You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com
# Table of Contents

1 Overview of vCAC Deployment ............................................... 1
   Portal Website .......................................................................... 1
   Reports Website ........................................................................ 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
   Planning Your Installation ......................................................... 5
      Authorization Store ............................................................. 5
      Database Deployment .......................................................... 6
      SSL (HTTPS) Configuration .................................................. 6
      Firewall Configuration ......................................................... 6
   vCAC Installation Profiles ......................................................... 7
      Core vCAC Components ....................................................... 7
      Agents and DEM Workers .................................................... 8
      Additional vCAC Components .............................................. 8
   Installation Prerequisite Checklist .............................................. 9
      Database Server Requirements ............................................. 9
      Web Server Requirements ................................................... 9
      vCAC Server Requirements .................................................. 10
      DEM Requirements ............................................................ 10
   vCAC Prerequisite Checker ....................................................... 11
   Users and Credentials Required for Installation ....................... 11
   Users and Credentials Required for vCAC Services .................. 12
   Installation Planner ................................................................. 13

3 Installing vCAC ........................................................................ 15
   High-Level Installation Process ............................................... 15
   Preparing the Authorization Store .......................................... 15
      Preparing a SQL-based Authorization Store ......................... 15
      Preparing an Active Directory–based Authorization Store .... 15
   Creating the vCAC Database ................................................... 16
4 Integrating with Provisioning Resources .......................... 37

DEM Worker Overview .................................................. 37
Amazon EC2 Requirements ........................................... 37
SCVMM Requirements ................................................... 37

vCAC Agent Overview .................................................. 38
Planning Your vCAC Proxy Agents .................................. 38
Configuring Proxy Agents .............................................. 39
Enabling Remote WMI Requests on Windows Machines .... 39
Virtual Desktop Integration ........................................... 40
External Provisioning Integration ................................... 40
Using Visual Basic Scripts in Provisioning ....................... 40
vCAC Agent Relationships ............................................. 41
vCAC Agent Installation Location and Requirements ........ 42

Hypervisor Proxy Agent Installation Requirements .......... 42
WMI Agent Installation Requirements ............................ 44
# Table of Contents

VDI Integration Agent Installation Requirements ............................................... 44  
EPI Agent Installation Requirements ................................................................. 46  
Preparing Endpoints for vSphere Agents .............................................................. 48  
Installing a vCAC Agent .................................................................................... 49  
Using a Script to Install Multiple Agents ............................................................ 56  
Modifying Proxy Agent Configurations ............................................................... 56  

## 5 Upgrading vCAC and vCAC Agents .............................................................. 59  

- Change to Default Transport Protocol ............................................................. 59  
- Overview of the vCAC Upgrade Process ......................................................... 59  
- Allow Machine-Related Operations to Complete ............................................ 60  
- Back Up DCAC Component Hosts ................................................................. 60  
- Verify the Current DCAC Version .................................................................. 60  
- Verify DEM and Agent Information ............................................................... 60  
- Stop DCAC Services ..................................................................................... 60  
- Identify and Back Up the DCAC Database .................................................... 61  
- Back Up Active Directory–based AzMan Store .............................................. 61  
- Extracting the Upgrade Files .......................................................................... 61  
- Upgrading the Database .................................................................................. 61  
- Determine the Report Service Username ...................................................... 62  
- Verify Installation Prerequisites ..................................................................... 63  
- Upgrade vCAC ............................................................................................... 64  
- Upgrade Distributed Execution Managers ..................................................... 68  
- Upgrade vCAC Agents ................................................................................... 68  
- Update the vCAC License ............................................................................. 70  
- Restart the Manager, DEM and Agent Services ............................................ 71  
- Start the Console ............................................................................................ 71  
- Post-Upgrade Steps ....................................................................................... 71  
  - Initiate Data Collection ................................................................................ 71  
  - Verify Email Settings .................................................................................. 72  
  - Rebuild WinPE Image .................................................................................. 73  
  - Enable Amazon EC2 Reservations ............................................................ 73  

## 6 Uninstalling and Reinstalling vCAC Components ........................................ 75  

- Uninstalling vCAC ........................................................................................ 75
A Installing the Extensibility Toolkits ........................................ 77

Installation Prerequisites ........................................................................... 77
Installing vCloud Automation Center Designer ................................. 77
Installing the vCloud Automation Center Development Kit ................. 78
Add vCAC Workflow Activities to Visual Studio .............................. 79
Updating the CloudUtil Application Configuration ......................... 80
Uninstalling the Extensibility Toolkits ............................................. 81
Upgrading the Extensibility Toolkits .............................................. 81
Restoring Custom Events ........................................................................ 81
About This Book

This guide describes the installation and initial configuration of VMware vCloud Automation Center™ (vCAC) 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.

There are three high-level tasks involved in setting up vCAC:

1. Installing the core vCAC components and starting the vCloud Automation Center Service (commonly called the Manager Service), then installing and starting at least one Distributed Execution Manager (DEM) Orchestrator and one DEM Worker to create a working vCAC instance.

2. Configuring vCAC to communicate with the provisioning resources in your environment. This can include:
   - Installing additional DEM Worker instances to manage provisioning
   - Installing and configuring vCAC agents, including proxy agents for XenServer and Hyper-V hosts and vCenter Server instances
   - Installing a Windows Management Instrumentation (WMI) agent to collect data from provisioned Windows machines
   - Installing agents to integrate vCAC with external systems

3. Installing optional vCAC components depending on the needs of your deployment. Several optional components are described in the vCloud Automation Center Operating Guide.
Chapter 1 Overview of vCAC Deployment

This chapter 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 cohosting some components.

Portal Website

The portal website provides access to the vCAC web console at http://web_server_hostname/DCAC. 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 Website

The reports website provides access to vCAC reports, available through a link in the vCAC console and at http://web_server_hostname/DCACReports. The reports website 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. By providing 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 as well as the DEMs and portal website.

The Model Manager is divided into two separately installable components — the Model Manager web service and the Model Manager data component. The Model Manager components should always be cohosted.

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

- Secure Multi-Tenancy — Controls who 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 then 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.
vCAC Agents

vCAC uses several different agents.

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.

Proxy agents communicate with the Manager Service. Each proxy agent 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 chapter guides you through the planning process for your vCloud Automation Center installation and provides a high-level overview of the installation process.

Planning Your Installation

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.

Authorization Store

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

- File-based authorization store
- SQL-based authorization store
- Active Directory authorization store

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

File-based Authorization Store

The file-based authorization store is implemented as an XML file on the vCAC Server (Manager Service host). If you select this option, the vCAC installer creates the authorization file automatically.

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 not supported if the Manager Service and Model Manager components are not cohosted (as in a typical production deployment).

SQL-based Authorization Store

The SQL-based authorization store uses the vCAC database to store authorization information. If you select this option, the vCAC installer provides an option to create the authorization tables in the database automatically. 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

The Active Directory authorization store is implemented using Active Directory (AD), or the Lightweight Directory Services (LDS) component of AD. If you select this option, you must prepare the authorization store in AD or LDS before installation. For details about preparing an Active Directory-based authorization store, see Preparing the Authorization Store.
Database Deployment

VMware recommends that you deploy a dedicated server running Microsoft SQL Server to host the vCAC database.

For your convenience, the vCAC installer provides an option to create the vCAC database automatically. If you do not want to create the vCAC database using the automatic installer, you can create the database manually. A third option is to create an empty database and use the installer to install the vCAC schema in the existing database.

When you install vCAC, you have the option to choose between connecting to the database using SQL-based authentication or Windows authentication.

SSL (HTTPS) Configuration

By default, vCAC and its components are installed to use HTTPS as the transport protocol (rather than HTTP). Installing with HTTPS ensures secure communication between vCAC components.

The following considerations apply when selecting the transport protocol for vCAC:

- You must use the same transport protocol for all vCAC components. If any one component is installed to use HTTPS, all components must be installed to use HTTPS, including all Distributed Execution Managers (DEMs) and agents.

- Before beginning an HTTPS installation, you must set up certificates in IIS on each web server or Manager Service host. Refer to the Microsoft documentation on configuring SSL for Internet Information Services. VMware recommends using domain certificates on vCAC hosts.

- When installing vCAC to use HTTPS, all host names provided during installation must be specified as fully qualified domain names.

- If vCAC is installed to use HTTPS, the vCAC Console can be accessed using either HTTP or HTTPS.

Firewall Configuration

All vCAC components (including Distributed Execution Managers and agents) and all virtualization hosts (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. The following tables describe the ports that must be open, depending on whether you are installing vCAC to work with HTTPS or HTTP.

