IaaS Configuration for Multi-Machine Services

vCloud Automation Center 6.0.0

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-001313-01

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

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

Contents

IaaS Configuration for Multi-Machine Services

The *IaaS Configuration for Multi-Machine Services* describes how to integrate multi-machine services in an existing VMware vCloud® Automation Center™ deployment.

This documentation is intended to be used with the following prerequisite guides:

- *IaaS Configuration for Virtual Platforms*

- *IaaS Configuration for Cloud Platforms*

- *IaaS Configuration for Physical Machines*

This documentation guides you through the following processes:

- Preparing for provisioning

- Creating multi-machine blueprints

All of the IaaS configuration steps that should be completed prior to machine provisioning are included in this document and its prerequisite guides. For information about managing provisioned machines, see *Tenant Administration*.

NOTE   Not all features and capabilities of vCloud Automation Center are available in all editions. For a comparison of feature sets in each edition, see https://www.vmware.com/products/vcloud-automation-center/.

Intended Audience

This information is intended for Infrastructure as a Service (IaaS) administrators, tenant administrators and business group managers, and fabric administrators seeking to integrate multi-machine services into their vCloud Automation Center deployment. It is written for experienced Windows or Linux system administrators who are familiar with virtualization technology and the basic concepts described in *Foundations and Concepts*.

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.

Using the Goal Navigator

The goal navigator guides you through high-level goals that you might want to accomplish in vCloud Automation Center.

The goals you can achieve depend on your role. To complete each goal, you must complete a sequence of steps that are presented on separate pages in the vCloud Automation Center console.

The goal navigator can answer the following questions:

- Where do I start?

- What are all the steps I need to complete to achieve a goal?

- What are the prerequisites for completing a particular task?

- Why do I need to do this step and how does this step help me achieve my goal?

The goal navigator is hidden by default. You can expand the goal navigator by clicking the icon on the left side of the screen.

After you select a goal, you navigate between the pages needed to accomplish the goal by clicking each step. The goal navigator does not validate that you completed a step, or force you to complete steps in a particular order. The steps are listed in the recommended sequence. You can return to each goal as many times as needed.

For each step, the goal navigator provides a description of the task you need to perform on the corresponding page. The goal navigator does not provide detailed information such as how to complete the forms on a page. You can hide the page information or move it to a more convenient position on the page. If you hide the page information, you can display it again by clicking the information icon on the goal navigator panel.

Introduction to Multi-Machine Services

1

The multi-machine services feature of VMware vCloud® Automation Center™ allows users to provision multi-machine services, and their component machines, in a virtual datacenter based on existing templates.

Multi-machine services are compound services comprised of multiple machines that can be provisioned and managed with vCloud Automation Center as a single entity.

For example, in a tiered application deployment, you might have one or more database servers, one or more application servers, and multiple web servers. In addition to creating blueprints for each of the server types, you can also create a multi-machine blueprint that includes all the machines that are needed for the entire application deployment. Users can then provision the multi-machine service and perform actions, such as rebooting, on all the component machines with a single action.

Multi-machine services are containers for their component machines. Component machines can be virtual, physical, or cloud, or any combination of the three.

The following characteristics describe multi-machine services in vCloud Automation Center:

- They are defined by a blueprint that references one or more component blueprints.

- They can have a lease duration associated with them.

- They are not counted as a machine in reports or licensing but their component machines are counted.

- Requests can be made subject to approval.

- Many machine operations, such as reboot, can be performed on the multi-machine service as a whole. The requested action is performed on all of the components in the service.

Some blueprint types, such as vCloud Director blueprints, cannot be added as components of a multi-machine blueprint.

This chapter includes the following topics:

- "Multi-Machine Concepts," on page 7

- "Multi-Machine Service Life Cycle," on page 8

- "Comparison of Multi-Machine Services and vCloud Director vApps," on page 9

Multi-Machine Concepts

These concepts apply to multi-machine services in vCloud Automation Center.

For more information about these core concepts, see *Foundations and Concepts*.

Component Blueprint

A machine blueprint that is part of a multimachine service. A component blueprint is referenced by a multi-machine blueprint. You can also use it to request standalone machines that are not part of a multimachine service.

Component Machine

A machine that is managed as part of a multimachine service. A multimachine service might include several component machines.

MultimachineBlueprint

A blueprint that defines a mutlimachine service.

MultimachineService

A compound service composed of multiple machines that vCloud Automation Center can provision and manage as a single entity.

Multi-Machine Service Life Cycle

Multi-machine services follow the same general life cycle as individual machines, from requesting and provisioning through managing and decommissioning.

A multi-machine blueprint contains references to blueprints for the component machines. For each component blueprint, it specifies the minimum and maximum number of machines for the multi-machine service.

A multi-machine blueprint can specify scripts, or workflows, to execute during the provisioning process or when powering the multi-machine service on or off. Scripts are executed by Distributed Execution Manager worker services or agents, not the component machines.

When users request a multi-machine service, they can specify the following settings:

- How many component machines to provision, based on limits specified in the multi-machine blueprint

- Specifications for the component machines, such as CPU, memory, and storage, based on the individual component blueprints

- General settings, such as lease duration and custom properties, to be applied to component machines in the multi-machine service

Before provisioning the multi-machine service, vCloud Automation Center allocates resources for all of the component machines. If the multi-machine service would cause a reservation to become over-allocated, its provisioning fails. After the resources are allocated, the component machines are provisioned and powered on.

After the multi-machine service is provisioned, the machine owner can perform various machine menu tasks on the multi-machine service as a whole, such as powering the multi-machine service off and on, or destroying the multi-machine service and its component machines.

If the multi-machine blueprint allows for a varying number of machines for any component type, the machine owner can add or delete machines from the multi-machine service after it is provisioned.

The machine owner can view the components that make up a multi-machine service and manage them as a group or individually. Most machine operations are available for individual component machines, except for changing the owner or lease.

These operations are inclusive to the multi-machine service and modify the group as a whole. Conversely, some actions are inclusive to the individual components, such as suspending, redeploying, and connecting using Microsoft Remote Desktop Protocol or VMware Remote Console.

Comparison of Multi-Machine Services and vCloud Director vApps

vCloud Automation Center offers two primary ways to provision multiple machines as a single service. You can use vCloud Automation Center multi-machine services or vCloud Director vApps to group component machines.

The following table shows how entities are mapped between the two features.

Table 1-1. Comparison of Features

vCloud Automation Center Multi-Machine Service	vCloud Director vApp
Create a multi-machine blueprint that references individual machine blueprints in vCloud Automation Center.	Leverage existing vApp templates created in vCloud Director.
Provision machines of any type (virtual, physical, or cloud) as part of a service.	Provision virtual machines by using the vCloud Director interface only.
Manage component machines of a multi-machine service by using vCloud Automation Center.	Manage vApp virtual machines by using vCloud Automation Center.
Access to the component portal for Microsoft Remote Desktop Protocol, Virtual Network Computing, and SSH depends on the guest and console and the endpoint, for example VMware Remote Console for vSphere.	Access to the component portal for Microsoft Remote Desktop Protocol, Virtual Network Computing, and SSH depends on the guest and console and the endpoint, for example VMware Remote Console for vCloud Director.
Application-specific networks may be defined in a multi-machine blueprint for vCloud Networking and Security and NSX.	Application-specific networks are defined in a vApp.
Component machines can be added or removed after initial provisioning.	Component machines cannot be added or removed after initial provisioning.
vCloud Automation Center defines startup and shutdown order.	The vApp template defines startup and shutdown order.

