

vCloud Automation Center KVM (RHEV) Integration Guide

vCloud Automation Center 5.2

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

EN-001226-00

vmware[®]

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Copyright © 2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

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

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

Contents

About This Book 1

1 Planning for KVM (RHEV) Integration 3

About VMware vCloud® Automation Center™ 3

About Red Hat Virtualization 4

KVM (RHEV) Endpoints 4

Gathering Information About KVM (RHEV) Resources 4

Planning vCAC User Groups and Policies 5

Global Administrators 5

Provisioning Groups and Users 5

KVM (RHEV) Compute Resources, Enterprise Groups, and Virtual Reservations 5

Approval Policies 6

The KVM (RHEV)-Based Provisioning Process 6

2 Adding KVM (RHEV) Resources to vCAC 7

Required KVM (RHEV) Configuration 7

DEM Worker 7

Enabling Remote WMI Requests on Windows Machines 7

Specifying User Credentials for KVM (RHEV) 8

Creating and Importing a KVM (RHEV) Endpoint 8

Creating a KVM (RHEV) Endpoint 8

Importing a KVM (RHEV) Endpoint 9

Starting Endpoint Data Collection Manually 9

Creating an Enterprise Group 10

Managing Machine Prefixes 10

Standards for Host Names 11

Machine Name Limitations in vCAC 11

Creating and Managing Machine Prefixes 11

Managing Provisioning Groups 11

Creating a Provisioning Group 11

Viewing, Deleting, and Editing Provisioning Groups 13

About Reservations 14

Creating a KVM (RHEV) Reservation 15

Viewing, Deleting, and Editing Reservations 17

3 Creating Blueprints for KVM (RHEV) 19

- Custom Properties for KVM (RHEV) Integration 19
- Workflows 21

- Creating a Basic KVM (RHEV) Blueprint 21

 - Preparing for WIM-Based Provisioning with VirtIO drivers 24

- Creating a Clone KVM (RHEV) Blueprint 24

 - Creating a Template to Provision by Cloning Within RHEV 25

 - Creating a KVM (RHEV) Blueprint for Provisioning by Cloning 26

4 Optional Configuration 29

- Configuring Approvals 29

 - Creating a New Approval Group 30

 - Creating a New Approval Policy 31

- Creating a Reservation Policy 32

 - Assigning a Reservation Policy to a Reservation 32

 - Assigning a Reservation Policy to a Blueprint 32

 - Viewing the Reservations Belonging to a Reservation Policy 33

- About Storage Reservation Policies 33

 - Creating a Storage Reservation Policy 34

 - Assigning Storage Reservation Policies to a Compute Resource 34

- Creating Build Profiles 34

5 Managing KVM (RHEV) Machines 37

- Connecting to a KVM (RHEV) Machine's Console 37

About This Book

The *vCloud Automation Center KVM (RHEV) Integration Guide* provides information about provisioning and managing virtual machines by using VMware vCloud® Automation Center™. It describes how to configure vCloud Automation Center (vCAC) and set up provisioning with Red Hat Enterprise Virtualization (RHEV). It covers:

- Bringing RHEV resources under management by vCAC
- Creating blueprints for provisioning with RHEV

Before configuring vCAC and setting up provisioning with RHEV, you must:

- Install vCAC in a development or production environment. For detailed instructions about installing vCAC, see the *vCloud Automation Center Installation Guide*.
- Install a supported version of RHEV. For detailed instructions about installing RHEV, see the Red Hat Enterprise Virtualization documentation.
- Prepare virtual machine images or templates and verify that all of the prerequisites for the provisioning methods you are planning to use are met. For information about supported provisioning methods, refer to the *vCloud Automation Center Support Matrix*.

Intended Audience

This book is intended for anyone who wants to configure vCAC and set up provisioning with RHEV. The information in this book is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation go to <http://www.vmware.com/support/pubs>.

Document Feedback

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

Technical Support and Education Resources

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

Online and Telephone Support

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

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

Support Offerings

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

VMware Professional Services

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

Chapter 1 Planning for KVM (RHEV) Integration

1

VMware vCloud® Automation Center™ works with the KVM (RHEV) virtualization platform to provision and manage the virtual machines created by that platform and the virtualization compute resources they are created on.

About VMware vCloud® Automation Center™

VMware vCloud® Automation Center™ provides an enterprise-wide system for provisioning virtual, cloud and physical machines. It allows you to manage the machine life cycle from user request and administrative approval through decommissioning and resource reclamation, while improving resource cost control and management. Built-in customization and extensibility features also make vCloud Automation Center a highly flexible means for customizing machine configurations as needed and integrating machine provisioning and management with other enterprise-critical systems.

A virtual machine is a server, workstation, desktop, or other computer system implemented entirely in software, using resources provided by one or more hardware systems. Virtualization allows an enterprise to provide users with the systems they need without having to individually procure, transport, build, install and configure hardware systems and the software deployed on them. The benefits of virtual machine provisioning include:

- Users get exactly the machines they need faster and with less overhead
- Users can roll back to start fresh whenever they need to
- Provisioning capacity is as scalable as underlying hardware resources
- Fewer person-hours are devoted to installing and configuring physical systems
- Hardware resources are used more efficiently, with faster provisioning and dynamic workload rebalancing making data centers more agile
- Hardware remains under the direct control of data centers personnel for more manageable security, maintenance, update, repair, and backup/restore
- Remote users access data sources using local hardware, improving performance
- Compliance with regulatory, corporate, and other enterprise computing requirements is easier
- User workspaces are improved by the removal of unnecessary hardware

For information about installing vCAC, see the *vCloud Automation Center Installation Guide*. For detailed information about virtual machine life cycle, the different types of provisioning, preparing for provisioning, and provisioning with vCAC, see the *vCloud Automation Center Operating Guide*.

About Red Hat Virtualization

Red Hat® Enterprise Virtualization (RHEV) is an enterprise virtualization product produced by Red Hat Inc. RHEV builds on the Kernel-based Virtual Machine (KVM) hypervisor and the oVirt open virtualization management platform.

For more information about Red Hat Enterprise Virtualization, see the [Red Hat Enterprise Virtualization documentation](#).

KVM (RHEV) Endpoints

By using the KVM (RHEV) integration in vCAC users can provision virtual machines in a RHEV environment. You can map a vCAC endpoint to a RHEV environment and collect data on the compute resources (KVM hosts).

Gathering Information About KVM (RHEV) Resources

To provision virtual machines with vCAC, you must create a KVM (RHEV) endpoint so that vCAC can collect data about the compute resources.

The KVM (RHEV) compute resources are hosts or clusters within the RHEV environment. Making the KVM (RHEV) compute resources available for provisioning involves two steps:

1. Creating a KVM (RHEV) endpoint. This enables vCAC to collect information about KVM (RHEV) compute resources.
2. Adding the KVM (RHEV) compute resources to an enterprise group.

After you create an endpoint, vCAC initiates the endpoint data collection. KVM (RHEV) Endpoint Data Collection collects the basic information about the compute resources (in this case the KVM hosts). It also collects information about templates and ISO images in the RHEV environment.

If a cluster in your RHEV environment is not assigned to a datacenter, the information from the cluster cannot be collected during the endpoint data collection in vCAC.

If a user creates, updates, or deletes any templates or ISO images, the user must then run KVM (RHEV) Endpoint data collection to collect that object, before it can be used in vCAC.

After the compute resources are added to an enterprise group, vCAC initiates compute resource data collection. There are two types of data collection supported by the KVM (RHEV) integration:

- **Inventory data collection** – Updates the vCAC record of the virtual machines whose resource usage is tied to that compute resource, including detailed information about the networks, storage, virtual machines and so on. This also includes information about unmanaged virtual machines (machines provisioned outside of vCAC).
- **State data collection** – Updates the vCAC record of the power state of each machine discovered through inventory data collection. State data collection also records missing machines that are managed by vCAC but cannot be detected on the virtualization compute resource or cloud endpoint.

When you destroy virtual machines in your RHEV environment, the information about the storage in RHEV is not updated immediately. Because of this, the storage information in vCAC might be inaccurate. The information in vCAC is updated with the correct storage values when the next inventory data collection is executed. Data collection is triggered automatically at regular intervals. You can configure the frequency of data collection or start it manually. For more information about compute resource data collection, see the *vCloud Automation Center Operating Guide*.

To discover compute resources for KVM (RHEV), create a KVM (RHEV) endpoint representing the KVM (RHEV) instance. For detailed instructions about creating a KVM (RHEV) endpoint, and running endpoint data collection manually, see: [“Creating and Importing a KVM \(RHEV\) Endpoint.”](#)

Planning vCAC User Groups and Policies

Before configuring KVM (RHEV) integration, consider planning and setting up the vCAC user groups and policies.

For detailed information about vCAC user groups and policies, see the *vCloud Automation Center Operating Guide*.

Global Administrators

Global administrators are responsible for setting up and maintaining the vCAC site, so that the provisioning group members can request and use machines. A global administrator role does not enable a user to request machines.

Table 1 Global administrator roles

Role	Description
vCAC Administrator	vCAC administrators manage endpoints and endpoint credentials, cloud service accounts, physical machines and storage devices, enterprise groups, and license keys. They also configure vCAC agents, assign global administrator roles and review user rights, and monitor DEM status and logs.
Enterprise administrator	Enterprise administrators manage compute resources and physical machines, reservations and reservation policies, provisioning groups, global blueprints, build profiles, approval policies, and other global elements. They also track resource usage and reclaim virtual machines.
Access administrator	Access administrators can modify provisioning group memberships.
Approver	If an approval policy is specified in a blueprint, approvers can either accept or reject requests to build machines.

