.
3. Install the version of vCAC Designer or the vCloud Automation Center Development Kit that matches the version of your vCAC instance.
Appendix B Installing the vCAC Self-Service Portal Website

The vCAC Self-Service Portal Website is a standalone interface that streamlines a user’s ability to request access to virtual, cloud or physical machines. This portal is not the same as the Self-Service option that is available from the vCAC Console.

When a user accesses the vCAC Self-Service Portal Website, all of the policies controlling machine specifications, provisioning, approval, management, and disposal have been completed by the administrator in the vCAC Console. This enables users to request and manage machines for their own use according to these policies. The vCloud Automation Center Operating Guide provides details on using the vCAC Self-Service Portal Website.

Downloading the vCAC Self-Service Portal Website

The vCloud Automation Center installation package for extensibility contains the installer for the vCAC Self-Service Portal Website.

To download the vCloud Automation Center installation package for extensibility:

1. Download the zip file for vCloud Automation Center extensibility or the vCloud Automation Center Development Kit from the VMware downloads page at http://www.vmware.com/download/.
2. Extract the files from the zip archive.

Installation Package Contents

Table 1 describes the installer options for the vCAC Self-Service Portal Website.

Table 1 Installer for vCAC Self-Service Portal Website

<table>
<thead>
<tr>
<th>Installation package</th>
<th>Installer Executable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCAC-521-Extensibility.zip</td>
<td>vCAC-SelfService-Setup.exe</td>
<td>vCAC Self-Service Portal Website installation program.</td>
</tr>
</tbody>
</table>

Note: As a precaution, always make a backup copy of your system and database before installing any new software on your systems.

Installation Prerequisites

This section provides you with the information about what software needs to be installed before you install the vCAC Self-Service Portal Website and instructions on how to verify that the prerequisite software is installed.

Before you begin installing the vCAC Self-Service Portal Website, you must install the core vCAC components are installed and configure according to your business needs and logic. For more information, see Chapter 3 Installing vCAC.

Prior to installing the vCAC Self-Service Portal, these components must be installed:

- IIS Server
Verifying Installation Prerequisites

Confirm that the components for the vCAC Self-Service Portal Website are available and meet the installation prerequisites by using the vCAC Prerequisite Checker.

To verify installation prerequisites:

1. Navigate to the directory where you extracted the vCloud Automation Center installation package, then navigate to the Tools subdirectory.
2. Right-click **vCAC-PrereqChecker-Setup** and select **Run as administrator**.
   
   The first time you install vCAC-PrereqChecker-Setup, it installs and launches the vCAC-Prerequisite Checker.
3. Select **vCAC Self-Service Portal Website** and clear the check boxes for the other components.
4. Click **Run Checker**.
   
   The vCAC Prerequisite Checker displays the list for requirements and the status of each one. If any of the requirements do not have a green check mark (✓) in the Status column, select that requirement and follow the instructions in the information pane to the right to resolve the problem.
5. (Optional) Save the vCAC Prerequisite Checker results.
6. Click **Run Checker**.
7. Exit the vCAC Prerequisite Checker.

Installing the vCAC Self-Service Portal Website

This section provides detailed instructions on installing the vCAC Self-Service Portal Website. The vCloud Automation Center installation package for extensibility contains the installer for the vCAC Self-Service Portal.

To install the vCAC Self-Service Portal Website:

1. Navigate to the directory where you extracted the vCAC-52-Extensibility.zip file, then navigate to the **Setups** subdirectory.

- IIS Server Anonymous Authentication Status
- IIS Server ASP.NET Module
- IIS Server Default Document Module
- IIS Server HTTP Redirect Module
- IIS Server ISAPI Extensions Module
- IIS Server ISAPI Filter Module
- IIS Server Windows Authentication Module
- IIS Server Static Content Module
- IIS Server Windows Authentication Status
2. Copy the vCAC-SelfService-Setup.exe file to the installation host machine.
3. Right-click vCAC-SelfService-Setup.exe and select Run as administrator.
   The Setup Wizard appears.
4. On the Welcome page, click Next.
5. Review and accept the terms of the license agreement and click Next.
6. On the Destination Folder page, select the folder you want to install to, then click Next.
7. On the Ready to Install the Program page, click Install.
   The Welcome to the vCAC Software Configuration Wizard page appears.
9. Click Next.
10. On the Welcome screen, click Next.
11. On the vCAC Database Information page:
    a. In Database instance, type the name of the database instance you typed when you set up
       your database.
    b. In Database name, type the name of the database (default value is DCAC).
    c. Select Use Windows identity of the currently logged on user to perform configuration
       tasks that involve database operations to use the credentials under which you are running
       the installer to connect to the database. Clear the check box to use SQL authentication and
       provide the credentials with which to connect to the database.
    d. Click Next.
12. On the Self Service Portal Model Manager Information page:
    a. In Service User Account, type the user name of the service account user who has access
       the database and is the owner of the selected database, or click Add Current User, then
       type and confirm the password.
    b. In Model Manager Configuration, type the host name of the Model Manager Web Service,
       type the name of the account that was used to install vCAC, then type and confirm the pass-
       word.
    c. VMware recommends that you click Test to test connectivity to the Model Manager host
       before proceeding.
14. Click Finish.

**Enabling the Connect Using SSH option for Linux Machines**

The Connect Using SSH option can be made available for Linux machines provisioned in vCAC. Enabling this option requires additional system configuration after installing the Self-Service Portal as well as per-blueprint configuration.

To enable the use of the Connect Using SSH option:
1. On the vCAC Manager Service host, edit the file `C:\Program Files (86)\DynamicOps\Self-Service Portal\Web.config`.

2. At the end of the `<appSettings>` section, before `</appSettings>`, insert:

   ```xml
   <add key="ShowConnectUsingSsh" value="true" />
   ```

3. Execute an IIS reset and restart the Manager Service.

4. Add the custom property `Machine.SSH` with a value of `true` to a blueprint or a build profile incorporated to each blueprint for which you want to enable the option.

For any powered on machine provisioned from the blueprint, the Connect Using SSH menu option appears. When you select it the browser attempts to load the URL `ssh://machine_name`, which requires an SSH URL handler to be installed on the system on which you clicked the link. SSH must also be enabled on the guest operating system.

**Upgrading or Reinstalling the vCAC Self-Service Portal**

You can upgrade or reinstall the VMware vCloud Automation Center Self-Service Portal instance using the vCAC 5.2.1 installer, `setup.exe`. 