Configuring IaaS for Multi-Machine Services

2

Administrators and managers bring resources under vCloud Automation Center management, allocate resources for users, and prepare for machine provisioning.

This chapter includes the following topics:

Configuring IaaS for Multi-Machine Services Overview

IaaS administrators, tenant administrators or business group managers, and fabric administrators perform required and optional configurations to implement multi-machine services in vCloud Automation Center.

The following is a high-level overview of the steps required to integrate multi-machine services into an existing vCloud Automation Center deployment.

See the following documents for prerequisite information about how to create the necessary network profiles, fabric groups, business groups, reservation policies, and machine endpoints.

- *IaaS Configuration for Virtual Platforms*
- *IaaS Configuration for Cloud Platforms*
- *IaaS Configuration for Physical Machines*

In the following step sequence, cited topics that are not linked to this guide are located in one of the above listed documents.

1   An IaaS administrator configures credentials and endpoints to bring resources under vCloud Automation Center management. See *Bringing Resources Under vCloud Automation Center Management*.

2   A fabric administrator configures the machine prefixes used to create names for machines provisioned by vCloud Automation Center. See *Configure Machine Prefixes*.

3   A tenant administrator creates at least one business group of users who can request machines. See *Create a Business Group*.

4   A fabric administrator creates at least one reservation to allocate resources to a business group. See *Create a Reservation*.

   Create reservations for all the resources that can be used in multi-machine services in the same business group. To ensure that component machines are provisioned on the appropriate resources, use reservation policies to associate specific reservations with each blueprint that is a component of a multi-machine service.

5   Depending on your intended method of provisioning, preparation outside of vCloud Automation Center might be required. For example, if you intend to provision by cloning, create a template and customization object. See *Preparing for Provisioning*.

6   A tenant administrator or business group manager creates machine blueprints. They can then create multi-machine blueprints. See "Create a Multi-Machine Blueprint," on page 27.

NOTE   Users who are enabled to provision machines with a specific multi-machine blueprint must be part of the same business group.

---

7   A fabric administrator can create storage reservation policies to group datastores that have similar characteristics, such as speed or price. See *Configure a Storage Reservation Policy*.

8   A tenant administrator or business group manager can configure advanced blueprint settings. See *Configuring Advanced Blueprint Settings*.

Before users can request machines, a tenant administrator must configure the service catalog. See *Tenant Administration*.

Managing Network and Security Virtualization

Network and security virtualization allows virtual machines to communicate with each other over physical and virtual networks securely and efficiently.

vCloud Automation Center supports virtualized networks based on the vCloud Networking and Security and NSX platforms.

A fabric administrator can create external network profiles to define existing physical networks, and create templates of NAT, routed, and private network profiles. Network templates define network specifications such as subnet masks, gateway IP addresses, DNS/WINS and DHCP settings, and static IP ranges.

A tenant administrator or business group manager can use the templates to define multi-machine service networks. In a multi-machine blueprint, you can configure network adapters and load balancing for all components provisioned from that multi-machine blueprint.

In the multi-machine blueprint, you select a transport zone which identifies the vSphere endpoint. The multi-machine blueprint and the reservations used in the provisioning must have the same transport zone setting. Transport zones are defined in the NSX and vCloud Networking and Security environments.

Create an Endpoint for Network and Security Virtualization

An IaaS administrator creates a combined instance of a vSphere endpoint and a vCloud Networking and Security or NSX endpoint.

You can optimize this solution for audit and troubleshooting by creating a service account on vSphere and vCloud Networking and Security or NSX so that a clear audit trail can be tied back to vCloud Automation Center.

Prerequisites

■   Log in to the vCloud Automation Center console as an **IaaS administrator**.

■   A system administrator must have installed a vCloud Networking and Security or NSX instance, and that instance must be accessible when you create the endpoint for network and security virtualization.

■   An IaaS administrator must have created a vSphere endpoint. The vSphere server targeted by the endpoint must be configured to communicate with the vCloud Networking and Security or NSX instance.

- An IaaS administrator must have created credentials for the vCloud Networking and Security or NSX management console to be used as the endpoint. These credentials can be the same ones used for logging on to vSphere.

Procedure

1 Select **Infrastructure > Endpoints > Endpoints**.

2 Locate a vSphere endpoint and click **Edit** in the drop-down menu.

3 Select the **Specify manager for network and security platform** check box.

  A set of text boxes for the new manager appear.

4 Type the URI for the management console of the vCloud Networking and Security or NSX platform in the **Address** text box.

5 Click the **Credentials** text box and select the necessary credentials.

6 Click **OK**.

7 Click **OK**.

Create a Reservation for Network and Security Virtualization

An IaaS administrator can use a reservation to assign external networks and routed gateways to network profiles for basic and multi-machine networks, specify the transport zone, and assign security groups to multi-machine components.

In the reservation, you specify a transport zone to indicate the diameter and scope of the compute infrastructure available for network virtualization. You can also assign external networks and routed gateways to specify how application tiers connect to external networks.

When vCloud Automation Center provisions a multi-machine service with NAT, routed, or private networking, it provisions a routed gateway as the network router for that service. The routed gateway is a management machine that consumes compute resources like other virtual machines but manages the network communications for the multi-machine components. The reservation used to provision the routed gateway determines the external network used for NAT and routed network profiles. It also determines the reservation routed gateway used to configure routed networks. The reservation routed gateway links routed networks together with entries in the routing table.

You can specify a routed gateway reservation policy in the multi-machine blueprint to identify which reservations to use when provisioning the multi-machine routed gateway. By default, vCloud Automation Center uses the same reservations for the routed gateway and the multi-machine components.

You select one or more security groups in the reservation to enforce baseline security policy for all component machines provisioned with that reservation in vCloud Automation Center. This means that every component machine provisioned with the relevant reservation is added to these specified security groups.

Successful provisioning of components requires the transport zone of the reservation to match the transport zone of a multi-machine blueprint when that blueprint defines multi-machine networks. Similarly, provisioning a multi-machine router gateway requires matching transport zones for the reservation and the multi-machine blueprint.

When selecting a reservation routed gateway and network profile on a reservation for configuring routed networks, select the network path to be used in linking routed networks together and assign it the external network profile that was used to configure the routed network profile. The list of network profiles available to be assigned to a network path is filtered to match the subnet of the network path based on the subnet mask and primary IP address selected for the network interface. The routed gateway must be configured in the NSX or vCloud Networking and Security environment and vCNS Inventory data collection must have run.

Prerequisites

- Log in to the vCloud Automation Center console as an **IaaS administrator**.

- A tenant administrator must have created a business group. For information on creating a business group, see *IaaS Configuration for Virtual Platforms*.

- An IaaS administrator must have created a vCloud Networking and Security or NSX endpoint. See

Procedure

1 Select **Infrastructure > Reservations > Reservations**.

2 Select **New Reservation > Virtual > vSphere (vCenter)**.

3 Click the **Reservation Information** tab.

4 Select a compute resource from the **Compute resource** drop-down menu.

   The reservation name appears in the Name text box.

5 Select a tenant from the **Tenant** drop-down menu.

6 Select a business group from the **Business group** drop-down menu.

7 (Optional) Select a reservation policy from the **Reservation policy** drop-down box.

   You use a reservation policy to restrict provisioning to specific reservations, such as assigning this reservation to the routed gateway of a multi-machine service.