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

<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>
</tbody>
</table>
Table 2  TCP Ports used by vCAC (HTTP)

<table>
<thead>
<tr>
<th>Source Component</th>
<th>Target Component</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy agents</td>
<td>Manager Service</td>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>virtualization host</td>
<td>Manager Service</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 section 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

The following table 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 3  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>DCACPrereqCheckerInstaller.msi</td>
</tr>
<tr>
<td>Database Server</td>
<td>vCAC Database</td>
<td><em>(using vCAC installer)</em> DCAC-Manager-Setup.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>(manual installation)</em> DBInstall.zip</td>
</tr>
<tr>
<td>Web Server</td>
<td>Model Manager (Web and Data)</td>
<td>DCAC-Manager-Setup.exe</td>
</tr>
<tr>
<td></td>
<td>Portal Website</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reports Website</td>
<td></td>
</tr>
</tbody>
</table>
vCAC Agent 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 type of agents varies depending on the provisioning resources in your implementation.

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

**Table 4 vCAC Agent and DEM Installers**

<table>
<thead>
<tr>
<th>vCAC Component</th>
<th>Installer File Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEM Worker</td>
<td>DCAC-Dem-Setup.exe</td>
<td>VMware strongly recommends that you install and run the Prerequisite Checker (DCACPrereqCheckerInstaller.msi) before installing the DEM.</td>
</tr>
<tr>
<td>vCAC Agent</td>
<td>DCAC-Agent-Setup.exe</td>
<td></td>
</tr>
</tbody>
</table>

**Additional vCAC Components**

The following components are optional and may or may not apply depending on your implementation.

**Table 5 Optional vCAC Components and Installers**

<table>
<thead>
<tr>
<th>vCAC Component</th>
<th>Purpose</th>
<th>Installer File or Directory Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AzMan utility</td>
<td>Creates Active Directory-based authorization store</td>
<td>AzManUtil.zip</td>
</tr>
<tr>
<td>vCAC Designer</td>
<td>Includes the vCloud Automation Center Designer application, which provides a visual workflow editor for customizing vCAC workflows and a graphical interface for managing skills, and the basic CloudUtil command-line tool.</td>
<td>DesignCenter-Setup.exe</td>
</tr>
</tbody>
</table>
| vCloud Automation Center
  Development Kit                  | Includes vCloud Automation Center Designer, an extended set of CloudUtil commands, and the Workflow Generator plugin for Visual Studio. This component requires the vCAC Development Kit License. | CDK-Setup.exe                    |
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
- No firewalls between Database Server and the web server or vCAC Server, or ports opened as described in Firewall Configuration
- IIS Server Metabase Module installed
- If using SQL Server Express, the SQL Server Browser service must be running.

### Web Server Requirements

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

<table>
<thead>
<tr>
<th>vCAC Component</th>
<th>Purpose</th>
<th>Installer File or Directory Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEBuilder utility</td>
<td>Creates WinPE images. For more information, see the vCloud Automation Center Operating Guide.</td>
<td>DCAC-WinPEBuilder-Setup.exe</td>
</tr>
<tr>
<td>vCAC Bulk Operations Client</td>
<td>Enables an enterprise administrator to perform actions on multiple machines simultaneously. For more information, see the vCloud Automation Center Operating Guide.</td>
<td>DCACBulkOperationsClientInstaller.msi</td>
</tr>
<tr>
<td>vCAC Guest Agent executables</td>
<td>Used in WIM-based and SCCM-based provisioning. For more information, see the vCloud Automation Center Operating Guide.</td>
<td>DCAC-GuestAgent2010Zip.zip</td>
</tr>
<tr>
<td>Linux Guest Agent installation files</td>
<td>Used in Red Hat Linux kickstart or SUSE autoYaST provisioning. For more information, see the vCloud Automation Center Operating Guide.</td>
<td>LinuxGuestAgentPkgs</td>
</tr>
<tr>
<td>vCAC Self-Service Portal</td>
<td>Provides an interface that streamlines a user's ability to request access to virtual, cloud or physical machines. For more information, see the vCloud Automation Center Self-Service Portal Guide.</td>
<td>DCAC-SelfService-Setup.exe</td>
</tr>
</tbody>
</table>
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.

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.
- IIS Server with Metabase module installed

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.
The vCAC Prerequisite Checker helps you ensure that you have satisfied all installation prerequisites. When you run the 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 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 exe-
vCloud Automation Center

Cut 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.

This following table describes the required privileges for each service or component.

#### Table 6 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>
<tr>
<td>Model Manager Web</td>
<td>Domain user with the following:</td>
</tr>
<tr>
<td></td>
<td>- Local Administrator privileges on host on which Model Manager Web is installed</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Full Administrator privileges are not required if the service user has modify privileges for C:\Windows\Temp</td>
</tr>
<tr>
<td></td>
<td>- <strong>dbo</strong> privileges for the vCAC database</td>
</tr>
<tr>
<td>Manager Service</td>
<td>Domain user with the following:</td>
</tr>
<tr>
<td></td>
<td>- Local Administrator privileges on host on which Manager Service is installed</td>
</tr>
<tr>
<td></td>
<td>- Local Administrator privileges on all hosts on which Model Manager Website is installed</td>
</tr>
<tr>
<td></td>
<td>- <strong>dbo</strong> privileges for the vCAC database</td>
</tr>
<tr>
<td></td>
<td>In order 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.</td>
</tr>
<tr>
<td>DEM</td>
<td>Domain user with local Administrator privileges on all hosts on which Model Manager Web is installed</td>
</tr>
<tr>
<td>Proxy Agent</td>
<td>Domain user</td>
</tr>
</tbody>
</table>
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:**

- _______________________

### Transport Protocol

**Circle one:**

- HTTPS
- HTTP

### Table 7 Database Server Information

<table>
<thead>
<tr>
<th>Property</th>
<th>Installer and Page</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance name</td>
<td>DCAC-Manager-Setup.exe &gt; vCAC Database Connection Configuration</td>
<td>(vCAC Database Configuration page when not installing the database component)</td>
</tr>
<tr>
<td>Database name</td>
<td>DCAC-Manager-Setup.exe &gt; vCAC Database Configuration</td>
<td></td>
</tr>
<tr>
<td>Database user credentials</td>
<td>DCAC-Manager-Setup.exe &gt; vCAC Database Connection Configuration</td>
<td>(vCAC Database Configuration page when not installing the database component)</td>
</tr>
<tr>
<td>Database data directory</td>
<td>DCAC-Manager-Setup.exe &gt; vCAC Database Configuration</td>
<td></td>
</tr>
<tr>
<td>Database log directory</td>
<td>DCAC-Manager-Setup.exe &gt; vCAC Database Configuration</td>
<td></td>
</tr>
</tbody>
</table>

### Table 8 Web Server Information

<table>
<thead>
<tr>
<th>Property</th>
<th>Installer and Page</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name (fully qualified domain name of web server or web cluster)</td>
<td>DCAC-Manager-Setup.exe &gt; Model Manager Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DCAC-Manager-Setup.exe &gt; vCAC Email Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DCAC-Dem-Setup.exe &gt; Manager Service and Model Manager Web Service Host Configuration</td>
<td></td>
</tr>
<tr>
<td>Website name</td>
<td>DCAC-Manager-Setup.exe &gt; IIS Site Bindings Page</td>
<td></td>
</tr>
<tr>
<td>Model Manager log directory</td>
<td>DCAC-Manager-Setup.exe &gt; Model Manager Configuration</td>
<td></td>
</tr>
</tbody>
</table>
## vCAC Server Information

<table>
<thead>
<tr>
<th>Property</th>
<th>Installer and Page</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Manager Web service user credentials</td>
<td>DCAC-Manager-Setup.exe &gt; Model Manager Configuration DCAC-Dem-Setup.exe &gt; Manager Service and Model Manager Web Service Host Configuration</td>
<td></td>
</tr>
<tr>
<td>Web portal user credentials</td>
<td>DCAC-Manager-Setup.exe &gt; Web Portal Configuration</td>
<td></td>
</tr>
</tbody>
</table>

## Email Server Information

<table>
<thead>
<tr>
<th>Property</th>
<th>Installer and Page</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP server host name</td>
<td>DCAC-Manager-Setup.exe &gt; vCAC Email Configuration</td>
<td>Defaults to 25; can be edited post-installation</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>DCAC-Manager-Setup.exe &gt; vCAC Email Configuration</td>
<td></td>
</tr>
<tr>
<td>Email address from which to send notifications</td>
<td>DCAC-Manager-Setup.exe &gt; vCAC Email Configuration</td>
<td></td>
</tr>
<tr>
<td>SMTP server user credentials</td>
<td>DCAC-Manager-Setup.exe &gt; vCAC Email Configuration</td>
<td></td>
</tr>
</tbody>
</table>

### SMTP protocol

Circle one: **SSL** non-SSL
Chapter 3 Installing vCAC

This chapter describes the procedures for installing the core vCAC components in a typical deployment topology.