A vCAC user can have more than one global administrator role, and can be both a global administrator and a provisioning group member in any role.

The vCAC installation procedure initially assigns the vCAC administrator role to the local Administrators group on the vCAC server. For detailed information about setting up vCAC roles and elements needed for provisioning virtual machines, see the *vCloud Automation Center Operating Guide*.

Provisioning Groups and Users

A provisioning group is a collection of machine consumers, often corresponding to a line of business, a department, or other organizational unit. To request machines, a vCAC user must belong to at least one provisioning group. Each group has access to a set of blueprints used to request machines.

A group must have at least one provisioning group manager, who maintains blueprints for the group and may approve machine requests. Groups can also contain support users, who can request and manage machines on behalf of other group members. A vCAC user can be a member of more than one provisioning group and can have different roles in different groups.

KVM (RHEV) Compute Resources, Enterprise Groups, and Virtual Reservations

A KVM (RHEV) compute resource is a vCAC object representing a KVM host or host cluster within the KVM (RHEV) virtualization platform. The virtual machines requested by provisioning group members are provisioned on compute resources.

Compute resources are organized into enterprise groups and managed by Enterprise Administrators. Enterprise groups are independent of provisioning groups.

A virtual reservation is a share of one compute resource's resources — memory, CPU and storage — reserved for use by a particular provisioning group in provisioning machines.

Each virtual reservation is for one provisioning group only but a group may have multiple reservations on the same compute resource or reservations on multiple compute resources.

Each virtual reservation can be added to one reservation policy. The reservation from which a particular virtual machine is provisioned is determined by vCAC based on the reservation policy specified in the blueprint, if any, the priorities and current usage of the provisioning group's various virtual reservations, and other factors.

Approval Policies

Approval policies determine whose approval is needed to provision a machine from the blueprint.

For information about approval policies, see “Configuring Approvals” on page 29.

The KVM (RHEV)-Based Provisioning Process

The following scenario describes the KVM (RHEV)-based provisioning process:

1. A vCAC user requests a machine by selecting a blueprint for KVM (RHEV) provisioning, which specifies:
 - a KVM (RHEV) server and a collection on that server, as well as other information needed to interact with the server
 - the location of a bootable ISO image
2. When the request is approved (or if it does not require approval), vCAC creates a virtual machine.
3. vCAC creates the machine in the specified KVM (RHEV) collection on the specified KVM (RHEV) server.
4. vCAC attaches the ISO image to the virtual machine's CD-ROM drive, then powers the machine on.
5. When the machine boots from the ISO image, control is passed to the KVM (RHEV) task sequence corresponding to the ISO image, and the machine is provisioned according to the task sequence. The required final task in the sequence is to install the vCAC guest agent software package, which runs a script to install and start the guest agent.
6. When the guest agent reports the success of its final work item, vCAC terminates the provisioning workflow. The machine is now provisioned and under vCAC management.

When the virtual machine is eventually destroyed, it is unregistered from the KVM (RHEV) collection.

Chapter 2 Adding KVM (RHEV) Resources to vCAC

2

This chapter provides details about the required KVM (RHEV) configuration. It also provides instructions about how to configure vCAC to communicate with the KVM (RHEV) instance and how to add KVM (RHEV) resources to vCAC.

Required KVM (RHEV) Configuration

- Each KVM (RHEV) environment must be joined to the domain containing the vCAC server.
- The credentials used to manage the endpoint representing a KVM (RHEV) environment must have Administrator privileges on the RHEV environment. These credentials must also have sufficient privileges to create objects on the hosts within the environment.

DEM Worker

DEM Workers manage virtual machines depending on the hypervisor management platform.

Typically, the DEM Worker runs as a service on the vCAC server. Without a running DEM Worker and DEM Orchestrator, vCAC cannot operate. When this is the case, the console displays a banner indicating the problem.

For more information about installing the Distributed Execution Manager, see *vCloud Automation Center Installation Guide*

Enabling Remote WMI Requests on Windows Machines

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

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

1. In each domain to which Windows virtual machines that are provisioned and managed by vCAC may be joined, create an Active Directory group.
2. Add the service credentials of the WMI agents that may need to execute remote WMI requests on the provisioned machines to the Active Directory group.
3. Enable remote WMI requests for the Active Directory groups containing the agent credentials on each Windows machine provisioned.

Specifying User Credentials for KVM (RHEV)

The credentials for KVM (RHEV) are stored in vCAC. Because the same credentials can be used for multiple endpoints, credentials are managed separately from endpoints and associated when endpoints are created or edited. Once credentials are created and saved in vCAC, they can be used for multiple endpoints as appropriate.

To provision virtual machines, the credentials used to manage the endpoint representing a KVM (RHEV) instance must have sufficient privileges to create objects on the hosts within the KVM (RHEV) instance.

To add the credentials for a KVM (RHEV) endpoint to vCAC:

1. Log in to vCAC as an administrator.
2. Select **vCAC Administrator > Credentials**.
3. Click **New Credentials** in the title bar.
4. Type a name for the credentials and, optionally, a description.
5. Type the user name for the KVM (RHEV) instance in `username@domain` format.
6. Type the password for the username. You must repeat the password for verification.
7. Click the **Save** icon.

Creating and Importing a KVM (RHEV) Endpoint

In the KVM (RHEV) integration you do not have to install an agent acting as a proxy between vCAC and the KVM (RHEV) endpoint, because every requested action triggers a workflow executed by a DEM Worker.

Creating a KVM (RHEV) Endpoint

To create an endpoint:

1. Log in to vCAC as a vCAC administrator.
2. Click **vCAC Administrator > Endpoints**.
3. Click **New Endpoint > Virtual > KVM (RHEV)** in the title bar.
4. Type a name for the endpoint and, optionally, a description.
Typically, the name indicates the KVM (RHEV) instance that the endpoint is for.
5. Specify the URL address of the instance by using a compute resource FQDN or IP address:
The URL must be of the type: `https://FQDN` or `https://IP_address`.
6. Click the **Browse** button to display the Credentials list.
7. (Optional) If you have not created credentials, or you need to create new ones, create new credentials.
 - a. Click the **New Credentials** link in the title bar.
 - b. Type the credentials for the KVM (RHEV) instance that the endpoint will represent.
The user name must be in `username@domain` format.
 - c. Type a name and, optionally, a description.
 - d. Click the **Save** icon to save the credentials.
8. Select the credentials you want to use for this endpoint and click **OK**.
9. (Optional) Create a custom property.

- a. Click **New Property**.
- b. Type a name of the property and a value.
- c. Select whether the property should be encrypted.
- d. Click the **Save** icon to save the property.

Repeat this procedure for all the needed custom properties.

10. Click **OK** to save the endpoint.

Repeat this procedure for all the needed endpoints.

Importing a KVM (RHEV) Endpoint

In addition to creating an endpoint, you can also import a KVM (RHEV) endpoint. You can add multiple endpoints of multiple types all at once by loading a CSV file containing the required information. The CSV file must contain a header row that determines the order of the fields (which are case-sensitive). Fields include:

- InterfaceType (in this case, **Kvm**)
- Address
- Credentials
- Name
- Description
- DataCenter
- Row
- Rack

To import an endpoint:

1. Log in to vCAC as a vCAC administrator.
2. Click **vCAC Administrator > Endpoints**.
3. Click the **Import Endpoints** link in the title bar and browse to the CSV file.
4. Click **Open**.

Starting Endpoint Data Collection Manually

You can start KVM (RHEV) endpoint data collection manually at any time to update the information in vCAC about the KVM (RHEV) compute resources and the templates and ISO images in the RHEV environment.

To start endpoint data collection:

1. Log in to vCAC as a vCAC administrator and click **vCAC Administrator > Endpoints**.
2. Point to a KVM (RHEV) resource and click **Data Collection**.
3. On the Data Collection page, click **Start**.

The endpoint data collection is started and the information in vCAC about the KVM (RHEV) compute resources in the selected endpoint are updated.

Creating an Enterprise Group

Enterprise Administrators are responsible for managing the reservations and machines on virtualization compute resources and cloud endpoints.

The users you assign as Enterprise Administrators have vCAC management access to any compute resources and endpoints you add to the group. For example, they are able to create virtual reservations on the compute resources, disable data collection, and so on. The Enterprise Administrators are also able to:

- Create and manage global vCAC elements including provisioning groups, reservations, build profiles, and global blueprints
- Manage virtual machines provisioned on the compute resources and endpoints in the group

Note: You can add an Active Directory security group as an Enterprise Administrator to give this role to all members of the security group. Do not add Active Directory distribution groups, because distribution groups cannot be authenticated against and therefore cannot convey vCAC roles.

Creating an enterprise group involves adding compute resources to an enterprise group and assigning at least one Enterprise Administrator to the group.

To create an enterprise group:

1. Log in to vCAC as a vCAC administrator.
2. Select **vCAC Administrator > Enterprise Groups**.
3. Click the **New Enterprise Group** link in the title bar.
4. Type a name and, optionally, a description for the new enterprise group.
5. Select the compute resources you want to add to the group.
6. Select the user names you want to assign as Enterprise Administrators from the drop-down menu.
If the users are not local users of the vCAC server, you must specify the user names in DOMAIN\username format.
7. Click **OK** to save the group.

If you add yourself as an Enterprise Administrator, the **Enterprise Administrator** activity group appears in the activity pane.

Repeat this procedure to create multiple enterprise groups containing compute resources, as needed.

Managing Machine Prefixes

Each blueprint has a machine prefix associated with it. The machine prefix is used to generate the names of the machines provisioned from that blueprint. The prefixes can be used to indicate the provisioning group or blueprint of a machine (or both) in its name. A prefix is a base name to be followed by a counter of a specified number of digits. For example, a prefix of **g1dw** (for **group1** and **developer workstation**) with a counter of three digits produces machines named **g1dw001**, **g1dw002**, and so on. A prefix can also specify a number other than **1** to start the counter.