8 Type a priority level in the **Priority** text box, or click the up and down arrows.

9 Click the **Network** tab.

10 Assign an external network profile to an external, physical network.

   a Select the check box for an external network in the **Network Paths** table.

   b Select an external network profile from the **Network Profile** drop-down menu.

   c Repeat steps a through c to enable additional physical networks on this reservation.

11 Select a transport zone from the **Transport zone** drop-down menu.

   The transport zones in a reservation and a multi-machine blueprint must match for provisioning to occur.

12 Select the check boxes of the security group or groups you want to assign to the reservation in the **Security groups** list.

13 (Optional) Select a routed gateway, if needed.

   a Select the check box of a routed gateway in the **Routed Gateways** table.

      The selected routed gateway becomes editable.

   b Select a network path from the **Network Path** drop-down menu.

 c Select an external network profile from the **Network Profile** drop-down menu.

  Only the external network profiles used to create routed network profiles are available in the menu.

 d Click the **Save** icon ( ).

 e Repeat steps a through e to select more routed gateways, if needed.

14 Click **OK**.

Creating a Network Profile

A fabric administrator creates external network profiles and templates for NAT, routed, and private network profiles.

Fabric administrators create network profiles to define existing, physical networks and networks for virtual machines provisioned as part of multi-machine services. A network profile can define one of four types of networks.

- External networks are existing physical networks configured on the vSphere server. They are the external part of the NAT and Routed types of networks. An external network profile can define a range of static IP addresses available on the external network. An external network profile with a static IP range is a prerequisite for NAT and routed networks.

- NAT (Network Address Translation) virtual networks are created at provisioning time. They are networks that use one set of IP addresses for external communication and another set for internal communications. With one-to-one NAT networks, every virtual machine is assigned an external IP address from the external network profile and an internal IP address from the NAT network profile. With one-to-many NAT networks, all machines share a single IP address from the external network profile for external communication. A NAT network profile defines local and external networks that use a translation table for mutual communication.

- Routed virtual networks are created at provisioning time. They represent a routable IP space divided across subnets that are linked together with a routing table. Every new routed network has the next available subnet assigned to it and an entry in the routing table to connect it to other routed networks that use the same network profile. The virtual machines that are provisioned with routed networks that have the same routed network profile are able to communicate with each other and the external network. A routed network profile defines a routable space and available subnets.

- Private virtual networks are created at provisioning time. They are internal networks that have no connection to external, public networks. The virtual machines in a private network communicate only with each other. You can communicate with a virtual machine in a private network with the VMRC option in vCloud Automation Center. A private network profile defines an internal network, ranges of static IP addresses, and a range of DHCP addresses.

In general, vCloud Automation Center uses vSphere DHCP to assign IP addresses to the machines it provisions, regardless of which provisioning method is used. When provisioning virtual machines by cloning or using kickstart/autoYaST provisioning, however, the requesting machine owner can assign static IP addresses from a predetermined range.

Fabric administrators specify the ranges of IP addresses that can be used in network profiles. Each IP address in the specified ranges allocated to a machine is automatically reclaimed for reassignment when the machine is destroyed and the ReclaimDestroyedStaticIPAddresses workflow executes.

A fabric administrator creates external network profiles and templates for NAT, private, and routed network profiles on the Network Profiles page. A tenant administrator or business group manager creates NAT, private, and routed network profiles in multi-machine blueprints for use in configuring network adapters and load balancers for the multi-machine components.

Create an External Network Profile

A fabric administrator can create an external network profile to define external network properties and a range of static IP addresses.

Prerequisites

Log in to the vCloud Automation Center console as a **fabric administrator**.

Procedure

1 Specify Network Profile Information on page 16

The network profile information identifies the external network properties and specifies settings for an existing network. An external network profile is a requirement of NAT and routed network profiles.

2 Configure IP Ranges on page 16

A fabric administrator can define zero or more ranges of static IP addresses for use in provisioning a network. An external network profile must have at least one static IP range for use with routed and NAT network profiles.

Specify Network Profile Information

The network profile information identifies the external network properties and specifies settings for an existing network. An external network profile is a requirement of NAT and routed network profiles.

Prerequisites

Log in to the vCloud Automation Center console as a **fabric administrator**.

Procedure

1 Select **Infrastructure > Reservations > Network Profiles**.

2 Select **New Network Profile > External**.

3 Type a **Name** and, optionally, a **Description**.

4 Type a mask address in the **Subnet mask** text box.

For example, 255.255.0.0.

5 Type an IP address in the **Gateway** text box.

You must have a gateway IP address to add an IP range.

6 In the DNS/WINS group, type values as needed.

What to do next

You can "Configure IP Ranges," on page 20 for static IP addresses.

Configure IP Ranges

A fabric administrator can define zero or more ranges of static IP addresses for use in provisioning a network. An external network profile must have at least one static IP range for use with routed and NAT network profiles.

Prerequisites

"Specify Network Profile Information," on page 16.

Procedure

1 Click the **IP Ranges** tab.

2   Click **New Network Range**.

The New Network Range dialog box appears.

3   Type a **Name** and, optionally, a **Description**.

4   Type an IP address in the **Starting IP address** text box.

5   Type an IP address in the **Ending IP address** text box.

6   Click **OK**.

The newly defined IP address range appears in the Defined Ranges list. The IP addresses in the range appear in the Defined IP Addresses list.

7   (Optional) Upload one or more IP addresses from a CSV file, if available.

A row in the CSV file has the format *ip_address,mname,status*.

CSV Field	Description
ip_address	An IP address
mname	Name of a managed machine in vCloud Automation Center. If the field is empty, defaults to no name.
status	Allocated or Unallocated, case-sensitive. If the field is empty, defaults to Unallocated.

a   Click **Browse** next to the **Upload CSV** text box.

b   Navigate to the CSV file and click **Open**.

c   Click **Process CSV File**.

The uploaded IP addresses appear in the Defined IP Addresses list. If the upload fails, diagnostic messages appear that identify the problems.

8   (Optional) Click in the **Defined IP Addresses** text boxes and type a partial address or name, or select a date from the popup calendar, to filter the view of IP address entries to only those that match.

9   Click **OK**.

Create a Private Network Profile

A fabric administrator can create a private network profile template to define an internal network and assign ranges of static IP and DHCP addresses to it.

Prerequisites

Log in to the vCloud Automation Center console as a **fabric administrator**.

Procedure

1   Specify Network Profile Information on page 18

The network profile information identifies the private network profile and settings for an internal network.

2   Configure IP Ranges on page 18

A fabric administrator can define one or more ranges of static IP addresses for use in provisioning a network.

Specify Network Profile Information

The network profile information identifies the private network profile and settings for an internal network.

Prerequisites

Log in to the vCloud Automation Center console as a **fabric administrator**.

Procedure

1 Select **Infrastructure > Reservations > Network Profiles**.

2 Select **New Network Profile > Private**.

3 Type a **Name** and, optionally, a **Description**.

4 Type a mask address in the **Subnet mask** text box.

For example, 255.255.0.0.

5 Type an IP address in the **Gateway** text box.

6 (Optional) In the DHCP group, select the **Enabled** check box and type the values, as needed.

The DHCP range cannot overlap the range of static IP addresses. Lease time defines how long a machine can use an IP address.

What to do next

You can "Configure IP Ranges," on page 18 for static IP addresses.

Configure IP Ranges

A fabric administrator can define one or more ranges of static IP addresses for use in provisioning a network.

Prerequisites

"Specify Network Profile Information," on page 16.

Procedure

1 Click the **IP Ranges** tab.

2 Click **New Network Range**.

The New Network Range dialog box appears.