High-Level Installation Process

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

To install the core vCAC components:

1. Prepare the authorization store if necessary.
2. Install the vCAC database.
3. Install the web components.
4. Install the Manager Service.
5. Install the Distributed Execution Managers.

After you have installed vCAC and verified your installation, you can proceed to configure vCAC to communicate with the provisioning resources in your environment, described in Appendix 4.

Optionally, you can install the vCAC Self-Service Portal or extensibility toolkits. For information about installing the Self-Service Portal, see the vCloud Automation Center Self-Service Portal Guide. For information about installing the extensibility toolkits, see Appendix A.

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.

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.

To create an Active Directory authorization store:

2. Extract the contents of the zip file 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 the **Store name** field, enter 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 following sections describe how to create the vCAC database. You have the following options for creating the database:

- Use the vCAC installer to create the vCAC database.
- Create an empty database and use the installer to install the vCAC schema in the existing database.
- Create the database manually.
Verifying Installation Prerequisites

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

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

To verify vCAC database server prerequisites:

1. Install the vCAC Prerequisite Checker.
   a. Download the installer file, DCACPrereqCheckerInstaller.msi, from the VMware product page at http://www.vmware.com/products to the installation host.
   b. Open a command prompt as administrator and navigate to the directory containing the installer.
   c. Execute the installer and follow the steps in the installer wizard.
2. Navigate to the installation directory. Typically, this is %SystemDrive%\Program Files (x86)\DynamicOps\DCAC Prereq Checker.
3. Right-click PrereqChecker.exe and select Run as administrator.
4. In the vCAC Prerequisite Checker, 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.
5. Click Run Checker.
   The 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 7 until all requirements are satisfied.
8. Exit the Prerequisite Checker.

Preparing 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 installer.

If you are creating the database using the installer or setting up the vCAC database manually, you can skip this step.

To prepare an empty database for use with vCAC:

1. Download the DBInstall.zip file from the VMware product page at http://www.vmware.com/products to the database host and extract it to a local directory.
2. Log in to the database host as a user with sufficient rights to create and drop databases (sysadmin privileges) within the SQL Server instance.
3. 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>$(DBName)</td>
<td>Name of the database, such as DCAC</td>
</tr>
<tr>
<td>$(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>

4. 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. Open SQL Server Management Studio.
6. Click **New Query**.
   
   A SQL Query window opens in the right-hand pane.
7. On the **Query** menu, ensure that **SQLCMD Mode** is selected.
8. Paste the entire modified contents of `CreateDatabase.sql` into the query window.
9. Click **Execute**.

**Creating the vCAC Database Using the Installer**

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

To create the vCAC database using the installer:

1. Download the installer file, `DCAC-Manager-Setup.exe`, from the VMware product page at http://www.vmware.com/products to the installation host.

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

2. Navigate to the directory containing the installer, right-click the installation executable 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**.
5. On the vCAC License Configuration page, provide the full file path to your vCAC license file:
   
   a. Click **Browse**.
   
   b. Browse to the location of your vCAC license file (XML).
   
   c. Select the file and click **Open**.
   
   d. Click **Next**.
6. On the Custom Setup page, select **Database** and cancel the selection for all other features, then click **Next**.

7. On the vCAC Database Connection Configuration page:
   a. Select **Use Windows Authentication** 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.
   
   b. In the **SQL Database Server Instance** box, specify the database instance in the format `hostname\instancename` (or `hostname` if using the default instance), or accept the default value `localhost`.
   
   c. Click **Next**.

8. On the vCAC Database Configuration page:
   a. If you previously prepared an empty database to use for vCAC, select **Use pre-created empty database** to indicate that the installer should create the vCAC schema in the existing database.
   
   b. VMware recommends that you select **Use default SQL Database data and log directory**. To specify alternative locations for the data and log directories, clear the check box.
   
   c. In the **SQL Database Name** box, type the name of the database or accept the default value of `DCAC`.
   
   d. Click **Test Connection** to ensure that the credentials being used have the necessary permissions.
      
      If the credentials do not have the proper permissions, cancel the installation and configure the permissions in SQL Server. For more information, see Users and Credentials Required for Installation.
   
   e. Click **Next**.

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

### 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 the following:

- .NET 2.0 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.

To create the vCAC database using the provided scripts:

1. Download the `DBInstall.zip` file from the VMware product page at http://www.vmware.com/products to the database host and extract it to a local directory.