Enterprise Administrators are responsible for managing machine prefixes as necessary. When you create a provisioning group, you must assign one of the existing machine prefixes as its default. This does not restrict Provisioning Group Managers (PGMs) when they create blueprints, as using the group's default prefix is optional. An Enterprise Administrator can change the default prefix of a provisioning group at any time.

Standards for Host Names

To conform to standard host name limitations, machine prefixes must contain only the ASCII letters **a** through **z** (case-insensitive), the digits **0** through **9** and the hyphen (-). They must not begin with a hyphen. No other symbols, punctuation characters, or blank spaces can be used.

To conform to the Windows limit of 15 characters in host names, machine prefixes should not be longer than 15 characters, including the digits. Longer compute resource names are truncated when a machine is provisioned, and updated at the next data collection from the virtualization compute resource.

Machine Name Limitations in vCAC

vCAC does not support multiple virtual machines with the same name within a single vCAC instance. This can occur if vCAC provisions a machine using the name of an existing unmanaged virtual machine, so it is important to choose prefixes that do not overlap with existing naming practices outside of vCAC.

Creating and Managing Machine Prefixes

To create a new machine prefix:

1. Log in to vCAC as a vCAC administrator.
2. Select **Enterprise Administrator > Machine Prefixes**.
3. Click **New machine prefix** link in the title bar.
4. Type the machine prefix, number of digits, and the next number.

Note: You must use enough digits to prevent a machine prefix from rolling back to the starting number and generating names that are still in use. For example, if thousands of machines with names generated from a single prefix will exist concurrently, you should specify four or five digits for the prefix.

5. Click the **Save** icon to save the prefix.

To manage machine prefixes:

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Machine Prefixes**.

The table that appears shows all existing prefixes, their counter lengths (Number of Digits), and the next counter number to be generated (Next Number). The Next Number cell of the table is updated every time a machine is built using the specific prefix. For instance, if the prefix **ABC-server** shows a counter length of four digits and a next number of 27, the next name generated is **ABC-server0027**. You can change the next number at any time to reset the counter, or to skip certain numbers (especially when lengthening the counter).

Managing Provisioning Groups

Enterprise Administrators create and manage provisioning groups, which often represent business units, functional units, or departments. Only provisioning group members can request machines, and provisioning groups cannot function without appropriately designated PGMs who create blueprints, approve requests, and manage machines.

Creating a Provisioning Group

You create provisioning groups by adding users to a group. When a valid user entry can no longer be resolved by vCAC, for example because the user was removed from Active Directory, the entry is replaced by **Account unknown (SID)**, where *SID* is the system identification number of the user account. This is done to allow for situations in which a user name temporarily becomes invalid. If the user account is

restored, the **Account unknown** entry is converted back to the user name. If you know the account will not be restored, you can simply delete the **Account unknown** entry.

To create a provisioning group:

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Provisioning Groups**.
3. Click **New Provisioning Group** in the title bar.
4. Specify the provisioning group settings.

You can also use the **Copy from existing group** drop-down menu to copy the settings from any of the existing provisioning groups and then modify the settings and membership as needed and save the group with a new name.

- a. Type the name and, optionally, a description of the group

Provisioning groups typically represent organizational units such as a department or line of business, and the group name and description should reflect this basis and provide useful information about the group.

- b. Enter one or more email addresses (including group aliases) or Active Directory accounts for the users specified as PGM. Multiple entries must be separated by commas (with no spaces), for example:

JoeAdmin@VMware.com,VMware\TinaVP,WeiMgr@VMware.com

These addresses are shown in the My Pending Requests lists of group members.

- c. Specify the default machine prefix for blueprints created by the group's managers. You can add a prefix or modify an existing one, if necessary, by clicking the **Manage machine prefixes** link to go to the Machine Prefixes page.
- d. Specify the default active directory container for machines provisioned by group members (such as **ou=test,ou=servers,dc=VMware,dc=local**)
- e. Enter group manager, support user, and user memberships. A group can have more than one manager, and a user can be manager of more than one group.

You can enter users manually or use the drop-down menu at the top of each text box to select the users to add. Only users who currently own at least one machine listed on the Enterprise Machines page are included in the drop-down list.

If the users you specify are not local users of the vCAC server, you must enter the user names in DOMAIN\username format.

Any changes you make to group membership are reflected in the console immediately after you save the new or modified provisioning group. For example, if you change a member's role from manager to user, the member immediately loses access to the **Provisioning Group Manager** activities (including managing blueprints, approving requests and so on) for that group, and this change is immediately reflected in the member's console.

Note: You can add an Active Directory security group as a provisioning group member to give provisioning group membership to all members of the security group. Do not, however, add Active Directory distribution groups, as distribution groups cannot be authenticated against and thus cannot convey vCAC roles.

- f. Include any custom properties to be applied to all machines created by members of this provisioning group.

Typically, the custom properties that you create in a provisioning group are different from those in build profiles and blueprints, having to do with resource management or line-of-business accounting.

Custom property values in reservations override those in provisioning groups, and those in provisioning groups override the custom properties in blueprints and build profiles. Because properties from these sources may be applied to so many machines provisioned from so many blueprints, they should be used carefully, and restricted to purposes applicable to all the machines they are applied to.

- Select the **Encrypt** check box to ensure that a secure property (such as a password) is never visible in plain text.
- To save your changes to a property, click the **Save** icon. The properties you add or modify are not saved until you save the provisioning group.

Note: When entering custom properties, verify that property values do not contain trailing spaces, because trailing spaces might result in provisioning failure.

5. Click **OK** to save the provisioning group.

The provisioning group is saved as well as any custom properties you created.

Viewing, Deleting, and Editing Provisioning Groups

To view and edit existing provisioning groups:

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Provisioning Groups**.

By default, the Provisioning groups page shows the following information for each group:

- The name of the group
- One or more PGM email addresses or Active Directory accounts
- The description of the group
- The number of existing virtual machines provisioned on the group's reservations
- The percentage of the group's total reserved virtual capacity that is currently allocated to virtual machines for machine quota (maximum number of machines that can be provisioned), memory, and storage

Total reserved virtual capacity is the sum of all of the group's existing reservations on all virtualization compute resources, not just those in the enterprise groups you manage.

The final (**Total**) row aggregates the usage statistics for all provisioning groups, showing the total virtual machine quota, memory and storage allocated out of reserved capacity for all compute resources in the entire vCAC site.

You can sort and filter individual columns and change the included columns by using the **Columns** control. You can also create complex filters by using the Filters control. Additional **virtual** columns available include:

- The total storage used by the group
- The storage used by the group as a percentage of reserved storage.

Note: The amount of storage allocated to a machine is the same as the amount used by it when standard storage technology is in use. However, when machines are provisioned using a space-efficient technology such as thin provisioning, a machine's storage used can be less than its storage allocated because the machine uses storage only as needed. You can calculate the storage saved using space-efficient technology by comparing the amount of allocated storage shown in the **Stor-**

age Allocated % column and the amount of used storage shown in the optional **Storage Used** column.

These additional columns are also totaled for all provisioning groups in the final row.

Changes you make in the list display persist from one view of the list to the next.

To export the information in the list:

- Select an option from the **Export** drop-down menu.

You can export the information in the list to an Adobe Acrobat Reader (PDF), Microsoft Office Excel (XLSX, XLS or CSV) or Microsoft Office Word (RTF) file.

To edit a provisioning group:

- Point to a provisioning group and click **Edit**.

You can edit the selected group's settings.

To delete a provisioning group:

- Point to a provisioning group and click **Delete**.

You can delete the selected group. You cannot delete a group that has one or more reservations or blueprints associated with it.

The first step in deleting an active provisioning group involves preventing further requests for machines from group members so you can delete the reservations, blueprints, and group when all existing machines have been destroyed or decommissioned. There are two ways to accomplish this:

- Disable all of the group's blueprints by deselecting the **Enabled** check box for each blueprint.
- Disable all of the group's reservations.

To view provisioning group information:

- Point to a provisioning group and click **Group Information**.

Detailed information about the selected provisioning group is displayed. It includes a list of the group's reservation with status, a list of the global and local blueprints available to group members requesting machines, and a list of all machines provisioned from the group's reservations.

To view provisioning group reservations information:

- Point to a provisioning group and click **View Reservations**.

The Reservations page is displayed. The page contains a summary of that group's virtual reservations on compute resources and endpoints in your enterprise groups. The information is useful because it lets you identify situations in which you might have to increase reservation capacity for the group.

The list of the displayed reservations can be further filtered, for instance for a particular compute resource.

About Reservations

Each provisioning group must have at least one reservation in order for its members to provision machines of that type. Enterprise Administrators are responsible for providing the provisioning groups they create with reservations as needed.

Compute resources, endpoints, and enterprise groups are independent of provisioning groups, but each reservation is for one provisioning group only. Each provisioning group can have as many reservations as desired.

A virtual reservation is a description of the share of a compute resource or compute resource cluster's resources—memory, CPU, and storage—reserved for use by a particular provisioning group in provisioning virtual machines. A virtual reservation for any provisioning group within a vCAC site can be made on any compute resource or compute resource cluster known to vCAC and belonging to an enterprise group.

For more detailed information about reservations, see *vCloud Automation Center Operating Guide*.

Creating a KVM (RHEV) Reservation

To create a KVM (RHEV) reservation:

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Reservations**.
3. Click **New Reservation** in the title bar, and select the type of reservation: **Virtual > KVM (RHEV)**.
4. Specify the reservation information or use the **Copy from existing reservation** drop-down menu to copy the settings from an existing reservation.