3 Type a **Name** and, optionally, a **Description**.

4 Type an IP address in the **Starting IP address** text box.

5 Type an IP address in the **Ending IP address** text box.

6 Click **OK**.

The newly defined IP address range appears in the Defined Ranges list. The IP addresses in the range appear in the Defined IP Addresses list.

7 (Optional) Upload one or more IP addresses from a CSV file, if available.

A row in the CSV file has the format *ip_address*,*mname*,*status*.

CSV Field	Description
ip_address	An IP address
mname	Name of a managed machine in vCloud Automation Center. If the field is empty, defaults to no name.
status	Allocated or Unallocated, case-sensitive. If the field is empty, defaults to Unallocated.

    a   Click **Browse** next to the **Upload CSV** text box.

    b   Navigate to the CSV file and click **Open**.

    c   Click **Process CSV File**.

    The uploaded IP addresses appear in the Defined IP Addresses list. If the upload fails, diagnostic messages appear that identify the problems.

8   (Optional) Click in the **Defined IP Addresses** text boxes and type a partial address or name, or select a date from the popup calendar, to filter the view of IP address entries to only those that match.

9   Click **OK**.

Create a NAT Network Profile

A fabric administrator can create a NAT network profile template to define a NAT network and assign ranges of static IP and DHCP addresses to it.

Prerequisites

Log in to the vCloud Automation Center console as a **fabric administrator**.

Procedure

1   Specify Network Profile Information on page 19

    The network profile information identifies the NAT network properties, its underlying external network profile, the NAT type, and other values used in provisioning the network.

2   Configure IP Ranges on page 20

    A fabric administrator can define one or more ranges of static IP addresses for use in provisioning a network.

Specify Network Profile Information

The network profile information identifies the NAT network properties, its underlying external network profile, the NAT type, and other values used in provisioning the network.

Prerequisites

■   Log in to the vCloud Automation Center console as a **fabric administrator**.

■   "Create an External Network Profile," on page 16.

Procedure

1   Select **Infrastructure > Reservations > Network Profiles**.

2   Select **New Network Profile > NAT**.

3   Type a **Name** and, optionally, a **Description**.

4   Select an external network profile from the drop-down menu.

5   Select a NAT type from the drop-down menu.

Option	Description
One-to-One	Assign an external static IP address to each network adapter. Every machine can access the external network and is accessible from the external network.
One-to-Many	One external IP address is shared among all machines on the network. An internal machine can have either DHCP or static IP addresses. Every machine can access the external network, but no machine is accessible from the external network. Selecting this option enables the **Enabled** check box in the DHCP group.

6   Type a mask address in the **Subnet mask** text box.

For example, 255.255.0.0.

7   Type an IP address in the **Gateway** text box.

The gateway address is required for a one-to-one NAT network profile.

8   (Optional) In the DNS/WINS group, type values as needed.

The external network profile provides these values, which you can edit.

9   (Optional) In the DHCP group, select the **Enabled** check box and type the values as needed.

You can select the check box only if you set the NAT type to one-to-many.

What to do next

A NAT network profile requires DHCP information or an IP range. For information on creating an IP range, see "Configure IP Ranges," on page 20.

Configure IP Ranges

A fabric administrator can define one or more ranges of static IP addresses for use in provisioning a network.

Prerequisites

"Specify Network Profile Information," on page 16.

Procedure

1   Click the **IP Ranges** tab.

2   Click **New Network Range**.

The New Network Range dialog box appears.

3   Type a **Name** and, optionally, a **Description**.

4   Type an IP address in the **Starting IP address** text box.

5   Type an IP address in the **Ending IP address** text box.

6   Click **OK**.

The newly defined IP address range appears in the Defined Ranges list. The IP addresses in the range appear in the Defined IP Addresses list.

7   (Optional) Upload one or more IP addresses from a CSV file, if available.

A row in the CSV file has the format *ip_address,mname,status*.

CSV Field	Description
ip_address	An IP address
mname	Name of a managed machine in vCloud Automation Center. If the field is empty, defaults to no name.
status	Allocated or Unallocated, case-sensitive. If the field is empty, defaults to Unallocated.

a   Click **Browse** next to the **Upload CSV** text box.

b   Navigate to the CSV file and click **Open**.

c   Click **Process CSV File**.

The uploaded IP addresses appear in the Defined IP Addresses list. If the upload fails, diagnostic messages appear that identify the problems.

8   (Optional) Click in the **Defined IP Addresses** text boxes and type a partial address or name, or select a date from the popup calendar, to filter the view of IP address entries to only those that match.

9   Click **OK**.

Create a Routed Network Profile

A fabric administrator can create a routed network profile to define a routable IP space and available subnets for routed networks.

Prerequisites

Log in to the vCloud Automation Center console as a **fabric administrator**.

Procedure

1   Specify Network Profile Information on page 21

The network profile information identifies the routed network properties, its underlying external network profile, and other values used in provisioning the network.

2   Configure IP Ranges on page 22

A fabric administrator can define one or more ranges of static IP addresses for use in provisioning a network.

Specify Network Profile Information

The network profile information identifies the routed network properties, its underlying external network profile, and other values used in provisioning the network.

Prerequisites

- Log in to the vCloud Automation Center console as a **fabric administrator**.

- "Create an External Network Profile," on page 16.

Procedure

1   Select **Infrastructure > Reservations > Network Profiles**.

2   Select **New Network Profile > Routed**.

3   Type a **Name** and, optionally, a **Description**.

4   Select an external network profile from the drop-down menu.

5   Type a mask address in the **Subnet mask** text box.

For example, 255.255.0.0.

6 Type a mask address in the **Range subnet mask** text box.

For example, 255.255.255.0.

7 Type an IP address in the **Base IP** text box.

8 (Optional) In the DNS/WINS group, type values as needed.

The external network profile provides these values, which you can edit.

What to do next

A routed network profile requires an IP range. For information on creating an IP range, see "Configure IP Ranges," on page 22.

Configure IP Ranges

A fabric administrator can define one or more ranges of static IP addresses for use in provisioning a network.

During multi-machine provisioning, every new multi-machine routed network allocates the next available subnet range and uses it as its IP space.

Prerequisites

"Specify Network Profile Information," on page 16.

Procedure

1 Click the **IP Ranges** tab.

2 Click **Generate Ranges**.

You must type the subnet mask, range subnet mask, and base IP addresses on the **Network Profile Information** tab before you can generate IP ranges. Starting with the base IP address, vCloud Automation Center generates ranges based on the range subnet mask.

For example, vCloud Automation Center generates ranges of 254 IP addresses if the subnet mask is 255.255.0.0 and the range subnet mask is 255.255.255.0.

3 Click **New Network Range**.

The New Network Range dialog box appears.

4 Type a **Name** and, optionally, a **Description**.

5 Type an IP address in the **Starting IP address** text box.

This IP address must match the base IP address in the routed network profile.

6 Type an IP address in the **Ending IP address** text box.

7 Click **OK**.

The newly defined IP address range appears in the Defined Ranges list.

8 Click **OK**.

Cost Information for Multi-Machine Services

The cost of a multi-machine service is based on the cost of its component machines and any markup added to the multi-machine service.

Cost Calculation for Multi-Machine Services

Several factors can contribute to the calculation of cost for multi-machine services.

The daily cost of a multi-machine service is based on the costs of its component machines and the cost specified in the multi-machine service blueprint.