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

4. Execute the following command with the arguments described in the table below:

```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 host\instance name (or hostname if using the default instance). Default is localhost.</td>
</tr>
<tr>
<td>DBName</td>
<td>Name of the vCAC database. Default is DCAC.</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>
<tr>
<td>ServiceUser</td>
<td>User name under which the vCAC Manager Service runs.</td>
</tr>
<tr>
<td>ReportLogin</td>
<td>User name under which the vCAC web services run.</td>
</tr>
</tbody>
</table>

## Creating a SQL-based Authorization Store Manually

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

To create a SQL-based authorization store manually:

1. Download the **DBInstall.zip** file from the VMware product page at http://www.vmware.com/products to the database host and extract it to a local directory if you have not already done so.

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

3. 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**.

4. Repeat step 3 with **AzManStoreExtSP.sql** followed by **AzManStoreData.sql**.

5. Exit SQL Server Management Studio.

## 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 provided with vCAC on the database to enable the Manager Service to communicate with it.

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

1. Download the DBInstall.zip file from the VMware product page at http://www.vmware.com/products to the database host and extract it to a local directory.

2. Edit VMPSOpsUser.sql and replace all instances of $(ServiceUser) with the username 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 Appendix 2 for information about Manager Service credentials.)

3. Open SQL Server Management Studio.

4. Select the vCAC database (DCAC by default) under Databases in the left hand pane.

5. Click New Query.

   A SQL Query window opens in the right hand pane.

6. Paste the entire modified contents of VMPSOpsUser.sql into the query window.

7. Click Execute.

### Installing the Web Components

The web components of vCAC include the portal website, reports website, and the Model Manager. The Model Manager consists of two installable components: Model Manager Web and Model Manager Data, which should be cohosted.

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

To install the vCAC web components:

1. Install the vCAC Prerequisite Checker.
   a. Download the installer file, DCACPrereqCheckerInstaller.msi, from the VMware product page at http://www.vmware.com/products to the installation host.
   b. Open a command prompt as administrator and navigate to the directory containing the installer.
   c. Execute the installer and follow the steps in the installer wizard.

2. Run the vCAC Prerequisite Checker to verify the installation prerequisites.
   a. Navigate to the directory where the Prerequisite Checker is installed. Typically, this is %SystemDrive%\Program Files (x86)\DynamicOps\DCAC Prereq Checker.
   b. Right-click PrereqChecker.exe and select Run as administrator.

   The vCAC Prerequisite Checker launches.

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

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

e. Click **Run Checker**.

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

g. 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.

h. Repeat Step f until all requirements are satisfied.

i. Exit the Prerequisite Checker.

3. Download the installer file, **DCAC-Manager-Setup.exe**, from the VMware product page at http://www.vmware.com/products to the installation host.

4. Navigate to the directory containing the installer, right-click the installation executable and select **Run as administrator**.

5. On the Welcome page, click **Next**.

6. On the End-User License Agreement page, read the License Agreement, click **I accept the terms in the License Agreement**, then click **Next**.

7. On the vCAC License Configuration page, provide the full file path to your vCAC license file:
   a. Click **Browse**.
   b. Browse to the location of your vCAC license file (XML).
   c. Select the file and click **Open**.
   d. Click **Next**.

8. On the Custom Setup page, select **Model Manager** (entire feature), **Website**, and **Report.Website**. Cancel the selection for all other features, then click **Next**.

9. On the IIS Site Bindings Configuration page:
   a. Leave **Enable Web Farm Support** unselected. (This option enables tracking of user session information in a shared session state database. For information about a web farm-based installation, see Installing the Web Components in Web Farm Configuration.)
   b. Choose the website under which to create the vCAC web application from the drop-down list.
   c. Select the transport protocol to use for vCAC: **HTTPS** or **HTTP**.

   **Note:** You must use the same transport protocol for all vCAC components. The default is HTTPS, which requires that all host names specified during the installation process be fully qualified domain names.
   
   d. For an HTTPS installation:
      • 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**.

- Specify the HTTPS port for the IIS site.
- Select a certificate from the drop-down list.

e. Click **Next**.

10. On the vCAC Database Configuration page:

a. Select **Use Windows Authentication** 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.

b. In the **SQL Database Server Instance** box, specify the database instance in the format `hostname\instance` name (or `hostname` if using the default instance), or accept the default value `localhost`.

c. In the **SQL Database Name** box, type the name of the database (default value is `DCAC`).

d. Click **Test Connection** to ensure that the credentials being used to connect to the database have the necessary permissions.

e. Click **Next**.

11. On the AzMan Authorization Store Selection page, select the type of AzMan authorization store you want to use.

- If you select **MSSQL Server store**, select **Create AzMan authorization store** to create the authorization store database. The authorization store must exist in order to install the Model Manager Data component. If you have already created the authorization store manually or during a previous run of the installer, leave this unselected. You only need to create the authorization store once for your deployment.

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

12. On the vCAC Email Configuration page:

a. Select **Enable SSL** to communicate with the email server using SSL.

b. In the **vCAC Website Hostname** box, 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 enter `vCAC-web-cluster.example.com` in this field, the base URL for email links is `http://vCAC-web-cluster.example.com/DCAC`.

c. In the **SMTP Server** box, specify the host name of the SMTP server.

d. In the **From Address** box, specify the email address that should appear in the From: field of vCAC notification emails (typically the domain administrator email).

e. If you do not want to use anonymous authentication with the SMTP server, clear the selection for **Use Anonymous SMTP Authentication** and specify the user credentials with which to authenticate with the SMTP server.

13. On the Model Manager Configuration page:

a. VMware recommends that you select **Use Default Log Location**. To specify an alternative location for the log directory, clear the check box.
b. Specify the host name of the Model Manager web service.

c. Specify the user credentials under which to run the Model Manager web service.

d. Click Next.

13. On the vCAC Web Portal Configuration page:
   a. VMware recommends that you select Use Default Log Location. To specify an alternative
      location for the log directory, clear the check box.
   b. Specify the user credentials under which to run the portal website.
   c. Click Next.

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

For information about setting up additional web servers, see About Installing Redundant Web Servers.

**Installing the Manager Service**

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 website in IIS
for use with vCAC, then proceed with the vCAC installation.

To install the Manager Service:

1. Install the vCAC Prerequisite Checker.
   a. Download the installer file, DCACPrereqCheckerInstaller.msi, from the VMware product
      page at http://www.vmware.com/products to the installation host.
   b. Open a command prompt as administrator and navigate to the directory containing the
      installer.
   c. Execute the installer and follow the steps in the installer wizard.

2. Run the vCAC Prerequisite Checker to verify the installation prerequisites.
   a. Navigate to the directory where the Prerequisite Checker is installed. Typically, this is
      %SystemDrive%\Program Files (x86)\DynamicOps\DCAC Prereq Checker.
   b. Right-click PrereqChecker.exe and select Run as administrator.
      The vCAC Prerequisite Checker launches.
   c. Under Core Install, select Manager Service and clear the check boxes for the other com-
      ponents, including those under Core Upgrade, DEM Install, and vCAC Self-Service Por-
      tal Install.
   d. 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.
      • From the Web site drop-down list, choose the name of the website under which you are
        creating the vCAC web application.
   e. Click Run Checker.
f. The Prerequisite Checker displays the list of requirements for the selected component and the status of each one.

g. 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.

h. Repeat Step f until all requirements are satisfied.

i. Exit the Prerequisite Checker.


4. Navigate to the directory containing the installer, right-click the installation executable and select Run as administrator.

5. On the Welcome page, click Next.

6. On the End-User License Agreement page, read the License Agreement, click I accept the terms in the License Agreement, then click Next.

7. On the vCAC License Configuration page, provide the full file path to your vCAC license file:
   a. Click Browse.
   b. Browse to the location of your vCAC license file (XML).
   c. Select the file and click Open.
   d. Click Next.

8. On the Custom Setup page, select Manager Service. Cancel the selection for all other features, then click Next.

9. On the IIS Site Bindings Configuration page:
   a. Leave Enable Web Farm Support unselected. (This option enables tracking of user session information in a shared session state database. For information about a web farm-based installation, see Installing the Web Components in Web Farm Configuration.)
   b. Choose the website under which to create the vCAC web application from the drop-down list.
   c. Select the transport protocol to use for vCAC: HTTPS or HTTP.

   **Note:** You must use the same transport protocol for all vCAC components. The default is HTTPS, which requires that all host names specified during the installation process be fully qualified domain names.

   d. For an HTTPS installation:
      - 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.
      - Specify the HTTPS port for the IIS site.
      - Select a certificate from the drop-down list.
On the vCAC Database Configuration page:

10. On the vCAC Database Configuration page:
   a. Select **Use Windows Authentication** 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.
   
   b. In the **SQL Database Server Instance** box, specify the database instance in the format `hostname\instancename` (or `hostname` if using the default instance), or accept the default value `localhost`.
   
   c. In the **SQL Database Name** box, type the name of the database (default value is `DCAC`).
   
   d. Click **Test Connection** to ensure that the credentials being used to connect to the database have the necessary permissions.
   
   e. Click **Next**.

11. On the AzMan Authorization Store Selection page, select the type of AzMan authorization store you want to use. This must be the same authorization store type that you selected when installing the web components.

   - If you select **MSSQL Server store**, leave **Create AzMan authorization store** unselected. (VMware recommends that you create the authorization store database when you install the Model Manager Data component). You only need to create the authorization store once for your deployment.
   
   - If you select **Active Directory store**, provide the Active Directory connection string to the authorization store that you previously created.

12. On the vCAC Service Configuration page:
   a. Select **Start Manager Service** to start the vCloud Automation Center service automatically when the installation completes.
   
   b. VMware recommends that you select **Use Default Log Location**. To specify an alternative location for the log directory, clear the check box.
   
   c. If you select **Disaster Recovery cold standby node**, the vCloud Automation Center service is installed in **Manual** startup mode rather than **Automatic**.
   
   d. Specify the user credentials under which to run the vCloud Automation Center service.
   
   e. Click **Next**.

13. On the Model Manager Configuration page:
   a. VMware recommends that you select **Check Model Manager Web Service host name** to force the installer to test connectivity to the Model Manager host before proceeding.
   
   b. Specify the **Model Manager Web Service Hostname**.
   
   c. For an HTTP installation, specify the **HTTP Port** on which the Model Manager service is listening. (In an HTTPS installation, the port specified on the IIS Site Bindings page is used.)

14. On the Ready to Install page, click **Install**.

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

Installing the DEM Orchestrator or Worker

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

To install the DEM:

1. Install the vCAC Prerequisite Checker.
   a. Download the installer file, DCACPrereqCheckerInstaller.msi, from the VMware product page at http://www.vmware.com/products to the installation host.
   b. Open a command prompt as administrator and navigate to the directory containing the installer.
   c. Execute the installer and follow the steps in the installer wizard.

2. Run the vCAC Prerequisite Checker to verify the installation prerequisites.
   a. Navigate to the directory where the Prerequisite Checker is installed. Typically, this is %SystemDrive%\Program Files (x86)\DynamicOps\DCAC Prereq Checker.
   b. Right-click PrereqChecker.exe and select Run as administrator.
      The vCAC Prerequisite Checker launches.
   c. 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.
   d. Click Run Checker.
   e. The Prerequisite Checker displays the list of requirements for the selected component and the status of each one.
   f. 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.
   g. Repeat Step f until all requirements are satisfied.
   h. Exit the Prerequisite Checker.

4. Navigate to the directory containing the installer, right-click the installation executable and select **Run as administrator**.

5. On the Welcome page, click **Next**.

6. On the End-User License Agreement page, read the License Agreement, click **I accept the terms in the License Agreement**, then click **Next**.

7. On the DEM Instance Configuration page:
   a. In the **DEM Instance Name** box, provide a name that uniquely identifies this instance in your deployment.
   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.
   d. Select **Use HTTPS** if you are installing vCAC to use HTTPS as the transport protocol.
   
   **Note:** You must use the same transport protocol for all vCAC components. The default is HTTPS, which requires that all host names specified during the installation process be fully qualified domain names.

   e. Click **Next**.

8. On the Custom Setup page, click **Next**.

9. On the Manager Service and Model Manager Web Service Host Configuration page:
   a. In the **Manager Service Hostname:Port** box, specify the host name of the Manager Service host and the port on which the DEM connects to the Manager Service. The port for HTTPS is typically 443; if using HTTP, the port is 9003.
   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 for HTTP is typically 443; if using HTTP, the default port is 80.
   c. Specify the user credentials under which the Model Manager web service is running.
   d. Click **Next**.

10. On the Service Configuration page:
    a. VMware recommends that you select **Register Distributed Execution Manager Service** to install the DEM as a Windows service.
    b. Select **Start Distributed Execution Manager Service** to start the DEM service automatically when the installation completes.
    c. Specify the user credentials under which to run the DEM service.
    d. Click **Next**.

11. On the Ready to Install page, click **Install**.
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 the following address: `https://vCAC_portal_hostname/DCAC`.
   Substitute `http://` for `https://` if you installed vCAC to use HTTP as the transport protocol.
2. When prompted, provide Windows credentials for a user with local administrator privileges on the Manager Service host.

   The vCAC Console loads.

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.

**Installation Troubleshooting**

When you execute the **DCAC-Manager-Setup.exe** file, a log file is generated on the system drive. The path is `%SystemDrive%\vcacLog\datestamp.log`, where *datestamp* indicates the date and time. If you have problems during installation you can consult this log and provide it to VMware support for assistance.

**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 green check mark to save.
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 clustered hosts: 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 selection for **Start Manager Service** and select **Disaster Recovery cold standby node**.
  b. Enter 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 Appendix 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.

The DEM Orchestrator 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. 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.

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 AzMan authorization store** on the AzMan Authorization Store Selection page; the store was created when you installed the first web server with the Model Manager Data component.

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:
   a. Select **Start > Administrative Tools > Services**.
   b. Stop any vCloud Automation Center Agent services (see Appendix 4), 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 within the cluster.

3. Activate the failover vCAC Server within the cluster.

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.
   a. Select **Start > Administrative Tools > Services**.
   b. Start the vCloud Automation Center service, the Distributed Execution Manager services and any vCloud Automation Center Agent services (see Appendix 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 as follows:

1. Create the session state database.
2. Prepare the authorization store if necessary.
3. Install the vCAC database.
4. Install the web components in web farm configuration.
5. Install the Manager Service, selecting Enable Web Farm Support on the IIS Site Bindings Configuration page.
6. Install the Distributed Execution Managers.

The installation procedures are the same as described for the non-web farm configuration except for installing the web components, described in Installing the Web Components in Web Farm Configuration.
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’s 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.

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`.

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. Download the `DBInstall.zip` file from the VMware product page at [http://www.vmware.com/products](http://www.vmware.com/products) to the database host and extract it to a local directory.
   b. 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')`.
   c. Open SQL Server Management Studio.
   d. Select the session state database under `Databases` in the left hand pane.
   e. Click **New Query**.
      A SQL Query window opens in the right hand pane.
   f. Paste the entire modified contents of `GrantAspSessionStateUserPermission.sql` into the query window.
   g. Click **Execute**.

Installing the Web Components in Web Farm Configuration

The web components of vCAC include the portal website and reports website as well as the Model Manager. The Model Manager consists of two installable components: Model Manager Web and Model Manager Data. Model Manager Data should only be installed on the first web cluster host.

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

To install the vCAC web components in web farm configuration:
1. **Install the vCAC Prerequisite Checker.**
   a. Download the installer file, `DCACPrereqCheckerInstaller.msi`, from the VMware product page at http://www.vmware.com/products to the installation host.
   b. Open a command prompt as administrator and navigate to the directory containing the installer.
   c. Execute the installer and follow the steps in the installer wizard.

2. **Run the vCAC Prerequisite Checker to verify the installation prerequisites.**
   a. Navigate to the directory where the Prerequisite Checker is installed. Typically, this is `%SystemDrive%\Program Files (x86)\DynamicOps\DCAC Prereq Checker`.
   b. Right-click `PrereqChecker.exe` and select **Run as administrator**.
      The vCAC Prerequisite Checker launches.
   c. Under **Core Install**, select **Website** and **Model Manager Web Services** and clear the check boxes for the other components, including those under **Core Upgrade**, **DEM Install**, and **vCAC Self-Service Portal Install**.
   d. If you are not installing the web components in the Default Web Site in IIS, specify the website to validate:
      - Click the **Settings** tab.
      - From the **Web site** drop-down list, choose the name of the website under which you are creating the vCAC web application.
   e. Click **Run Checker**.
   f. The Prerequisite Checker displays the list of requirements for the selected component and the status of each one.
   g. 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.
   h. Repeat Step f until all requirements are satisfied.
   i. Exit the Prerequisite Checker.

3. **Download the installer file, `DCAC-Manager-Setup.exe`, from the VMware product page at http://www.vmware.com/products to the installation host.**

4. Navigate to the directory containing the installer, right-click the installation executable and select **Run as administrator**.

5. On the Welcome page, click **Next**.

6. On the End-User License Agreement page, read the License Agreement, click **I accept the terms in the License Agreement**, then click **Next**.

7. On the vCAC License Configuration page, provide the full file path to your vCAC license file:
   a. Click **Browse**.
   b. Browse to the location of your vCAC license file (XML).
   c. Select the file and click **Open**.
d. Click **Next**.

8. On the Custom Setup page, select **Model Manager**, **Website**, and **Report.Website**. Cancel the selection for all other features, then click **Next**.

9. On the IIS Site Bindings Configuration page:
   a. Select **Enable Web Farm Support**.
   b. Choose the website under which to create the vCAC web application from the drop-down list.
   c. Select the transport protocol to use for vCAC: **HTTPS** or **HTTP**.

   **Note:** You must use the same transport protocol for all vCAC components. The default is HTTPS, which requires that all host names specified during the installation process be fully qualified domain names.

   d. For an HTTPS installation:
      - 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**.
      - Specify the HTTPS port for the IIS site.
      - Select a certificate from the drop-down list.
   e. Click **Next**.

10. On the vCAC Database Configuration page:
    a. Select **Use Windows Authentication** 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.
    b. In the **SQL Database Server Instance** box, specify the database instance in the format `hostname\instancename` (or `hostname` if using the default instance), or accept the default value `localhost`.
    c. In the **SQL Database Name** box, type the name of the database (default value is `DCAC`).
    d. Click **Next**.

11. On the AzMan Authorization Store Selection page, select the type of AzMan authorization store you want to use.
    - If you select **MSSQL Server store**, select **Create AzMan authorization store** to create the authorization store database. The authorization store must exist in order to install the Model Manager Data component. You only need to create the authorization store once for your deployment.
    - If you select **Active Directory store**, provide the Active Directory connection string to the authorization store that you previously created.

12. On the vCAC Email Configuration page:
    a. Select **Enable SSL** to communicate with the email server using SSL.
b. In the vCAC Website Hostname box, 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 enter vCAC-web-cluster.example.com in this field, the base URL for email links is http://vCAC-web-cluster.example.com/DCAC.

c. In the SMTP Server box, specify the host name of the SMTP server.

d. In the From Address box, specify the email address that should appear in the From: field of vCAC notification emails.

e. If you do not want to use anonymous authentication with the SMTP server, clear the selection for Use Anonymous SMTP Authentication and specify the user credentials with which to authenticate with the SMTP server.

13. On the Model Manager Configuration page:

   a. VMware recommends that you select Use Default Log Location. To specify an alternative location for the log directory, clear the check box.

   b. Specify the host name of the Model Manager web service.

   c. Specify the user credentials under which to run the Model Manager web service.

   d. Click Next.

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

   **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.
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. The following sections describe 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 What's New Guide.

For information about general DEM prerequisites, see Chapter 2. 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, HTTP and 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 What’s New Guide What’s New 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 PowerShell command prompt:

```
help about_signing
help Set-ExecutionPolicy
```
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.
### 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:

<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.
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’s 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
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, DCAC Agents\agentname, under the vCAC install directory (typically %SystemDrive%\Program Files (x86)\DynamicOps), 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](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>Inventory</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>Virtual Machine</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>
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:

<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></td>
<td>Rename</td>
<td>Rename</td>
</tr>
<tr>
<td></td>
<td>Add Existing Disk</td>
<td>Add Existing Disk</td>
</tr>
<tr>
<td></td>
<td>Add New Disk</td>
<td>Add New Disk</td>
</tr>
<tr>
<td></td>
<td>Remove Disk</td>
<td>Remove Disk</td>
</tr>
<tr>
<td></td>
<td>Change CPU Count</td>
<td>Change CPU Count</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td>Memory</td>
</tr>
<tr>
<td></td>
<td>Add or Remove Device</td>
<td>Add or Remove Device</td>
</tr>
<tr>
<td></td>
<td>Settings</td>
<td>Settings</td>
</tr>
<tr>
<td></td>
<td>Change Resource</td>
<td>Change Resource</td>
</tr>
<tr>
<td></td>
<td>Advanced</td>
<td>Advanced</td>
</tr>
<tr>
<td></td>
<td>Swap Placement</td>
<td>Swap Placement</td>
</tr>
<tr>
<td></td>
<td>Modify Device Settings</td>
<td>Modify Device Settings</td>
</tr>
<tr>
<td></td>
<td>Disk Change Tracking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set Annotation (5.0 and 5.1 only)</td>
<td></td>
</tr>
<tr>
<td>Provisioning</td>
<td>Customize</td>
<td>Customize</td>
</tr>
<tr>
<td></td>
<td>Clone</td>
<td>Clone</td>
</tr>
<tr>
<td></td>
<td>Deploy Template</td>
<td>Deploy Template</td>
</tr>
<tr>
<td></td>
<td>Read Customization Specs</td>
<td>Read Customization Specs</td>
</tr>
<tr>
<td>State</td>
<td>Create Snapshot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remove Snapshot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Revert to Snapshot</td>
<td></td>
</tr>
<tr>
<td>Resource</td>
<td>Assign VM to Res Pool</td>
<td>Assign VM to Res Pool</td>
</tr>
<tr>
<td></td>
<td>Migrate</td>
<td>Migrate</td>
</tr>
<tr>
<td>Permissions</td>
<td>Modify Permission</td>
<td>Modify Permission</td>
</tr>
<tr>
<td></td>
<td>Assign Network</td>
<td></td>
</tr>
</tbody>
</table>
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, enter 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.
- Optionally, 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. Enter the following command

     ```
     mfreg.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
  ```