You can then modify the settings as needed and save the reservation with a new name. Copying the reservation also copies the provisioning group and compute resource/endpoint settings along with others; once you have created the reservation these cannot be changed, so if you want to change them do it right away, before saving the reservation.

All reservations settings but reservation policy, quota, and custom properties are required. Descriptive reservation names are helpful in allowing you and other Enterprise Administrators to manage virtual reservation usage site wide.

- a. Specify the compute resource a virtual reservation is on.
- b. Type a name for the reservation.
- c. Specify the provisioning group the reservation is for.

Note: After you create a reservation, you cannot change the compute resource or endpoint a reservation is on. You also cannot change the provisioning group for which you created the reservation.

- d. Specify the reservation policy in which to place the reservation. A reservation policy is a collection of reservations that can be selected in a blueprint to restrict all machine provisioning from that blueprint to those reservations. A reservation need not belong to a reservation policy, but can belong to only one.
- e. Enter the maximum number of machines that can be provisioned from the reservation. Leave the **Machine quota** field empty to specify no limit. Only the machines that are turned on are counted in virtual reservation allocated machine quota statistics.
- f. Specify the priority of the reservation, for use in determining which reservation to use when two or more are available to a provisioning group. Lower-numbered reservations are used first.
- g. Include any custom properties to be used in provisioning machines on the reservation.

Typically, these would be different from those in build profiles and blueprints, having to do with resource management.

Custom property values in reservations override those in provisioning groups, and those in provisioning groups override those in blueprints and build profiles. Because properties from these sources may be applied to so many machines provisioned from so many blueprints, they should be used carefully, and restricted to purposes applicable to all the machines they are applied to.

- Select the **Encrypt** check box to ensure that a secure property (such as a password) is never visible in plain text.

- To save your changes to a property, click the **Save** icon. The properties you add or modify are not saved until you save the provisioning group.

Note: When entering custom properties, always ensure that property values do not contain trailing spaces, as these may cause provisioning to fail.

5. On the **Resources** tab, specify the number of resource settings for the KVM (RHEV) reservation:
 - a. In the **Memory** section, specify how much of the virtualization compute resource's memory is reserved by this reservation.

The Memory section also displays the current total physical, allocated, and reserved memory of the compute resource. You can specify an amount of memory for the current reservation within the context of the compute resource's overall usage. If physical and reserved memory on the compute resource are currently the same and there is no more unreserved memory available, adding a reservation or adding memory to an existing reservation causes the compute resource to become overreserved. If reserved and allocated are the same but physical is larger, more machines can be provisioned on the compute resource if more memory is reserved. Only machines that are turned on are included in allocated memory statistics.

- b. In the **Storage** section, you can select storage paths and specify how much storage on each is reserved by this reservation. You must select at least one storage path.

For each storage path available on the selected compute resource, this section shows you:

- The current physical, free, and reserved storage on the entire storage path. The Reserved figure is for all vCAC reservations, not just the one you are currently editing. Remember that a storage path can be deliberately overreserved as discussed earlier in this section.
- The amount of storage reserved by the reservation you are editing and the storage currently allocated from it to virtual machines. (Remember that the amount actually used by those machines is less if space-efficient storage is in use.)

The statistics let you select among the available storage paths and specify an amount of storage for the current reservation within the context of each storage path's overall usage to avoid overreservation of storage paths.

A storage cost is also displayed for each storage path. This cost is specified on the Cost Profile tab for the compute resource the reservation is on, either in the cost profile assigned to the compute resource or in the storage cost profile assigned to the individual storage path. If no cost profile of either type is assigned, the storage cost is 0.

When selecting multiple storage paths, you can assign a priority to each, which determines the order in which vCAC evaluates them for provisioning once the reservation has been selected. If you do not specify priorities or specify equal priorities, ordering is random.

You can also disable each storage path in an existing reservation to prevent new machines from being provisioned on it. This is usually done prior to decommissioning a storage device; once existing machines provisioned on the path are disposed of, the storage can be removed from the compute resource.

Note: All storage paths included in any virtual reservation on a compute resource cluster are accessible to all compute resources in the cluster. Storage paths local to a single compute resource are available when creating a reservation on a cluster.

- c. In the **Network** section, select the network paths to be assigned to machines provisioned under this reservation.

You must select at least one. If you select more than one, machines are distributed among them in round-robin fashion.
6. Click **OK** to save the reservation.

Viewing, Deleting, and Editing Reservations

Enterprise Administrators can access the Reservations page to view and manage reservations in one of several ways:

1. Log in to vCAC as an Enterprise Administrator.
2. Under **Enterprise Administrator** in the activity pane:
 - Select **Reservations** to display all virtual and cloud reservations on all compute resources and endpoints in the enterprise groups you manage
 - Select **Provisioning Groups**, point to a listed provisioning group and then select **View Reservations** to display that group's reservations of all types
 - Select **Compute Resources**, point to a listed compute resource and then select **View Reservations** to display all virtual reservations on that compute resource

The Reservations page by default shows each reservation's name, type, provisioning group and priority, and includes several columns indicating provisioning capacity usage, including total machines on the reservation, percentage of total machines that is allocated and percentage of reserved capacity allocated for machine quota as well as memory and storage.

Note: Only machines that are turned on are included in virtual reservation allocated quota and memory statistics. Allocated storage statistics include all virtual machines, off or on.

To edit a selected reservation:

- Point to a reservation name and click **Edit**

You can edit the selected reservation's settings.

To delete a selected reservation:

- Point to a reservation name and click **Delete**.

Allows you to delete the selected reservation. This option is not available if there are provisioned machines on this reservation.

To view the machines in a selected reservation:

- Point to a reservation name and click **View Machines**.

The list of the machines available in this reservation is displayed.

Chapter 3 Creating Blueprints for KVM (RHEV)

3

A blueprint is the complete specification for a virtual machine, determining the machine's attributes, the manner in which it is provisioned, and its policy and management settings. To request a machine, a group member must select a blueprint from which it will be provisioned.

When you create a blueprint, you specify some information using controls in the console and some using custom properties. Custom properties can also be specified in build profiles. Multiple build profiles can be incorporated into any blueprint by selecting from a list.

Blueprints can be global or local:

- **Global blueprints** – Global blueprints are created and managed by enterprise administrators and are available to all provisioning groups.
- **Local blueprints** – Local blueprints are typically created by PGMs and are available to members of the provisioning group only.

You can create blueprints as an Enterprise Administrator or as a PGM:

- As an Enterprise Administrator, select **Enterprise Administrator > Global Blueprints** and click **New Blueprint** to create a global blueprint.
- As a PGM of the provisioning group, select **Provisioning Group Manager > Blueprints**, edit a global blueprint, and select it for the provisioning group.
- As a PGM of the provisioning group you created, select **Provisioning Group Manager > Blueprints** and click **New Blueprint** to create a local blueprint.

The following sections describe the custom properties for the KVM (RHEV) integration, the workflows which you can use in creating blueprints as well as some basic procedures to create KVM (RHEV) blueprints. These procedures apply to both local and global blueprints.

Custom Properties for KVM (RHEV) Integration

This section describes the custom properties specific for the KVM (RHEV) integration and selected properties that are useful for KVM (RHEV) blueprints. For detailed information about the custom properties for Windows WinPE/WIM, Red Hat Linux Kickstart, Microsoft System Center Configuration Manager (SCCM) provisioning and so on, see the *vCloud Automation Center Operating Guide*.

You can use these custom properties to modify the settings of the newly provisioned virtual machines. The custom properties can be used in the same way for both creating and cloning virtual machines.

When the same property exists in more than one source, a specific order is followed when applying to the machine. This order is as follows, with the latter overriding earlier:

- Build profile
- Blueprint

- Provisioning group
- Compute resource
- Reservations
- Endpoint
- Runtime

A custom property can be marked as runtime when:

- The property is marked as **Prompt User**, which means that the user must supply a value for it when requesting a machine. This requires machine requestors to customize individual characteristics of each machine, or gives them the option of doing so when a default value is provided for the required property.
- Any administrative user (such as enterprise administrator or provisioning group manager) who is modifying or adding property values in the property grid.

Any runtime property takes higher precedence and overrides property coming from any source in vCAC.

Table 2 Custom Properties for KVM (RHEV) Integration

Property	Description
VirtualMachine.Admin.NetworkInterfaceType	<p>Indicates the network interface type. Use this custom property to modify the network settings of the newly provisioned virtual machine. The supported network adapters are:</p> <ul style="list-style-type: none"> • E1000 • VirtIO • RTL8139 • RTL8139 VirtIO <p>The default value is E1000.</p>
VirtualMachine.Admin.DiskInterfaceType	<p>Indicates the type of hard disk drivers. Use this custom property to modify the hard disk driver. The supported drivers are:</p> <ul style="list-style-type: none"> • IDE • VirtIO <p>The default value is IDE.</p>
VirtualMachine.Admin.CreateDiskTimeoutInSeconds	<p>Specifies how long, in seconds, to wait before timing out the disk creation process.</p> <p>The default value is 20 minutes per 1 GB of disk created. Use this custom property to increase the timeout period, especially if using IDE drivers or provisioning over a slow network.</p>

Property	Description
VirtualMachine.Admin.ThinProvision	<p>Determines whether thin provisioning is used for storage. If the value of this custom property is true, all disks are provisioned using thin provisioning.</p> <p>If the value is false and the blueprint action is Create, all disks are created as pre-allocated disks. If the blueprint action is Clone, the template is cloned as is (with thick or thin disks as specified in the template) and additional storage volumes added in vCAC are created as pre-allocated disks.</p> <p>The default value is <code>false</code>.</p> <hr/> <p>Note: When provisioning using cloning, it can take longer to provision disks using thick provisioning than thin provisioning.</p>
VirtualMachine.Admin.OverrideVncConsole	<p>Use this custom property to specify how the console of the provisioned virtual machine will be accessed.</p> <p>By default, vCAC sets the console display type in RHEV to be VNC. If you set this custom property to true, vCAC uses the default RHEV display type, which is Spice. For more information about Spice, see http://spice-space.org/.</p>
Machine.SSH	<p>Set this custom property to true to enable the Connect Using SSH menu option on provisioned virtual machines. For more information about enabling SSH, see the <i>vCloud Automation Center Operating Guide</i></p>
VirtualMachine.DiskN.Size	Size of machine's disk <i>N</i> in GB.
VirtualMachine.NetworkN.Name	Name of network to which network device <i>N</i> in a virtual machine is attached.