Table 2-1. Daily Cost Drivers

Cost Driver	Calculated Cost
Component machine cost	Total cost of all the component machines in the multi-machine service. The factors that contribute to the component machine cost depend on the type of machine. For details about how costs for different machine types are calculated, see the *IaaS Configuration for Virtual Platforms, IaaS Configuration for Physical Machines,* or *IaaS Configuration for Cloud Platforms*.
Blueprint cost (multi-machine service)	The value for daily cost specified in the multi-machine blueprint is added to the total cost of the multi-machine service. This value can represent a markup for using the multi-machine service in addition to the costs of the component machines.

Lease cost is calculated as daily cost multiplied by the total number of days in the lease period (if applicable).

Cost-to-date is calculated as daily cost multiplied by the number of days a multi-machine service has been provisioned.

How Cost Is Displayed

The multi-machine service cost is displayed at various stages of the request and provisioning life cycle and is updated according to the current information in the request or on the provisioned item.

Table 2-2. Cost Displayed During the Request and Provisioning Life Cycle

Life Cycle Stage	Value Displayed for Cost
Viewing the catalog item details prior to request	Projected costs of the multi-machine service based on the cost profile, the values for machine resources specified in the component blueprints, lease duration specified in the multi-machine blueprint, and the daily costs specified in the component blueprints and multi-machine blueprint.
	The values of some of the cost drivers can be unknown before a machine is requested:
	■ The component blueprints can specify a range for machine resources or number of components of each type. The requester can specify any value within the blueprint range.
	■ There can be more than one reservation available for provisioning the component machines. If these reservations have different compute resources, different cost profiles can apply.
	■ There can be more than one datastore available for provisioning the component machines, either on the same reservation or on different reservations, that have different storage cost profiles.
	■ If either of the above is true, the daily cost is displayed as a range with the lower bound being the minimum resource usage multiplied by the lowest resource cost for memory, CPU, and storage, and the upper bound being the maximum resource usage multiplied by the highest cost.
	If the multi-machine blueprint specifies a value for lease duration, the lease cost is displayed as a range with the lower bound being the minimum lease duration multiplied by the minimum cost, and the upper bound being the maximum lease duration multiplied by the maximum cost.
Completing the request form	Projected costs based on the values for machine resources and lease duration specified in the request form and the blueprint cost.
	The daily cost can be a range if there is more than one reservation available for provisioning the component machines and these reservations have different compute resources that vary in cost. Alternatively, there can be more than one datastore available for provisioning the machine, either on the same reservation or on different reservations, that vary in cost.
	By default the request form shows the request for the multi-machine service, but the requester can select a specific component machine to edit the properties of the component. The values for daily and lease cost are automatically updated as the user edits the relevant values in the request form. The user can also specify the number of machines of each type in the multi-machine service, which affects the total cost.
Viewing details of a submitted request or approving a request	Projected costs based on the requested machine resources, lease duration, and blueprint cost.
	The daily cost can be a range if there is more than one reservation available for provisioning the component machines and these reservations have different compute resources or different datastores that vary in cost.
	Depending on the approval policy, an approver can have the opportunity to edit the number of component machines or the lease duration, which can affect the cost. The approval applies to the multi-machine service as a whole; the component machines are not approved separately.
Viewing the details of a provisioned multi-machine service	Actual daily cost, lease cost, and cost-to-date based on the resource usage of the provisioned component machines, lease duration, blueprint costs, and number of days since the multi-machine service was provisioned. You can view the cost details for both the multi-machine as a whole and its component machines.

Creating a Multi-Machine Blueprint

<div style="font-size:3em; text-align:right">3</div>

Machine blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

A tenant administrator or business group manager allows users to provision multi-machine services by creating one or more entitled multi-machine blueprints. Before you create a multi-machine blueprint, you must first create blueprints for each of the component machines you want to include in the multi-machine service. The component blueprints must be available to the same business groups as the multi-machine blueprint.

A multi-machine blueprint contains references to component blueprints. Before you can create a multi-machine blueprint, you must first create blueprints for each of the component machines that you want to include in the multi-machine. The component blueprints must be available to the same business group or groups as the multi-machine blueprint.

A multi-machine blueprint includes information that applies only to a multi-machine service as a whole. Configuration options, such as a reservation policy, apply only to component machines. Multi-machine services do not have an archive period; the service and its component machines are destroyed when they expire.

For information about what you can edit in multi-machine blueprints, and their component blueprints, see Chapter 4, "Managing Multi-Machine Blueprints," on page 43.

This chapter includes the following topics:

■ "Specifying Scripts for Multi-Machine Service Provisioning," on page 26

■ "Specifying Custom Properties for Multi-Machine Services," on page 26

■ "Specifying Actions for Multi-Machine Services," on page 27

■ "Create a Multi-Machine Blueprint," on page 27

■ "Configuring Multi-Machine Blueprints for Network and Security Virtualization," on page 33

■ "Publish a Blueprint," on page 40

■ "Configure Network Adapters for Component Machines Using External Network Profiles," on page 41

Specifying Scripts for Multi-Machine Service Provisioning

You can designate scripts or workflows to execute at specific points during the multi-machine service life cycle. Scripts are executed on the Distributed Execution Manager worker machine, not on the guest operating system of the component machine.

The following table describes the multi-machine life cycle stages at which scripts can execute. For information about how to specify custom logic to execute at each stage, see "Specify Scripting Information for a Multi-Machine Blueprint," on page 30.

Table 3-1. Script Execution Stages in the Multi-Machine Life Cycle

Stage	Description
Pre-provisioning	Executes after all necessary approvals are complete, but before provisioning any machines.
Post-provisioning	Executes after all component machines are provisioned and powered on.
Pre-startup	Executes before powering on the multi-machine service and all its component machines.
Post-startup	Executes immediately after powering on the multi-machine service and all its component machines. The multi-machine service state is set to On after the post-startup scripts execute.
Pre-shutdown	Executes immediately before shutting down or powering off the multi-machine service and its component machines.
Post-shutdown	Executes after shutting down or powering off the multi-machine service and its component machines. The multi-machine service state is set to Off after the post-shutdown scripts execute.

Provisioning scripts are executed only during the initial provisioning of a multi-machine service. The startup and shutdown scripts are executed every time the multi-machine service is powered on or off, except for when the service is initially powered on during provisioning. The pre-provisioning and post-provisioning scripts must include everything that you want to run before and after the initial power on action.

You can also run workflows during the various stages of the multi-machine life cycle. The workflows must accept an argument named *MasterMachine* of type *VirtualMachine (DynamicOps.ManagementModel.VirtualMachine)*. The *Components* property of *MasterMachine* is a list of *AppServiceComponents*, each of which represents a component machine of the multi-machine service.

Scripts or workflows must be installed in the Model Manager before you can use them in a multi-machine blueprint.

Specifying Custom Properties for Multi-Machine Services

Tenant administrators and business group managers can specify custom properties that apply to all component machines in a multi-machine service in the multi-machine blueprint. When the same property exists in more than one source, a specific order is followed when applying properties to the machine.

Custom properties in a multi-machine blueprint override properties specified in component blueprints. Runtime properties on the component machine, which are specified at request time or by editing the machine after it has been provisioned, override runtime properties specified at the multi-machine service level. This allows the multi-machine blueprint to apply consistent behavior across all of its component machines, while allowing a user to override the multi-machine service properties for each component type.

Custom properties on multi-machine service and component machines are processed in the following order.