  For PVS 5.6, see:

  ```
  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 13  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:

  ```
  %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:

  ```
  $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 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 green "go" icon to save the credentials. Select them and click **OK** to return to the New Endpoint page.

6. Click the green "go" icon to save the endpoint.

7. Repeat this procedure for all the needed endpoints.

### Installing a vCAC Agent

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

1. Download the installer file, **DCAC-Agent-Setup.exe**, from the VMware product page at http://www.vmware.com/products to the installation host.

2. Navigate to the directory containing the installer, right-click the installation executable 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 5 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. If vCAC was installed to use HTTPS, select **Use HTTPS as transport protocol**.

   **Note:** You must use the same transport protocol for all vCAC components. The default is HTTPS, which requires that all host names specified during the installation process be fully qualified domain names.

   c. In the **vCloud Automation Center Hostname:Port** box, specify the host name and port of the vCAC Server. The default port is 443 for HTTPS, 80 for HTTP.

   d. 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 for HTTPS, 80 for HTTP.

   **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)\DynamicOps\DCAC Agents) 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 creden-
tials; 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)\DynamicOps\DCAC 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.

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 also 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 DCAC-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.

```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=CoreAgent,vSphere-Agent
VSPHERE_AGENT_ENDPOINT=Vc1Endpoint MSINWINSTANCE=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)\DynamicOps\DCAC 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 14  Proxy Agent Configuration Properties**

<table>
<thead>
<tr>
<th>property</th>
<th>description</th>
</tr>
</thead>
<tbody>
<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 vCAC and vCAC Agents

If the vCAC installer detects an existing DCAC release 4.5 instance installed on the host, it automatically upgrades that instance to version 5.1. This automated upgrade process retains all existing configuration information.

The upgrade process does not, however, upgrade the existing database or the existing vCAC agents. The database must be upgraded before the vCAC instance is upgraded, and the agents after.

| Note: | The automated vCAC upgrade process is intended only for existing DCAC 4.5 instances upgrading to version 5.1. To upgrade from DCAC 4.1, first upgrade to 4.5 as described in the DCAC 4.5 Installation Guide. Earlier versions of Virtual Resource Manager (VRM) cannot be upgraded to vCAC. Contact your VMware support representative for more information and assistance. |

Change to Default Transport Protocol

In release 5.1, the default transport protocol when installing vCAC is HTTPS. VMware recommends using HTTPS to ensure secure communication between components.

If you are upgrading an existing installation that used HTTP, the transport protocol remains HTTP after upgrade for the core components, DEMs, and agents.

To upgrade other components, such as the extensibility toolkits, the Bulk Operations Client, and the Self-Service Portal, you must uninstall the existing version and install the new version, ensuring that you select the same transport protocol that was used for the upgraded components.

Overview of the vCAC Upgrade Process

To upgrade an existing DCAC 4.5 instance to release 5.1, you must take the following steps in this order:

1. Allow all current machine provisioning and disposing operations to complete.
2. Make a snapshot or full backup of all systems hosting vCAC components.
3. Verify that you are upgrading from DCAC 4.5.
4. Verify the names and hosts of all installed Distributed Execution Managers (DEMs) and proxy agents.
5. Stop all DCAC services on the Manager Service host and all DEM and proxy agent hosts.
6. Identify and back up the existing DCAC database in SQL Server.
8. Use the provided upgrade scripts to upgrade the existing DCAC database.
9. Determine the user name under which the DCAC report service is running.
10. Verify that release 5.1 prerequisites are met on each installation host.
11. Use the vCAC installer to upgrade all DCAC components.
12. Use the DEM installer to upgrade existing DEMs.
13. Use the vCAC agent installer to upgrade existing agents.
14. Update the license if appropriate.
15. Restart the upgraded Manager Service and agent and DEM services.
16. Start the vCAC Console.
17. Perform required post-upgrade steps as described in this guide.

Allow Machine-Related Operations to Complete

Ensure that all machine provisioning, reprovisioning, and disposing (destroying/decommissioning) operations have been completed and that no further machine-related operations will be initiated until upgrade is complete.

Back Up DCAC Component Hosts

VMware recommends that you make a snapshot or a full backup of each DCAC 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.

Verify the Current DCAC Version

Verify the version of the currently installed DCAC instance by selecting the About link in the upper right of the DCAC console. The version displayed must be 4.5 Build 81.

Verify DEM and Agent Information

After vCAC is upgraded, all existing DEMs and agents must be upgraded. You should have information about all DEM and agent instances and their hosts, but it is a good idea to verify this information.

To verify the names and hosts of existing DEMs, start the DCAC Console as a user in the DCAC Administrator role and select DCAC Administrator > Distributed Execution Status (see the vCloud Automation Center Operating Guide for more information). When you later run the DEM installer on each of the DEM hosts and choose Upgrade, the installer lists the currently installed DEMs that can be upgraded.

To verify the names of existing DCAC agents, select Start > Administrative Tools > Services on the DCAC server and on any other host on which agents may be installed and note each VMware vCloud Automation Center Agent – agentname service that is running. When you later run the agent installer on that host and choose Upgrade, these agent names are listed.

Stop DCAC Services

To stop the DCAC services, first log into all DEM and agent hosts other than the DCAC Server (Manager Service host), and then the DCAC Server, as a user with full administrative access, select Start > Administrative Tools > Services and stop the following services:

- Each VMware vCloud Automation Center Agent – agentname service
Each VMware DEM-role - instancename service
• The VMware vCloud Automation Center service (DCAC Server only)

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

### Identify and Back Up the DCAC Database

To identify and back up the current DCAC database:

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

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

3. Make a backup of the current DCAC 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 in which they cannot be accidentally destroyed.

### Back Up Active Directory–based AzMan Store

If you are using an Active Directory–based authorization store, create a backup before proceeding with the upgrade. See the Microsoft documentation for details.

### Upgrade the Database

To upgrade the existing DCAC database to vCAC 5.1, follow these procedures to

- Extract the upgrade files
- Upgrade the database

### Extracting the Upgrade Files

The vCAC 5.1 installation file **DBUpgrade.zip** contains the files required to upgrade the existing vCAC database. Extract its contents to the database host or to another location with network access to the database host.

### Upgrading the Database

Execute the program **DBUpgrade.exe** to upgrade your database.
The **DBUpgrade.exe** program takes as arguments the SQL Server instance and name of the vCAC database and either a flag to use Windows authentication to access the database or credentials to do so. An optional argument indicates the path to the log file for the operation (by default it is **dbupgrade.log** in the same directory). Run the program with no arguments to display this usage information:

```
DBUpgrade {-S sql_instance} {-d dbname} {-E || {-U sql_login -P login_password}} [-l upgrade_logfile]
```

Use `-E` for trusted connection (using Windows Authentication)

Use `-l` to specify full path name to upgrade log file. Otherwise dbupgrade.log is assumed.

For example, to update the database **DCAC** in the default SQL Server instance on the local host, using your current Windows credentials for authentication and authorization, you would issue the command

```
DBUpgrade –S localhost –d DCAC –E
```

To update the database **DCAC45** in the SQL Server instance **DCACInstance** on host **dbhost**, using SQL authentication and a nondefault location for the log file, you would issue the command

```
DBUpgrade –S dbhost\DCACInstance –d DCAC45 –U SqlUser
   –P SqlPassword –l %SystemDrive%\DCACDBUpgrade\DCACDBUpgradeLog_31Dec.log
```

Your database is now upgraded to vCAC 5.1.

**Determine the Report Service Username**

Unlike other configuration information, the credentials under which the DCAC report service is running in the existing instance cannot be obtained by the vCAC installer. To obtain the username, select **Application Pools** within IIS and make a note of the **Identity** shown for **DcacReportAppPool**, as shown:
Verify Installation Prerequisites

Verify that release 5.1 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.