Workflows

vCAC uses workflows to define its machine provisioning and management processes. The provisioning workflows define the process of building or cloning a machine and are specified in blueprints.

There are six provisioning workflows which you can use in the KVM (RHEV) integration:

- **BasicVmWorkflow** — for provisioning a machine with no guest operating system
- **ExternalProvisioningWorkflow** — for external provisioning services (such as Citrix and BMC BladeLogic)
- **LinuxKickstartWorkflow** — for kickstart provisioning
- **VirtualSccmProvisioningWorkflow** — for SCCM-based provisioning
- **WIMImageWorkflow** — for WIM-based provisioning
- **CloneWorkflow** — for cloning virtual machines from a KVM (RHEV) template

Creating a Basic KVM (RHEV) Blueprint

To create a basic KVM (RHEV) blueprint:

1. On the Blueprints or Global Blueprints page click **New Blueprint > Virtual > KVM (RHEV)**.
2. On the **Blueprint Information** tab specify the basic blueprint information:
 - a. Specify a name and, optionally, a description of the blueprint.
 - b. (Optional) Select the display icon for the blueprint and the images based on the blueprint.
 - c. Select whether the blueprint is global or local and whether it is a Master that can be copied.
If you create a global blueprint, PGMs can select it. If you make it a Master, they can copy it in creating local blueprints. The Global check box is locked unless you are both Enterprise Administrator and PGM, in which case you can decide whether the blueprint is global or local.
 - d. Specify the provisioning group a local blueprint belongs to, or the provisioning groups a global blueprint is selected for. In either case select one or more of the provisioning groups you already created. If you are an Enterprise Administrator only, the Groups check boxes are locked.
 - e. (Optional) Select the reservation policy to associate with the blueprint.
 - f. Select the machine prefix to generate names for machines created from the blueprint.
Leave this set to **Use group default** to use the default prefix you assigned to the provisioning group.
 - g. Select the approval policy to determine whose approval is needed to provision a machine from the blueprint.
If you have not created any approval policies, you can select **No Approval** or **Default Approval (Group Manager)**. Select **Default Approval (Group Manager)** to require group manager approval for basic and support user requests.
 - h. Select whether the blueprint should be enabled and available for machine requests.
 - i. Select whether requesting users have the option of selecting a provisioning location.
 - j. (Optional) Specify the maximum number of machines provisioned from this blueprint that any single user can own at one time.
 - k. Specify the length of the archive period, in days, that expired virtual machines built from the blueprint will remain available for reactivation during that time. If you specify **0**, machines are destroyed immediately when expire.
 - l. (Optional) You can specify the daily cost for the blueprint.
For virtual machines, this is used together with the cost profiles associated with the compute resource and storage path on which the virtual machine is provisioned.
3. On the **Build Information tab**, specify how the machine is to be provisioned.
 - a. From the **Blueprint type** drop-down menu, select whether the virtual machine is to be defined as a server or a workstation for licensing, integration and record-keeping purposes.
 - b. From the **Actions** drop-down menu, select **Create** to create the virtual machine.
 - c. From the **Provisioning workflow** drop-down menu, select the **BasicVmWorkflow** provisioning workflow.
 - d. Select the ISO to use for provisioning.
 - e. Specify the minimum and, optionally, maximum memory, CPU count, and storage specifications for the machine, as well as optional approval thresholds for these settings.
The memory, CPU count, and storage specifications determine the resources allocated to the virtual machine. If you supply a maximum, the machine requestor can optionally increase the specification up to that limit. (An exception is the Reserved storage specification for cloning blueprints, which has a Minimum counter only.)

- f. In **Lease (days)**, specify the length of the machine's lease (time until it expires) in days.
A blank setting means no expiration date. As with the machine specifications, you can set a maximum to allow the requesting user to increase lease length up to that figure and an approval threshold above which the machine requires approval (if an approval policy is set on the Blueprint Information tab).
- g. Add storage volumes:
- Click the **Add Volume** link.
 - Specify the capacity in GB.
 - You can optionally specify a drive letter or mount path, or provide a label and storage reservation policy.
 - Click the **Save** icon to save the volume.
- h. (Optional) Select whether to allow users to see and change the storage reservation policies.
- i. (Optional) Specify the Maximum number of volumes.
If you leave the text box blank, the default value (15) will be used. To disable adding volumes, set to 0.

Note: You cannot create more than three IDE disks for a single machine in RHEV. This limitation does not apply to VirtIO disks.

- j. (Optional) Specify the Maximum number of network adapters.
If you leave the text box blank, there is no maximum number. To disable adding network adapters, set to 0.
4. (Optional) On the **Properties** tab, specify the additional properties.

Note: For information about the custom properties supported in the KVM (RHEV) integration, see [“Custom Properties for KVM \(RHEV\) Integration.”](#)

- a. Select the check boxes of the available Build profiles to use.
- b. Include any custom properties.
Custom properties can be added directly to the blueprint or instead added to an incorporated build profile.
- Select the **Encrypt** check box to ensure that a secure property (such as a password) is never visible in plain text.
 - Click the **Save** icon to save the property. The properties you enter or modify are not saved until you save the blueprint by clicking **OK**.
5. On the **Security** tab, specify the access settings:
- a. Specify the user names of the group members who can request machines from the blueprint, or on whose behalf machines can be requested by support users.
If you do not specify user names, the entire group can own machines provisioned from the blueprint. The settings available on blueprint tabs depend on your role. Enterprise Administrators and Provisioning Group Managers can perform different activities.
- b. The machine operations that are available to owners of machines created from the blueprint, including various power cycle options, reprovisioning the machine, and so on.

Note: Customized operations you have added to the machine menu using vCAC Designer automatically appear on the **Security** tab, and must be selected like other operations to be made available to the user.

Support users always have access to all operations, including those not selected on the Security tab, both for their own machines and while working on behalf of other users. PGMs have access to all operations.

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

Preparing for WIM-Based Provisioning with VirtIO drivers

If you are using VirtIO for network or storage interfaces, you must ensure that the necessary drivers are included in your WinPE image and WIM image. VirtIO generally offers better performance when provisioning with KVM (RHEV).

Windows drivers for VirtIO are included as part of the Red Hat Enterprise Virtualization and are located in the `/usr/share/virtio-win` directory on the file system of the Red Hat Enterprise Virtualization Manager. The drivers are also included in the Red Hat Enterprise Virtualization Guest Tools located `/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso`.

The high-level process for enabling WIM-based provisioning is as follows:

1. Create a WIM image from a Windows reference machine with the VirtIO drivers installed or insert the drivers into an existing WIM image.
2. Create a WinPE image with the VirtIO drivers using the PE Builder utility provided with vCAC, or insert the drivers into a WinPE image created using other means.
3. Upload the WinPE image ISO to the Red Hat Enterprise Virtualization ISO storage domains using the `rhev-iso-uploader` command. For more information about managing ISO images in RHEV, refer to the Red Hat documentation.
4. Create a virtual blueprint for KVM (RHEV) with WIM provisioning and select the WinPE ISO on the Build Information tab. The custom properties **Image.ISO.Location** and **Image.ISO.Name** are not used for KVM (RHEV) blueprints.

For more information about WIM-based provisioning in vCAC, see the *vCloud Automation Center Operating Guide*.

To create a WinPE image with VirtIO drivers using PE Builder:

1. Install the PE Builder utility.
2. Copy the driver files to the PE Builder plugins directory, typically `%SystemDrive%\Program Files(x86)\Vmware\vCAC\PEBuilder\Plugins`.
3. Run the PE Builder utility.
4. Create a WinPE image as described in the *vCloud Automation Center Operating Guide*.

Creating a Clone KVM (RHEV) Blueprint

You can use vCAC to clone both Windows and Linux virtual machines. Cloning involves two objects:

- A template to clone from, created from a reference machine
- A customization object to customize the cloned machines by applying System Preparation Utility for Windows (SysPrep) information

Note: KVM (RHEV) does not support customization of cloned virtual machines. Unless you set up your Linux templates to generate unique hostnames and IP addresses,

the virtual machines that you provision in KVM (RHEV) by cloning always have the same names and IP addresses.

Creating a Template to Provision by Cloning Within RHEV

The Red Hat documentation provides general instructions for preparing Linux or Windows templates. For example, you can find the instructions for preparing templates in the Red Hat Enterprise Virtualization Administration Guide.