1 Build profile specified on component blueprint

2 Component blueprint

3 Build profile specified on multi-machine blueprint

4 Multi-Machine blueprint

5   Business group

6   Compute resource

7   Reservations

8   Endpoint

9   Request time specified on a multi-machine service

10   Request time specified on a component machine

A property value specified in a source that appears later in the list overrides values for the same property specified in sources earlier in the list. Custom properties specified in the multi-machine service are applied to all component machines in the service. If a property is designated as *Prompt User* on a component blueprint, the value specified at request time is applied to all machines of the same component type that are provisioned as part of that request. For information about how to add custom properties, see "Add Multi-Machine Blueprint Custom Properties," on page 31.

Some properties, such as *Hostname*, must be unique to each machine. Do not specify the property at the component level. If the *Hostname* property is specified at the component level, it is ignored.

Specifying Actions for Multi-Machine Services

Tenant administrators and business group managers use blueprints to control which actions are available to for machines that are provisioned from the blueprint.

The actions settings and entitlements specified for the multi-machine blueprint override settings in the component blueprints. For example, if you have a component blueprint that is restricted to userA and you add it as a component of a multi-machine blueprint that is available to everyone, the business group can provision the restricted machine as part of a multi-machine service. However, only userA can provision it as a standalone machine.

Create a Multi-Machine Blueprint

Machine blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings. A tenant administrator or business group manager creates a multi-machine blueprint for provisioning the multi-machine service and its component machines.

Prerequisites

Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

Procedure

1   Specify Blueprint Information for a Multi-Machine Blueprint on page 28

      Blueprint information settings specify how many machines can be provisioned and the daily cost.

2   Specify Build Information for a Multi-Machine Blueprint on page 29

      The build information settings determine the type and number of component machines that are provisioned.

3   Specify Network Information for a Multi-Machine Blueprint on page 30

      Network information settings determine the transport zone, network profile to use when provisioning, and reservation policy.

4   Specify Scripting Information for a Multi-Machine Blueprint on page 30

      Scripting information settings specify optional provisioning, startup, and shutdown processing scripts.

5

Adding custom properties to a blueprint gives you detailed control over the configuration of provisioned machines. Custom properties apply to all component machines in a multi-machine service.

6

Use blueprint actions and entitlements together to maintain detailed control over provisioned machines.

7

Blueprints are automatically saved in the draft state and must be manually published before they appear as catalog items.

What to do next

The blueprint is not available as a catalog item until it is published. See

Specify Blueprint Information for a Multi-Machine Blueprint

Blueprint information settings specify how many machines can be provisioned and the daily cost.

Prerequisites

Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

Procedure

1 Select **Infrastructure > Blueprints > Blueprints**.

2 Select **New Blueprint > Multi-Machine**.

3 Type a **Name** and, optionally, a **Description**.

4 (Optional) Select the **Master** check box to allow users to copy your blueprint.

5 Select who can provision machines with this blueprint.

Roles	Who Can Provision
If you are both a business group manager and a tenant administrator	■ Select the **Shared blueprint** check box to allow the blueprint to be entitled to users in any business group. ■ Deselect the **Shared blueprint** check box to create a local blueprint, and select a business group from the **Business group** drop-down menu.
Business group manager	Select a business group from the **Business group** drop-down menu.
Tenant administrator	Your blueprints are always shared. You cannot choose who can use them to provision machines.

Users who will be enabled to provision machines with this blueprint must all be members of the same business group.

6 Select a machine prefix from the **Machine prefix** drop-down menu.

You can select **Use group default** to accept the default machine prefix business group for the user.

7 (Optional) Type a number in the **Maximum per user** text box to limit the number of machines that a single user can provision with this blueprint.

8 Set the daily cost of the machine by typing the amount in the **Cost (daily)** text box.

This cost is for the multi-machine service in addition to the component machines.

Your blueprint is not finished. Do not navigate away from this page.

Specify Build Information for a Multi-Machine Blueprint

The build information settings determine the type and number of component machines that are provisioned.

Prerequisites

■ "Specify Blueprint Information for a Multi-Machine Blueprint," on page 28.

Procedure

1 Click the **Build Information** tab.

2 Click the **Add Blueprints** icon ( ).

The Add Blueprints dialog box appears, listing available blueprints. The blueprints you select must be available to the same business groups as the multi-machine blueprint.

3 Select one or more blueprints to add and click **OK**.

4 (Optional) Click the **Edit** icon ( ) next to the name of the component blueprint to edit.

a Type a blueprint display name in the **Name** text box.

b Type a minimum number of component machines in the **Minimum** text box.

This setting specifies the minimum number of component machines that can be included in the multi-machine service. A machine owner cannot request a multi-machine service with less than the minimum number of machines for each component type. This number determines if a multi-machine service provisioned from this blueprint is healthy. When the number of machines of a given component type that are provisioned or powered on is lower than this number, the multi-machine service is considered unhealthy and its state is set to off.

c (Optional) Type the maximum number of machines to be provisioned from the blueprint in the multi-machine service in the **Maximum** text box.

If you do not enter a value, the multi-machine service cannot have more than the minimum number of machines of this component type.

d (Optional) Adjust the **Startup Order** and **Shutdown Order** for the machines.

The startup and shutdown order do not apply at provisioning time. These orders are used only when you power the multi-machine service on or off after initial provisioning.

e (Optional) If available, type a component blueprint description in the **Description** text box.

This text box might be read-only.

f (Optional) Edit network information for the component blueprint by clicking **Edit** in the Network column.

5 (Optional) Specify the lease settings for provisioned machines, or leave blank for no expiration date.

a Type the minimum number of lease days in the **Minimum** text box.

If you only provide a minimum, this number becomes the value for all machines provisioned from this blueprint.

b (Optional) Type the maximum number of lease days in the **Maximum** text box to allow users to select their own settings within the range that you provide.

Your blueprint is not finished. Do not navigate away from this page.

Specify Network Information for a Multi-Machine Blueprint

Network information settings determine the transport zone, network profile to use when provisioning, and reservation policy.

For related information, see "Creating a Network Profile," on page 15 and "Configuring Multi-Machine Blueprints for Network and Security Virtualization," on page 33.

For more information about adding the available network profiles to your blueprint, see the following topics:

- "Add a NAT Network Profile to a Multi-Machine Blueprint," on page 35

- "Add a Private Network Profile to a Multi-Machine Blueprint," on page 33

- "Add a Routed Network Profile to a Multi-Machine Blueprint," on page 34

Prerequisites

- "Specify Build Information for a Multi-Machine Blueprint," on page 29.

- To add network information, a fabric administrator must have already created at least one external network profile. See "Create an External Network Profile," on page 16.

Procedure

1   Click the **Network** tab.

2   Select a transport zone from the **Transport zone** drop-down menu.

     A vCenter Server administrator creates transport zones and adds clusters to them. A transport zone defines which clusters the multi-machine networks will span. A vCenter Server administrator must prepare transport zones and clusters before networks can be provisioned.

3   Choose a network profile.

     - Select a network profile from the Network Profiles table.

     - Click **New Network Profile** and select **NAT**, **Private**, or **Routed** from the drop-down menu.

4   (Optional) Select a reservation policy from the **Reservation policy** drop-down menu.

     Fabric administrators can create reservation policies.

Your blueprint is not finished. Do not navigate away from this page.

Specify Scripting Information for a Multi-Machine Blueprint

Scripting information settings specify optional provisioning, startup, and shutdown processing scripts.

Prerequisites

- "Specify Network Information for a Multi-Machine Blueprint," on page 30.

Procedure

1   Click the **Scripting** tab.

2   Specify how to run custom logic for each stage of the life cycle.

     a   Select the name of a script in the appropriate provisioning, startup, or shutdown stage to run that script, or select **Workflow** to run a workflow.

     b   If you selected **Workflow**, type the name of the workflow in the **Workflow** text box.