To verify prerequisites before upgrading vCAC:

1. Install the vCAC Prerequisite Checker.
   a. Download the installer file, DCACPreqCheckerInstaller.msi, from the VMware product page at http://www.vmware.com/products to the installation host.
   b. Open a command prompt as administrator and navigate to the directory containing the installer.
   c. Execute the installer and follow the steps in the installer wizard.
2. Navigate to the installation directory. Typically, this is %SystemDrive%\Program Files (x86)\DynamicOps\DCAC Prereq Checker.
3. Right-click PrereqChecker.exe and select Run as administrator.
   The vCAC Prerequisite Checker launches.
4. Under Core Install, select the components that you are upgrading on the current host.
5. If you are upgrading the Model Manager, select CDK Workflows under Core Upgrade.
   If you are running the Prerequisite Checker on a different host from the Model Manager Web service host, specify the Model Manager host name and port under ModelManagerWeb settings.
6. If you are upgrading a DEM instance, select DEM under Core Upgrade.
7. If you are not installing the web components in the Default Web Site in IIS, specify the website to validate:
   a. Click the Settings tab.
   b. From the Web site drop-down list, choose the name of the website under which you are creating the vCAC web application.

8. Click **Run Checker**.
   The Prerequisite Checker displays the list of requirements for the selected component and the status of each one.
   If you selected **CDK Workflows**, the Prerequisite Checker displays a list of the customizable workflows and whether each one has been modified using vCAC Designer. You have the option to preserve the latest versions of your customized workflows when you upgrade.

9. 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.

10. Repeat Step 7 until all requirements are satisfied.

11. Exit the Prerequisite Checker.

### Upgrade vCAC

To upgrade the existing DCAC instance to vCAC 5.1, use the following procedure.

---

**Caution:** The DCAC database must be backed up and then upgraded using the instructions provided before the DCAC instance is upgraded.

---

1. Run the vCAC installer as instructed in Installing the vCAC Server in Chapter 3.

2. Following the End-User License Agreement page, the message “If you have custom events linked to a pre-installed model, they will need to be reapplied post upgrade.” appears.

   Custom events are created using the vCloud Automation Center Development Kit. If you have custom events that depend on the core Management Model entities, take steps described in Appendix A to reapply them after upgrading. If you are unsure whether this applies to you, contact VMware support.

   Click **OK** to continue with the upgrade process.

3. The installer detects that there is an existing installation of vCAC on the host and indicates the components that are installed and will be upgraded.
Note: If your vCAC components are installed on more than one host, run the installer on each host in turn, starting with the systems hosting the web components.

If the Model Manager components are installed, the Preserve my latest workflow versions check box appears. If you have used Design Center to customize workflows in the Model Manager, as described in the vCloud Automation Center Extensibility Guide, select this option to maintain the most recent version of each customized workflow before upgrade as the most recent version after upgrade. If you do not select this option, the version of each workflow provided with vCAC 5.1 becomes the most recent after upgrade, and the most recent version before upgrade becomes the second most recent. (Note that customized workflows are always preserved; the checkbox determines version order only.)

Note: If you are upgrading to vCloud Automation Center release 5.1 from release 4.5 and the release 4.5 version of Design Center is installed, the latter will no longer be functional after upgrade. You must uninstall it and install the release 5.1 version as described in Appendix A.

Note that the Model Manager Data component is not necessarily upgraded when you upgrade the host on which it is installed, but rather when you upgrade the host on which the Manager Service is installed. In configurations such as HA mode (see Installing in High Availability Mode in Chapter 3) in which the Manager Service is installed on more than one host, ensure that the Model Manager Data component is upgraded only once.

4. When you upgrade the Manager Service, use the Service Configuration page to enter the credentials to be used by the Manager Service. These credentials must have administrative access to the local machine and belong to the Windows Authorization Access group in all domains containing users to be authorized by vCAC. The username under which the Manager Service is cur-
rently running is already entered when the page is displayed, but you can change credentials if you wish.

![vCloud Automation Center](image)

**Note:** If you are uncertain about the requirements for these credentials, review Users and Credentials Required for vCAC Services in Chapter 2.

5. When upgrading the portal website, use the Web Portal Configuration page to enter the credentials to be used by the portal web service. The username under which the portal web service is
6. When upgrading the Model Manager Web service, use the Model Manager Configuration page to enter the credentials to be used by the Model Manager Web service. The username under which the Model Manager Web service is currently running is already entered when the page is displayed, but you can change credentials if you wish.

7. On the Ready to Install page, click **Install**.
Caution: There is no way to cancel the upgrade after you click Install.

The upgrade process does not start the Manager Service. Do not restart it until after you have upgraded the existing DEMs and vCAC agents as described below.)

Note: All existing authorization information and the existing configurations of the Manager Service, website, and reports website are preserved in the upgraded vCAC instance. Copies of the pre-upgrade configuration files are preserved for your reference in the vCAC server installation directory (typically %System-Drive%\Program Files (x86)\DynamicOps\DCAC Server) as follows:

ManagerService.exe.config.bak
Website\Web.config.bak
Report.\Website\Web.config.bak

However, any customizations applied to the basic user interface on the UI Customization tab of the vCAC Administrator > Customization activity (see the vCloud Automation Center Operating Guide) are lost following upgrade.

Upgrade Distributed Execution Managers

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

To upgrade Distributed Execution Managers:

1. Run the vCAC DEM installer as described in Installing the DEM Orchestrator or Worker in Chapter 3.
2. On the vCAC DEM Upgrade page, select Upgrade.
3. On the DEM Upgrade page, select a DEM instance to upgrade.
4. On the Service Configuration page, specify the credentials for the DEM user. The username under which the agent service is currently running is already entered when the page is displayed, but you can change credentials.
5. On the Ready to install page, click Install.
6. Repeat this procedure for each DEM instance in your vCAC deployment.

Upgrade vCAC Agents

The vCAC agent installer detects existing agents on the installation host and gives you the option of upgrading them.

To upgrade existing agents:

1. Run the vCAC agent installer as instructed in Installing a vCAC Agent in Chapter 4.
2. Following the End-User License Agreement page, the installer confirms that there are existing vCAC agents on the host. Select **Upgrade** and click **Next**.

3. The agent installer lists all existing agents by name. Select the agent you want to upgrade and click **Next**.

![vCAC Agent Upgrade](image)

![Agent Upgrade](image)
4. Use the Service Configuration page to enter the credentials to be used by the agent service. This user must have administrative access to the local machine. The username under which the agent service is currently running is already entered when the page is displayed, but you can change credentials or select Use Local System Account to use your current Windows credentials.

**Note:** For VDI and EPI agents, the user must have administrative access to all VDI servers or EPI with which the agent will interact. If you are uncertain about the requirements for these credentials, review vCAC Agent Installation Location and Requirements in Chapter 4.

5. Click **Install** on the next page to upgrade the agent.

6. Repeat this procedure for all existing agents.

The upgrade process does not start agent services. Do not restart them until after you have restarted the Manager Service.

The existing agent configurations are preserved in the upgraded agents. Copies of the pre-upgrade configuration files are preserved for your reference in the agent directories, under the name `VRMAgent.exe.config.bak`.

**Update the vCAC License**

If you have a new vCAC license, follow the instructions in Updating Your vCAC License in Chapter 6 to replace your existing license with the new license.
Restart the Manager, DEM and Agent Services

To restart all vCAC services, first log into the vCAC server (Manager Service host), and then all DEM and agent hosts other than the vCAC server, as a user with full administrative access, select **Start > Administrative Tools > Services**, and click the **Start** link for the following:

- The VMware vCloud Automation Center service (Manager Service host only)
- Each VMware DEM-*InstanceName* service
- Each VMware vCloud Automation Center Agent – *agentname* service

Start the Console

Once all the services are running after upgrade, 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 website data**.

   d. Click **Delete**.

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

2. Navigate to the following address: **https://vCAC_portal_hostname/DCAC**.

   Substitute **http://** for **https://** if you installed vCAC to use HTTP as the transport protocol.

3. When prompted, provide your Windows credentials.

   The vCAC Console loads.

Post-Upgrade Steps

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

Initiate Data Collection

Your upgraded vCAC instance is not fully operational until the first post-upgrade data collection for each of the compute resources and endpoints under vCAC management is completed.

Once the agent services are started, follow these steps:

1. Log in to the vCAC Console as an enterprise administrator.
2. Select **Enterprise Administrator > Compute Resources** to list all known virtualization hosts that belong to the enterprise groups of which you are administrator.

3. For each compute resource:
   a. Point to the name of the compute resource and click **Data Collection**.
   b. In the **Inventory** section, click **Request Now** to initiate inventory data collection.
   c. In the **State** section, click **Request Now** to initiate state data collection.

4. If your hosts belong to multiple enterprise groups with different administrators, repeat the above steps for each enterprise administrator.