To create the objects to provision by cloning within your RHEV environment:

1. Create a virtual machine in your RHEV environment with the desired Windows OS or Linux OS. You can create the virtual machine either directly in the RHEV environment, or by using vCAC.
2. For Linux reference machines, if you want to specify an external Linux customization script or other post-provisioning steps in the cloning blueprint, perform the following additional steps on the Linux reference machine:

- a. Install the vCAC gagent agent by using the RPM package located in the vCAC installation files LinuxGuestAgentPkgs folder and appropriate sub-folder by running the command

```
rpm -i gagent-version.rpm
```

- b. Configure the gagent service by running the following commands:

```
cd /usr/share/gagent
./installgagent.sh servername:port ssl
```

where *servername:port* is the name of the Manager Service host and the port number (default is 443)

3. For Windows reference machines, if you intend to specify post-provisioning steps in the cloning blueprint, install the Windows guest agent:
 - a. Download the zip file for vCloud Automation Center from the VMware downloads page at <http://www.vmware.com/download/>.
 - b. Extract the files from the zip archive.
 - c. Navigate to the directory where you extracted the zip archive, then navigate to the **Setups** subdirectory.
 - d. Copy the **GugentZip.zip** file to the Windows reference machine.
 - e. Extract the archive to **C:**.
 - f. The **VRMGuestAgent** directory is created.
 - f. Open an elevated command prompt using **Run as Administrator**.
 - g. Navigate to **C:\VRMGuestAgent**.
 - h. Run the following command:

```
winservice -i -p ssl -h hostname
```

where *hostname* is the fully qualified domain name of the Manager Service host.

4. Seal the virtual machine. Refer to the Red Hat documentation on sealing templates in preparation for deployment for instructions.
5. Turn the reference machine into a KVM (RHEV) template.
6. Run endpoint data collection on your KVM (RHEV) endpoint to collect the new template.

For detailed instructions about running endpoint data collection manually, see [“Starting Endpoint Data Collection Manually.”](#)

Creating a KVM (RHEV) Blueprint for Provisioning by Cloning

1. On the Blueprints or Global Blueprints page click **New Blueprint > Virtual > KVM (RHEV)**.
2. On the **Blueprint Information** tab, specify the basic blueprint information:
 - a. Specify a name and, optionally, a description of the blueprint.
 - b. (Optional) Select the display icon for the blueprint and the images based on the blueprint.
 - c. Select whether the blueprint is global or local and whether it is a Master that can be copied.
 If you create a global blueprint, PGMs can select it. If you make it a Master, they can copy it in creating local blueprints. The Global check box is locked unless you are both Enterprise Administrator and PGM, in which case you can decide whether the blueprint is global or local.
 - d. Specify the provisioning group a local blueprint belongs to, or the provisioning groups a global blueprint is selected for. In either case select one or more of the provisioning groups you already created. If you are an Enterprise Administrator only, the Groups check boxes are locked.
 - e. (Optional) Select the reservation policy to associate with the blueprint.
 - f. Select the machine prefix to generate names for machines created from the blueprint.
 Leave this set to **Use group default** to use the default prefix you assigned to the provisioning group.
 - g. Select the approval policy to determine whose approval is needed to provision a machine from the blueprint.
 If you have not created any approval policies, you can select **No Approval** or **Default Approval (Group Manager)**. Select **Default Approval (Group Manager)** to require group manager approval for basic and support user requests.
 - h. Select whether the blueprint should be enabled and available for machine requests.
 - i. Select whether requesting users have the option of selecting a provisioning location.
 - j. (Optional) Specify the maximum number of machines provisioned from this blueprint that any single user can own at one time.
 - k. Specify the length of the archive period, in days, that expired virtual machines built from the blueprint will remain available for reactivation during that time. If you specify **0**, machines are destroyed immediately when expire.
 - l. (Optional) You can specify the daily cost for the blueprint.
 For virtual machines, this is used together with the cost profiles associated with the compute resource and storage path on which the virtual machine is provisioned.
3. On the **Build Information** tab, specify how the machine is to be provisioned:
 - a. From the **Blueprint type** drop-down menu, select whether the virtual machine is to be defined as a server or a workstation for licensing, integration and record-keeping purposes.
 - b. From the **Actions** drop-down menu, select **Clone** to create the virtual machine.
 - c. From the **Provisioning workflow** drop-down menu, select **CloneWorkflow**.
 - d. Browse to select the template to use for cloning.

Note: The list of templates you can select from includes all templates on all available reservations. vCAC does not validate that the selected template exists on the reservation that is used when provisioning a machine from the blueprint.

To avoid errors during provisioning, verify that the template is available on all reservations that could be used to provision machines from this blueprint. To do this,

add the template to all possible reservations, or use reservation policies to restrict the blueprint to reservations where the template is available.

- e. Set the **# CPUs** and **Memory** specifications.

Note: When you clone a virtual machine from a template, the **Maximum Storage (GB)** text box is inactive, and you cannot modify the hard disk settings to edit the storage.

- f. In **Lease (days)** specify the length of the machine's lease (time until it expires) in days.

A blank setting means no expiration date. As with the machine specifications, you can set a maximum to allow the requesting user to increase lease length up to that figure and an approval threshold above which the machine requires approval (if an approval policy is set on the Blueprint Information tab).

- g. (Optional) Add storage volumes:

- Click the **Add Volume** link.
- Specify the capacity in GB.
- You can optionally specify a drive letter or mount path, and provide a label and storage reservation policy.
- Click the **Save** icon to save the volume.

Note: You cannot create more than three IDE disks for a single machine in RHEV. This limitation does not apply to VirtIO disks.

- h. (Optional) Select whether to allow users to see and change the storage reservation policies.

- i. (Optional) Specify the Maximum number of volumes.

If you leave the text box blank, the default value (15) is used. To disable adding volumes, set to 0.

- j. (Optional) Specify the Maximum number of network adapters.

If you leave the text box blank, there is no maximum number. To disable adding network adapters, set to 0.

4. (Optional) On the **Properties** tab, specify the additional properties:

Note: For information about the custom properties supported in the KVM (RHEV) integration, see [“Custom Properties for KVM \(RHEV\) Integration.”](#)

- a. Select the check boxes of the available Build profiles to use.

Custom properties can be added directly to the blueprint or instead added to an incorporated build profile.

- Select the **Encrypt** check box to ensure that a secure property (such as a password) is never visible in plain text.
- Click the **Save** icon to save the property. The properties you enter or modify are not saved until you save the blueprint by clicking **OK**.

5. On the **Security** tab, specify the access settings:

- Specify the user names of the group members who can request machines from the blueprint, or on whose behalf machines can be requested by support users.

If you do not specify user names, the entire group can own machines provisioned from the blueprint. The settings available on blueprint tabs depend on your role. Enterprise Administrators and Provisioning Group Managers can perform different activities.

- The machine operations that are available to owners of machines created from the blueprint, including various power cycle options, reprovisioning the machine, and so on.

Note: Customized operations you have added to the machine menu using vCAC Designer automatically appear on the **Security** tab, and must be selected like other operations to be made available to the user.

Support users always have access to all operations, including those not selected on the Security tab, both for their own machines and while working on behalf of other users. Provisioning group managers have access to all operations.

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

Chapter 4 Optional Configuration

4

Configuring Approvals

The approval policy assigned to a blueprint determines what approvals are required, if any, before a machine can be provisioned from it. By default, all vCAC sites have two options available: No Approval (approval is never required), and Default Approval (provisioning group manager approval required). If you want other vCAC users to review machine requests, you must place them in approval groups and then place those groups in additional approval policies. Those approval policies can then be selected by provisioning group managers and enterprise administrators creating blueprints.

An approval group is a collection of users, any one of whom can approve a machine request. An approval policy contains one or more approval groups, each of which must approve the machine request in a specified sequence. This means that in practice, all members of the first approval group in the policy see the request; when one of them approves it, they no longer see it and all members of the next approval group see it; and so on.

Email notifications are automatically sent to approvers when there is a machine request requiring their assessment. Notifications are also sent to the machine requestor when the approval process is complete.

If advanced approval support has been enabled by the vCAC administrator several additional features are available. Advanced approval support can be enabled on the **vCAC Administrator > Customization** page.

To manage approval groups and policies:

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Approval Groups & Policies**.

The Approval Groups and Policies page displays all existing groups and all existing policies.

To export the information about the approval groups and policies in the list:

- Select an option from the **Export** drop-down menu.

You can export the information in the list to an Adobe Acrobat Reader (PDF), Microsoft Office Excel (XLSX, XLS or CSV) or Microsoft Office Word (RTF) file.

To edit a group or policy:

- Point to a group's name and select **Edit**.

You can edit the selected group's or policy's settings.

To delete a group or policy:

- Point to a group's name and select **Delete**.

You can delete the selected group or policy.

Creating a New Approval Group

You create approval groups by adding users to a group. When a valid user entry can no longer be resolved by vCAC, for example because the user was removed from Active Directory, the entry is replaced by **Account unknown (SID)**, where *SID* is the system identification number of the user account. This is done to allow for situations in which a user name temporarily becomes invalid. If the user account is restored, the **Account unknown** entry is converted back to the user name. If you know the account will not be restored, you can simply delete the **Account unknown** entry.

To create a new approval group:

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Approval Groups & Policies**.
3. Click **New Approval Group** in the title bar.
4. Specify the approval group settings:
 - a. Provide a name and, optionally, a description.
 - b. Type one or more email addresses (including group aliases) or Active Directory accounts for the users specified as approvers. Multiple entries must be separated by commas. These addresses are shown in the My Pending Requests lists of group members.
 - c. Specify one or more approvers, selected from the drop-down list or entered directly into the **Approvers** text box.

Only users who own at least one machine listed on the Enterprise Machines page are included in the drop-down list. User names are validated when you save your changes. If one or more of the user names is not valid, the group remains open for editing.

If the users you specify are not local users of the vCAC server, you must enter the user names in DOMAIN\username format.

Any user who is included in at least one approval group sees the **Approvals** entry in the activity pane of the console and can use it to find out whether any machine approvals are pending.