Your blueprint is not finished. Do not navigate away from this page.

Add Multi-Machine Blueprint Custom Properties

Adding custom properties to a blueprint gives you detailed control over the configuration of provisioned machines. Custom properties apply to all component machines in a multi-machine service.

Prerequisites

- Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

- "Specify Scripting Information for a Multi-Machine Blueprint," on page 30.

Procedure

1   Click the **Properties** tab.

2   (Optional) Select one or more build profiles from the **Build profiles** menu.

    Build profiles contain groups of custom properties. Fabric administrators can create build profiles.

3   (Optional) Add any custom properties to your blueprint.

    a   Click **New Property**.

    b   Type the custom property in the **Name** text box.

    c   (Optional) Select the **Encrypted** check box to encrypt the custom property in the database.

    d   Type the value of the custom property in the **Value** text box.

    e   (Optional) Select the **Prompt user** check box to require the user to provide a value when they request a machine.

        If you choose to prompt the user for a value, any value you provide for the custom property is presented to the user as the default. If you do not provide a default, the user cannot continue with the machine request until they provide a value for the custom property.

    f   Click the **Save** icon ( ).

Your blueprint is not finished. Do not navigate away from this page.

Specify Actions for Multi-Machine Blueprints

Use blueprint actions and entitlements together to maintain detailed control over provisioned machines.

Entitlements control which machine operations specific users can access. Blueprint actions control which machine operations can be performed on machines provisioned from a blueprint. For example, if you disable the option to reprovision machines created from a blueprint, then the option to reprovision a machine created from the blueprint does not appear for any users. If you enable the reprovision machine operation, then users who are entitled to reprovision machines can reprovision machines created from this blueprint.

NOTE   The options that appear on the **Actions** tab depend on your platform and any customizations made to your vCloud Automation Center instance.

Prerequisites

"Add Multi-Machine Blueprint Custom Properties," on page 31.

Procedure

1   Click the **Actions** tab.

2   (Optional) Select the check boxes for each machine option to enable for machines provisioned from this blueprint.

3   Click **OK**.

Your blueprint is saved.

What to do next

The blueprint is not available as a catalog item until it is published. See "Publish a Blueprint," on page 32.

Publish a Blueprint

Blueprints are automatically saved in the draft state and must be manually published before they appear as catalog items.

You only need to publish a blueprint once. Any changes you make to a published blueprint are automatically reflected in the catalog.

Prerequisites

■   Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

■   Create a blueprint.

Procedure

1   Select **Infrastructure > Blueprints > Blueprints**.

2   Point to the blueprint you want to publish and click **Publish**.

3   Click **OK**.

Your blueprint is now a catalog item.

What to do next

Tenant administrators, business group managers, and service architects configure your catalog item and associate it with a service so that entitled users can request it from the catalog. For information about how to configure and manage the catalog, see *Tenant Administration*.

Configuring Multi-Machine Blueprints for Network and Security Virtualization

When you provision a multi-machine service in vCloud Automation Center, you can provision virtualized networks and related services for the vSphere component machines in that multi-machine service based on the vCloud Networking and Security and NSX platforms. Fabric administrators create network profile templates and external network profiles; they also create the reservations that determine the available networks and other settings. Tenant administrators and business group managers create NAT, routed, and private network profiles, virtual network adapters, and virtual load balancers, specify security groups, and apply the templates and specifications to the components in a multi-machine blueprint.

Adding Network Profiles to a Multi-Machine Blueprint

A tenant administrator or business group manager can create NAT, routed, and private network profiles for a multi-machine blueprint, and assign those profiles to virtual network adapters in the same multi-machine blueprint.

Tenant administrators and business group managers can create NAT and routed network profiles in multi-machine blueprints, based on network profile templates and external network profiles created by fabric administrators. Tenant administrators and business group managers can also create private network profiles in multi-machine blueprints, but private network profiles do not use external network profiles and do not require a template.

These network profiles determine network connectivity within application tiers and also between the application and external networks. Depending on the network profile, the application may connect to existing logical network objects such as routers and switches, or these objects may be dynamically created to connect the applications.

Add a Private Network Profile to a Multi-Machine Blueprint

A tenant administrator or business group manager can add a private network profile to a multi-machine blueprint, and then assign the network profile to virtual network adapters in the multi-machine blueprint.

You use a private network profile when the application or network needs to be provisioned in isolation from other applications and networks.

In this case, tiers or networks within the application can communicate with each other with routable connections, but these tiers are not connected to external networks. This means that users can connect to the application through console access only.

The most common use case for a private network profile is for a multi-tier application where the application and database tiers only need to communicate with each other, but do not need direct access from external networks. Usually, the web tier in this application is the routed or NAT type, to allow for external network access.

Another use case for this profile type is for performance testing, where a traffic-generating process can be deployed within one of the application tiers to simulate user activity on the application. This does not require external network access.

When creating a private network profile for a multi-machine component, you can create it with or without a template. You can change or reuse the template name because the network profile applies only to the current multi-machine blueprint, and because the IP address space is isolated behind a logical router gateway. Therefore, IP addresses do not conflict by reusing private network profiles.

For descriptions of the values required when creating a private network profile, see "Create a Private Network Profile," on page 17.

Prerequisites

- Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

- This procedure requires that you have already created a multi-machine blueprint that contains at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 27.

Procedure

1 Select **Infrastructure > Blueprints > Blueprints**.

2 Locate a multi-machine blueprint with at least one virtual component blueprint.

3 Click **Edit** in the drop-down menu.

4 Click the **Network** tab.

5 Select a transport zone from the **Transport zone** drop-down menu.

6 Click **New Network Profile > Private**.

The New Network Profile - Private window appears.

7 (Optional) Select a private network profile template from the **Copy from existing network profile** drop-down menu.

vCloud Automation Center inserts values from the template.

8 Click the **Network Profile Information** tab and type values as required in the text boxes.

9 Click the **IP Ranges** tab and add, delete, or edit the defined ranges as required.

10 Click **OK**.

The new network profile appears in the Network Profiles table on the **Network** tab.

What to do next

The new profile appears as a network profile choice when you create a network adapter. For more information, see "Configure Network Adapters for Component Machines," on page 36.

Add a Routed Network Profile to a Multi-Machine Blueprint

A tenant administrator or business group manager can add a routed network profile to a multi-machine blueprint, and assign the network profile to the virtual network adapters in the multi-machine blueprint.

You use a routed network profile when the application or network needs to be provisioned with full connectivity to applications and networks, using routable IP addresses.

In this case, all routed networks within the application can communicate with other routed networks with the same network profile and these networks also are connected to external networks. This means that users can connect to the application through network and console access.

The most common use case for a routed network profile is for a multi-tier application that is deployed in production and requires not only end-user access to the web tier (presentation layer), but also requires administrators to manage database and application servers through direct network access. More controls on network access can be enforced with a network firewall specified by a security group.

Because the network profiles you add to the multi-machine blueprint apply only to that blueprint, you can reuse the template names or change them as you see fit.

When you add a routed network profile to a multi-machine blueprint, you can change only the name and description. You can view but not change the remaining information from the template. For descriptions of the values required when creating a routed network profile, see "Create a Routed Network Profile," on page 21.

Prerequisites

- Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

- A fabric administrator must have created at least one routed network profile template, because you need one to add a routed network profile. For more information, see "Create a Routed Network Profile," on page 21.

- This procedure requires that you have already created a multi-machine blueprint that contains at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 27.