5. Log in to the vCAC Console as a vCAC administrator.

6. Select **vCAC Administrator > Endpoints** to list all known endpoints.

7. For each Dell iDRAC, HP iLO, Cisco UCS Manager, and Amazon EC2 endpoint, select the **Data Collection** option to start data collection, and click **Start** to initiate data collection.

Alternatively, you can wait for the next scheduled (usually daily) data collection from all managed hosts and endpoints to be completed.

### Verify Email Settings

In previous releases, configuration (such as SMTP server information) for sending emails from vCAC was managed in several locations, including the Manager Service configuration and Distributed Execution Manager configuration. Beginning in release 5.1, email configuration is managed in global properties.

The SMTP server and email from address specified in the Manager Service configuration from 4.5 are carried over to the new global properties during upgrade. Any base URL for email links that was specified in the Manager Service configuration is also preserved; if no value was present in the 4.5 configuration, then the Manager Service host name is used. You should verify that the settings for emails are correct after upgrading. Pay particular attention to the value of the Website URI if you are upgrading a distributed environment.

To verify email settings after upgrading to 5.1:

1. Log in to the vCAC Console as a vCAC administrator.

2. Click **vCAC Administrator > Global Properties**.

3. Review the values for the properties under **Group: Email** and **Group: Installation**.

4. If any of the values are not correct, edit them as follows:
   a. Click the pencil icon next to the name of the property.
   b. Specify the value of the property.
   c. Click the green check mark to save.
   d. After you have saved all the properties that need editing, restart the vCloud Automation Center service.

---

**Note:** If you have customized any email templates that use the **ServiceUriBase** parameter, you should update your templates to use the new **WebsiteURI**.
parameter, which is based on the Website URI global property. For more information, see the vCloud Automation Center What’s New Guide.

**Rebuild WinPE Image**

In release 5.1, the VirtualMachineAdmin.EncryptPasswords custom property is no longer required when you select the Encrypt checkbox on a custom property. If you use vCAC for WIM-based provisioning, you must regenerate your WinPE image in order to take advantage of this change.

- **Note:** Rebuilding a WinPE image is not required to use vCAC 5.1. If you do not update your WinPE image, you must continue to use the VirtualMachineAdmin.EncryptPasswords property when you want to encrypt a custom property.

To update your vCAC for the encryption changes:

1. Update the guest agent in your WinPE image using one of the following methods:
   - Install the 5.1 WinPEBuilder utility and generate a new ISO file.
   - Insert the 5.1 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 VirtualMachineAdmin.EncryptPasswords property. This property has no effect if you are using a 5.1 WinPE image.

**Enable Amazon EC2 Reservations**

If you use vCAC to manage Amazon EC2 reservations, you must re-enable them after upgrading.

To re-enable Amazon EC2 reservations:

1. Start the vCAC console as a user in the enterprise administrator role.
2. Select Enterprise Administrator > Reservations.
3. Point to the name of a cloud reservation and click Edit.
4. On the Reservation Information tab, select Enabled.
5. On the Resources tab, select one or more security groups from the Security groups list.
6. Click OK.
Chapter 6 Uninstalling and Reinstalling vCAC Components

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

Uninstalling vCAC

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. Stop vCAC services on all agent and DEM hosts and the Manager Service host by logging in as a user with administrative privileges, then selecting Start > Administrative Tools > Services. First stop all VMware vCloud Automation Center Agent services, then all VMware DEM services, and finally the VMware vCloud Automation Center service.

2. Use Control Panel > Uninstall or change a program to uninstall vCAC components from the hosts on which they are installed.

About Reinstalling vCAC

The following restrictions apply to reinstalling the same version of vCAC that you have previously uninstalled. For information about upgrading to a new version of vCAC, see Chapter 5.

If you reinstall the Manager Service while continuing to use the same vCAC database, you must do the following or reinstallation will fail:

- Do not select the Model Manager Data feature on the Custom Setup page.
- On the AzMan Authorization Store Selection page, select the same type of authorization store you selected when the Model Manager was first installed.

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)\DynamicOps\DCAC 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**

vCAC is distributed with a temporary 90-day evaluation license. To obtain a permanent vCAC license, contact your VMware customer representative. See the *vCloud Automation Center Operating Guide* for detailed information about licenses.

Please contact VMware Customer Support for all license-related queries and problems.

**Updating Your vCAC License**

You must provide the location of a valid vCAC license when installing vCAC. The vCAC installer places a copy of this license file in the vCAC Server installation directory (typically `%SystemDrive%\Program Files (x86)\DynamicOps\DCAC Server`) and renames it `lic.xml`.

To update your license:

1. Copy the new license file to the location of the existing license, with the same name—that is, `vCAC_server_install_directory\lic.xml`—overwriting the existing license.

   **Note:** Do not delete the existing license first.

   Once you have replaced the license file as above, vCAC automatically detects the new license file and updates your license.

2. If your previous license was invalid or expired, you must reload the license after updating the license file.
   a. Start the vCAC console as a user in the vCAC administrator role.
   b. Select `vCAC Administrator > License Info`.
   c. Click `Reload License`.
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.

There are two installer options for the extensibility toolkits. Choose only one of the following depending on your situation:

<table>
<thead>
<tr>
<th>Installer Executable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<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>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>

**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 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 must be installed.

**Installing vCloud Automation Center Designer**

To install vCAC Designer:

1. Download the installer file, DesignCenter-Setup.exe, from the VMware product page at http://www.vmware.com/products to the installation host.
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 End-User License Agreement page, read the License Agreement, click I accept the terms in the License Agreement, then click Next.

4. On the Custom Setup page, click Next.

5. On the Model Manager Web Service Hostname page:
   a. If the Model Manager Web component was installed to use HTTPS, select Use HTTPS and specify the fully qualified domain name.

   **Note:** You must use the same transport protocol for all vCAC components. The default is HTTPS, which requires that all host names specified during the installation process be fully qualified domain names.

   b. 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. The default port for HTTP is 80; if using HTTPS, change the port to the HTTPS port, typically 443.

   c. Specify the user credentials under which the Model Manager is running.

   d. 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.

6. 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.

**Note:** If you have 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. Download the installer file, **CDK-Setup.exe**, from the VMware product page at http://www.vmware.com/products to the installation host.

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 End-User License Agreement page, read the License Agreement, click I accept the terms in the License Agreement, then click Next.

4. On the License Configuration page, provide the full file path to your vCAC Development Kit license file (XML), or use Browse to select the license file. For more information or to obtain a vCAC Development Kit license, contact your VMware representative.

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 Addin to also install the Workflow Generator Visual Studio plugin.

   **Note:** The Visual Studio 2010 Addin option cannot be selected if the installer determines that Visual Studio 2010 is not installed.

   If the Visual Studio 2010 Addin option does not appear on the Custom Setup page at all, the license that you provided on the previous page is not valid for vCAC Development Kit, and the installer only offers the basic vCloud Automation Center Designer functionality. Contact VMware support for assistance with your vCAC Development Kit license.

6. On the Model Manager Web Service Hostname page:

   a. If the Model Manager Web component was installed to use HTTPS, select Use HTTPS and specify the fully qualified domain name.

      **Note:** You must use the same transport protocol for all vCAC components. The default is HTTPS, which requires that all host names specified during the installation process be fully qualified domain names.

   b. 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. The default port for HTTP is 80; if using HTTPS, change the port to the HTTPS port, typically 443.

   c. Specify the user credentials under which the Model Manager is running.

   d. 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.

**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)\DynamicOps\Design Center\Addin\Templates\version\DynamicOps.Cdk.Activities.dll` and click **OK**.
7. Repeat step 5 for **DynamicOps.Repository.dll**.
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)\DynamicOps\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:

```xml
<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 instance</td>
</tr>
<tr>
<td></td>
<td>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 instance</td>
</tr>
<tr>
<td></td>
<td>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:

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

<listeners>
  <add name="LogFileListener" ... fileName="%APPDATA%\VMware\vCloud Automation Center Designer\Logs\CloudUtil_All.log" ... />
```
...<\/listeners>
...
</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\DynamicOps\Design Center\AssemblyCache`.
3. Install the version of vCAC Designer or the vCloud Automation Center Development Kit that matches the version of your vCAC instance.

**Restoring Custom Events**

If you used the vCloud Automation Center Development Kit to install custom events that depend on the core Management Model entities, they are not preserved in an upgrade, and you must restore the events after upgrading.

*Note:* This procedure only applies to events that depend on the core data models, not events that depend on custom data models. If you are unsure whether your custom events are affected, contact VMware support.

To restore custom events:
1. Upgrade the extensibility toolkits as described in Appendix A.

2. Locate the event configuration files that you created in the previous version of vCAC.

3. From a command prompt on the vCAC Designer host, navigate to the vCAC Designer installation directory.

4. Issue the following command for each event that you need to restore:

   CloudUtil.exe Events-Install -c Event-Name.xml