Note: You can add an Active Directory security group as an approver to give this role to all members of the security group. Do not, however, add Active Directory distribution groups, as distribution groups cannot be authenticated against and thus cannot convey vCAC roles.

- d. (Optional) If advanced approval is enabled, you can specify delegates for specific approvers. To designate a delegate, click the **Add Delegate** link and select a group member from the drop-down list or enter the member's user name, then enter the user name of the delegate and click the **Save** icon.

One or more delegates are temporarily or indefinitely designated for one or more members of the group. These delegates become approvers and receive and can act on all requests that come to the user for which they are designated, in effect becoming members of the approval group.

Use DOMAIN\username format for user names. For existing delegations, click the edit icon next to the specified group member to modify delegates and the delete icon to remove them.

Note: Unless a delegate you designate is added to the email address or alias specified for the approval group, the delegate will not receive automatic emails about approval requests.

- e. (Optional) If advanced approval is enabled, you can specify custom properties, the values of which must be supplied by the group member approving a request. You cannot specify property values. If a value was provided by the blueprint or requesting user, it appears as the

default for the approver. Typically, this is used to let the approver confirm or modify a value provided by the requesting user.

Creating a New Approval Policy

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Approval Groups & Policies**.
3. Click **New Approval Group** in the title bar.
4. Specify the approval group settings:
 - a. Type a name and, optionally, a description.
 - b. Specify the approval groups included in the policy, and their sequence.
 - c. Select whether provisioning group manager approval is required in addition to the listed approval groups (PGM always comes first in the approval sequence).

Note: When **Group manager approval required** is selected, and a provisioning group manager is also included in an included approval group, that individual may have to approve twice, once as provisioning group manager and once as approver.

You can use the **Add**, **Remove**, **Up** and **Down** buttons to select the approval groups you want and set them in the desired sequence.

When advanced approval support is enabled, two additional entries are available in the **Group** box listing available approval groups, and can be added to the policy sequence:

- d. Specify the point in the approval process at which the machine is actually provisioned by using the **[Machine Provisioning]** entry indicates. Groups above the entry approve before provisioning, those below it approve after, allowing an approver to directly verify something about the provisioned machine before giving approval for it to be used. This entry can be used only once in a policy.

In general, when an approval policy is selected in a blueprint and at least one approval threshold is set, approval is required only when the requesting user meets or exceeds an approval threshold. When one or more approval groups appear after **[Machine provisioned]**, however, approval by these groups is always required, even when the requesting user did not exceed any approval threshold in the initial request. For example, suppose approval policy **Policy12** includes the following.

```
ApprovalGroupB
[Machine provisioned]
ApprovalGroupJ
```

If **Policy12** is selected in a blueprint with at least one approval threshold:

- When the requesting user meets or exceeds an approval threshold, approval by **ApprovalGroupB** is required before machine provisioning and by **ApprovalGroupJ** after provisioning.
- When the requesting user does not meet or exceed an approval threshold, approval from **ApprovalGroupJ** is required after machine provisioning.

Note: If an approval group in the policy prompts approvers for the values of properties applied to the machine during provisioning, such as compute resourcename, the group must appear above **[Machine Provisioning]** in the policy.

- e. Specify the points at which the approval workflow returns to the requestor, who can decide whether to continue with the request or cancel it by using the **<<Owner>>** entry. Because the requestor can examine the custom properties of the machine at that point in the workflow, this

is useful when one or more approval groups includes one or more custom property values to be supplied by approvers. For instance, if an administrator assigns an additional cost to the machine, to be charged to the requestor's provisioning group, when approving a request, the requestor can see this value in the machine's properties and may decide to cancel the request so as not to incur the additional cost. This entry can be used more than once in a policy.

Once you create an approval policy, it becomes available in the **Approval Policy** drop-down menu.

Creating a Reservation Policy

A reservation policy is a collection of reservations of one type that can be selected in a blueprint to restrict all machine provisioning from that blueprint to the reservations in the policy. A reservation need not belong to a reservation policy, but can belong to only one.

Reservation policies are site-wide elements. Any user creating or editing a blueprint can select from among all existing reservation policies. If the provisioning group from which a blueprint is selected to request a machine has no appropriate reservations included in the reservation policy specified in the blueprint, provisioning fails.

Enterprise Administrators are responsible for managing reservation policies as necessary. You place a reservation in a reservation policy when you add or edit the reservation. Reservations can be moved among policies as needed.

To create a reservation policy:

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Reservation Policies**.
The table that appears shows all existing policies with their descriptions.
3. Click the **New Reservation Policy** link in the Reservation Policies title bar.
4. Provide a name and, optionally, a description.
5. Click the **Save** icon.

After you have created the reservation policy, you can assign it to reservations and blueprints.

Assigning a Reservation Policy to a Reservation

When you create a new reservation, you are given the option to assign a reservation policy. To assign a reservation policy to an existing reservation, you edit the reservation.

To assign a reservation policy to an existing reservation:

1. Log in to vCAC as an enterprise administrator.
2. Navigate to **Enterprise Administrator > Reservations**.
3. Point to the reservation you are adding to a reservation policy.
4. Click **Edit**.
5. Select a Reservation policy from the drop-down menu.
6. Click **OK**.

Once you have assigned a reservation policy to one or more reservations, you can use the policy in blueprints.

Assigning a Reservation Policy to a Blueprint

When you create a new blueprint, you are given the option to assign a reservation policy. To assign a reservation policy to an existing blueprint, you edit the blueprint.

To assign a reservation policy to a blueprint:

1. Log in to vCAC as an enterprise administrator or provisioning group manager.
2. Navigate to the Blueprints page.
 - As an enterprise administrator, select **Enterprise Administrator > Global Blueprints**.
 - As a provisioning group manager, select **Provisioning Group Manager > Blueprints**.
3. Point to the blueprint you want to edit.
4. Click **Edit**.
5. Select a Reservation policy from the drop-down menu.
6. Click **OK**.

The machines provisioned from your blueprint are restricted to the reservations associated with the selected reservation policy.

Viewing the Reservations Belonging to a Reservation Policy

To view the reservations belonging to a reservation policy:

1. Select **Enterprise Administrator > Reservations**
2. Select **Column > Reservation Policy** to add the Reservation Policy column to the Reservations list.

About Storage Reservation Policies

Having the ability to assign the volumes of a virtual machine to different datastores allows you to control and use storage space more effectively. For example, you might deploy the operating system volume to a slower, less expensive datastore and the database volume to a faster datastore.

You can assign a single datastore or a storage reservation policy representing multiple datastores to a volume. When you assign a single datastore to a volume, vCAC uses that datastore at provisioning time, if possible. When you assign a storage reservation policy to a volume, vCAC uses one of its datastores at provisioning time, if possible. A storage reservation policy is essentially a tag applied to one or more datastores. It allows you to group datastores that have similar characteristics, such as speed or price. A datastore can be assigned to only one storage reservation policy at a time, but a storage reservation policy can have many different datastores.

The enterprise administrator creates a storage reservation policy and assigns it to one or more datastores. The enterprise administrator or provisioning group manager then assigns the storage reservation policy to a volume in a virtual blueprint. When a user requests a virtual machine that uses the blueprint, vCAC uses the storage reservation policy specified in the blueprint to select a datastore for the machine's volume.

You can do the following with datastores when adding or editing a volume in a virtual blueprint:

- Assign a single datastore to the volume. This one-to-one relationship allows vCAC to assign only the specified datastore at provisioning time. If the datastore is not available or lacks sufficient space, provisioning fails.
- Assign a storage reservation policy to the volume. This allows vCAC to select one of the datastores associated with the storage reservation policy at provisioning time. If the policy's datastores are unavailable or lack sufficient space, provisioning fails.
- Not assign a datastore or a storage reservation policy to a volume. This allows vCAC to select from all available datastores at provisioning time. Provisioning fails if a datastore with sufficient space is not available.

vCAC also uses a datastore's priority (as assigned by its reservation) to select a datastore from among eligible datastores at provisioning time.

You should avoid specifying a storage path and a storage reservation policy for the same volume, though there may be times when this is necessary. If you must specify a storage path and a storage reservation policy for the same volume, the storage path takes precedence over the storage reservation policy.

Creating a Storage Reservation Policy

An Enterprise Administrator can create, update, delete, and assign a storage reservation policy.

To create a storage reservation policy:

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Reservation Policies**.
3. Click the **New Storage Reservation Policy** link in the Storage Reservation Policies title bar.
4. Provide a name and, optionally, a description.
5. Click the **Save** icon to save your changes.

The new storage reservation policy appears at the bottom of the page. You can assign it to a compute resource.

Assigning Storage Reservation Policies to a Compute Resource

A storage reservation policy must be assigned to one or more datastores before you can use it with a volume. Assigning a storage reservation policy to multiple datastores creates an exclusive group of datastores for use with a blueprint.

An Enterprise Administrator can assign storage reservation policies to datastores on the Compute Resources page.

To assign a storage reservation policy to a datastore:

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Compute Resources**.
3. Point to an existing compute resource and click **Edit**.
4. Click the **Configuration** tab.
5. In the **Storage Path** column, click the edit icon next to the datastore you want to assign to a storage reservation policy.
6. In the **Storage Reservation Policy** column, from the drop-down menu you can select the storage reservation policy to assign to the datastore.
7. To assign storage reservation policies to additional datastores, repeat steps 4 and 5.
8. Click the **Save** icon to save the assignment.
9. Click **OK** to save the configuration.

Creating Build Profiles

A build profile is a set of properties applied to a machine when it is provisioned. These properties may determine the specification of the machine, the manner in which it is provisioned, operations to be performed after it is provisioned, or management information about it maintained within vCAC.

All build profiles are available to all provisioning groups. This makes it possible for a profile to serve as the basis for a set of similar blueprints within a provisioning group or across provisioning groups. An incorpo-

rated build profile is always read at machine build time, so the current version is always used no matter when the build profile was first incorporated in a blueprint.

For example, you may want to use WIM-based provisioning to provision similar machines with varying specifications (amount of memory or storage, number of disks to divide the storage between) from the same WIM image and WinPE ISO. In this case, properties that are shared between these blueprints—such as the names and locations of the WIM image and WinPE ISO—can be placed into a build profile, that can then be incorporated into multiple WIM-based provisioning blueprints (global or local).

You can create more than one build profile for a blueprint. Users can select from a list of build profiles on the Properties tab.

To place the properties you need into a build profile:

1. Log in to vCAC as an Enterprise Administrator.
2. Select **Enterprise Administrator > Build Profiles**.
3. Click the **New Build Profile** link in the title bar.
4. Type a name and, optionally, a description for the profile.
5. Specify the set of custom properties to include in this profile.

Note: When entering custom properties, always ensure that property values do not contain trailing spaces, as these may cause provisioning to fail.

6. (Optional) Select **Prompt User** to require the user to provide a value for the property or accept the value you supply as the default.

If you leave the value empty, the user must supply a value to use this property and continue with the machine request.

Note: When **Prompt User** is selected for a property, the requesting user is prompted only once for the value, even when requesting more than one machine. The value supplied is applied to all machines provisioned from the request. Selecting **Prompt User** for the Hostname property, restricts all requests from the blueprint to a single machine because the value of this property must be unique for each machine.

7. The **Encrypt** check box ensures that a secure property (such as a password) is never visible in plain text.
8. Click the **Save** icon to save the property.
9. Click **OK** to save the build profile.

Chapter 5 Managing KVM (RHEV) Machines

5

After you have provisioned a machine using KVM (RHEV), you can perform machine operations on it. For information about operations you can perform as a machine owner, provisioning group manager, or enterprise administrator, see the *vCloud Automation Center Operating Guide*.

Connecting to a KVM (RHEV) Machine's Console

You can connect to your provisioned machines using RDP (for Windows) or SSH (for Linux), as described in the *vCloud Automation Center Operating Guide*. For machines provisioned using KVM (RHEV), you can also connect to the console using VNC or spice.

By default, machines provisioned using vCAC use VNC. If you override this default using the custom property **VirtualMachine.Admin.OverrideVncConsole**, the console display type is spice.

Prerequisites

- A VNC or spice client must be installed on the machine from which you want to access the virtual machine.

To connect to a virtual machine's console:

1. Log in to the vCAC Console as a machine owner.
2. Click **Self-Service > My Machines**.
3. Point to the name of the machine to which you want to connect, and click **Show Console Ticket**.
The Show Console Ticket page displays.
4. Click **Request Now**.

The page refreshes with information that you can use to connect using a VNC client.

Note: The password is generated each time you click **Request Now** and is valid for 120 seconds. If the password has expired, click **Request Now** to generate a new password.

5. Launch the VNC or spice client.
6. Specify the **Address**, **Port**, and **Password** shown in the console ticket details to connect to the machine.

Glossary

AB blueprint

A specification for provisioning virtual or physical machines, determining the machines characteristics and the policies applied to it. A *local* blueprint belongs to a single provisioning group and can be used only by its members. A *global* blueprint is available to all provisioning group managers.

build profile

A set of custom properties that can be incorporated into blueprints.

C cloud machine

A virtual machine provisioned by a cloud service on its own hardware and network.

cloud reservation

Access to the provisioning services of a cloud service account for a particular provisioning group.

D Distributed Execution Manager (DEM)

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

EF endpoint

Information required for access to a group of virtualization compute resources to be managed by a vCAC proxy agent; to a cloud service account to be managed by vCAC; or to one or more physical management interfaces, including those of physical machines to be provisioned in vCAC and those of devices.

Enterprise Administrator

A global administrator who manages virtualization compute resources and physical machines, virtual, cloud and physical reservations, provisioning groups, global blueprints, build profiles, reservation policies, approval policies and other global elements, and tracks resource usage and reclaims machines as needed.

enterprise group

A group of virtualization compute resources and cloud endpoints managed by one or more Enterprise Administrators.

- GHI** global administrator
One of several vCAC roles responsible for setting up and maintaining the vCAC site so provisioning groups members can request and use machines.
- JKM** Model Manager
The Model Manager is used to create and manage custom models, which facilitate integration of vCAC with external entities and implement custom business processes. The Model Manager communicates with the vCAC database, vCAC console and Distributed Execution Managers (DEMs).
- OP** physical machine
A hardware system managed by vCAC that can be or has been provisioned with an operating system by vCAC.
- physical reservation
A set of physical machines reserved for provisioning by a particular provisioning group.
- provisioning group
A collection of machine consumers, typically corresponding to a line of business, department or other organizational group.
- Provisioning Group Manager (PGM)
A member of a provisioning group who maintains blueprints for the group and approves some machine requests
- proxy agent
The means by which vCAC communicates with a virtualization platform and the compute resources on which it provisions virtual machines, including regular collection of data about compute resources and machines.
- QRS** reservation policy
A collection of reservations that can be selected in a blueprint to restrict machine provisioning to the reservations in the policy; often used to group like resources to create defined service levels, or to make a specific type of resource easily available for a particular purpose.
- TUV** 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 can be local or remote.
- vCAC Manager Service
The vCloud Automation Center service (commonly called the Manager Service) coordinates vCAC communication between vCAC agents (including proxy agents), the vCAC database and SMTP.
- vCAC role
A global administrator assignment or provisioning group membership within vCAC that determines which vCAC activities are available to a user; a single user can be in multiple roles.
- vCAC web console
The browser-based interface to vCAC for machine owners and administrators.

vCAC workflow

A description of the activities (logical units of work) that make up a complex task, including order of execution and dependent relationships between them and the people or systems that perform them. vCAC uses workflows to define its machine provisioning and management processes. The master workflow defines all the states and stages within the machine lifecycle and is optimized to support long running, dynamic tasks; provisioning workflows define the process of building or cloning a machine and are specified in blueprints.

virtual machine

A computer system implemented entirely in software, using resources provided by one or more hardware systems.

virtual reservation

A share of one virtualization compute resource's resources dedicated to a particular provisioning group for use in provisioning virtual machines.

virtualization compute resource

A vCAC object representing a host, host cluster or pool within a virtualization platform on which virtual machines requested by vCAC users are provisioned.

virtualization platform

A catch-all term for a virtualization technology with which vCAC directly interacts, whether it is a virtualization manager (such as VirtualCenter) or a hypervisor of one type or another (such as XenServer and Hyper-V).

Index

A

- about RHEV **4**
- about vCAC **3**
- access administrators **5**
- approvals
 - create approval group **30**
 - create approval policy **31**
 - delete group or policy **29**
 - edit group or policy **29**
 - export information **29**
 - manage **29**
- approvers **5**

B

- basic blueprint information **22**
- basic KVM (RHEV) blueprint
 - build information **22**
 - create **21**
 - properties **23**
 - security information **23**
- blueprint
 - global **19**
 - local **19**
 - overview **19**
- build profile
 - create **35**
 - overview **34**

C

- clone KVM (RHEV) blueprint
 - basic information **26**
 - build information **22, 26**
 - properties **27**
 - security information **27**
- compute resource
 - standards for names **11**
- configure
 - approvals **29**
 - user credentials for KVM (RHEV) **8**
- console display **37**
- create
 - approval group **30**
 - approval policy **31**
 - basic KVM (RHEV) blueprint **21**
 - build profile **35**
 - enterprise group **10**

- KVM (RHEV) clone blueprint **26**
- KVM (RHEV) endpoint **8**
- KVM (RHEV) reservation **15**
 - machine prefix **11**
 - provisioning group **11**
 - reservation policy **32**
 - storage reservation policy **34**
 - template **25**
- custom properties **19**

D

- data collection
 - endpoint **4**
 - inventory **4**
 - state **4**
- DEM worker **7**

E

- enable WMI agents **7**
- endpoint data collection
 - start manually **9**
- enterprise administrators **5, 6**
- enterprise group **10**

G

- global administrators **6**

K

- KVM (RHEV) compute resources **5**
- KVM (RHEV) endpoint
 - create **8**
 - import **9**
- KVM (RHEV) endpoints **4**
- KVM (RHEV) integration
 - available workflows **21**
 - custom properties **19**
- KVM (RHEV) reservation
 - create **15**
 - delete **17**
 - edit **17**
 - view **17**
 - view machines **17**

M

- machine name limitations **11**
- machine prefix
 - create **11**

manage **11**
machine prefixes **10**

O

overview of
approval policies **6**
blueprint **19**
build profile **34**
provisioning groups **11**
reservation policy **32**
reservations **14**
RHEV **4**
storage reservation policy **33**
vCAC **3**
virtual machine **3**

P

provisioning group
create **11**
delete **14**
edit **14**
overview **5**
view **13**
provisioning process **6**

R

remote WMI requests **7**
required KVM (RHEV) configuration **7**
reservation policy **6**
assign to blueprint **32**
assign to reservation **32**
create **32**
overview **32**
RHEV (KVM) configuration **7**

S

standards for host names **11**
start endpoint data collection **9**
storage reservation policy
assign **34**
create **34**
overview **33**

T

template for provisioning **25**

U

user credentials for KVM (RHEV) **8**

V

vCAC administrator **5**
VirtIO
drivers **24**
virtual reservation **6**

VNC **37**

W

WIM-based provisioning
prepare for **24**
workflows for KVM (RHEV) blueprints **21**