Procedure

1 Select **Infrastructure > Blueprints > Blueprints**.

2 Locate a multi-machine blueprint with at least one virtual component blueprint.

3 Click **Edit** in the drop-down menu.

4 Click the **Network** tab.

5 Select a transport zone from the **Transport zone** drop-down menu.

6 Select **New Network Profile > Routed**.

The New Network Profile - Routed window appears.

7 Select a routed network profile template from the **Copy from existing network profile** drop-down menu.

vCloud Automation Center inserts values from the template.

8 (Optional) Click the **Network Profile Information** tab and change the name and description as desired.

9 (Optional) Click the **IP Ranges** tab to view the defined IP address ranges.

10 Click **OK**.

The new network profile appears in the Network Profiles table on the **Network** tab.

What to do next

The new profile appears as a network profile choice when you create a network adapter. For more information, see "Configure Network Adapters for Component Machines," on page 36.

Add a NAT Network Profile to a Multi-Machine Blueprint

A tenant administrator or business group manager can add a NAT network profile to a multi-machine blueprint, and assign the network profile to the component network adapters in the multi-machine blueprint.

You use a NAT network profile when the application or network needs to mask the IP addresses of the application workloads. This means that users can only connect to the external IP address of the NAT rule, which then translates the connection request and routes it to the application workload.

The most common use case for a NAT network profile is for a multi-tier application where the application and database tiers need to be masked or secured from direct access. Here, the application and database tiers have private network profiles and the web tier has a NAT network profile.

Another use case for this profile type is to support multiple, overlapping IP address spaces. If a large number of development and testing workloads need deployment but IP address space is limited, a combination of NAT profiles to support external access and private profiles to secure, mask internal IP addresses is suitable.

Because the network profiles you add to a multi-machine blueprint apply only to that blueprint, you can reuse the template names or change them as you see fit.

When you add a NAT network profile to a multi-machine blueprint, you can change some information like the name, description, gateway, DNS, and static IP ranges. You can view but not change the remaining information from the template. For descriptions of the values required when creating a NAT network profile, see "Create a NAT Network Profile," on page 19.

Prerequisites

■ Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

■ A fabric administrator must have created at least one NAT network profile template, because you need one to add a NAT network profile. For more information, see "Create a NAT Network Profile," on page 19.

■ This procedure requires that you have already created a multi-machine blueprint that contains at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 27.

Procedure

1 Select **Infrastructure > Blueprints > Blueprints**.

2 Locate a multi-machine blueprint with at least one virtual component blueprint.

3 Click **Edit** in the drop-down menu.

4 Click the **Network** tab.

5 Select a transport zone from the **Transport zone** drop-down menu.

6 Select **New Network Profile > NAT**.

The New Network Profile - NAT window appears.

7 Select a NAT network profile template from the **Copy from existing network profile** drop-down menu.

vCloud Automation Center inserts values from the template.

8 (Optional) Click the **Network Profile Information** tab and change the name, description, subnet mask, gateway, DNS, and DHCP settings (one-to-many NAT only), as desired.

9 Click the **IP Ranges** tab and add, delete, or edit the defined ranges as required.

You can also upload IP addresses with a CSV file.

10 Click **OK**.

The new network profile appears in the Network Profiles table on the **Network** tab.

What to do next

The new profile appears as a network profile choice when you create a network adapter. For more information, see "Configure Network Adapters for Component Machines," on page 36.

Configure Network Adapters for Component Machines

A tenant administrator or business group manager can configure a network adapter for a multi-machine blueprint, and then apply the network adapter to one or more component blueprints in that multi-machine blueprint. When you request the multi-machine service, vCloud Automation Center provisions the component machines with the network connection defined by the network adapter.

For related information, see "Configuring Multi-Machine Blueprints for Network and Security Virtualization," on page 33.

Prerequisites

■ Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

- Create a multi-machine blueprint with at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 27.

- A fabric administrator must have created all necessary external network profiles and templates for other types of network profiles. See "Creating a Network Profile," on page 15.

- A tenant administrator or business group manager must have created all necessary NAT, routed, and private network profiles. See "Adding Network Profiles to a Multi-Machine Blueprint," on page 33.

Procedure

1   Select **Infrastructure > Blueprints > Blueprints**.

2   Locate a multi-machine blueprint with at least one virtual component blueprint.

3   Click **Edit** in the drop-down menu.

4   Click the **Build Information** tab.

5   Locate a blueprint in the **Components** table that has **Edit** in the Network column.

6   Click **Edit**.

    The **Edit Network** dialog box appears.

7   Click **New Network Adapter**.

    New Network Adapter is not available if a component machine still exists that was provisioned with the multi-machine blueprint.

    An editable network adapter row appears.

8   Select a network profile from the **Network Profile** drop-down menu.

    To appear in the menu, NAT, routed, and private network profiles must exist in the multi-machine blueprint.

9   Select an assignment type from the **Assignment Type** drop-down menu.

Option	Description
Static IP	You can select this assignment type for any network profile with an IP range. This is the only assignment type allowed for routed and one-to-one NAT network profiles. You can type a static IP address in the **Address** text box for private and NAT network profiles only. The IP address must be part of an IP range in the network profile.
DHCP	You can select this assignment type for private, one-to-many NAT, and external network profiles if DHCP is enabled in the network profile.

10 Click ✅ to save the network adapter.

11 (Optional) Click **Edit** in the Custom Properties column to create or edit a custom property for the network adapter.

12 Click **OK**.

Configure Load Balancers for Component Machines

A tenant administrator or business group manager can configure a load balancer for a multi-machine component blueprint. All machines provisioned from the component blueprint are added as members of the load balancer.

When configuring a load balancer, you specify a network adapter and select a network profile (external, private, NAT, or Routed) for the virtual IP address. The network profile you select for the virtual IP address must be the same one used by the network adapter.

Prerequisites

- Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

- This procedure requires that you have already created a multi-machine blueprint that contains at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 27 .

- A tenant administrator must have added a network profile to the multi-machine blueprint. See "Adding Network Profiles to a Multi-Machine Blueprint," on page 33.

- A tenant administrator must have added a network adapter with a Static IP assignment type to the component machine. See "Configure Network Adapters for Component Machines," on page 36.

- You must have selected a transport zone on the Network tab of the multi-machine blueprint before you can configure load balancing.

Procedure

1   Select **Infrastructure > Blueprints > Blueprints**.

2   Locate a multi-machine blueprint with at least one virtual component blueprint.

3   Click **Edit** in the drop-down menu.

4   Click the **Build Information** tab.

5   Locate a blueprint in the **Components** table that has editable network settings.

    Look for **Edit** in the Network column.

6   Click the **Load Balancer** tab.

7   Select the service to use for load balancing.

    The load balancer settings are uneditable if a machine provisioned from this blueprint still exists.

    a   Select the service check box in the **Services** table.

        The service entry becomes editable.

    b   Type values in the text boxes as needed.

        vCloud Automation Center populates the text boxes with typical values.

    c   Click ⊘ to save the values and select the service.

        Selecting a service enables the text boxes for that service.

    d   (Optional) Repeat steps a through c to add other services as needed.

8   Type the URI in the **URI for HTTP service** text box, if enabled.

9   Type the ID of the network adapter in the **Network adapter** text box, or use the up and down arrows to select a value.

    The ID is in the # column of the Network Adapters table on the **Network** tab. During provisioning, a load balancer pool member assumes the IP address of the network adapter.

10   Select the network profile from the **Network profile** drop-down menu in the **Virtual IP** section.

An external, private, or NAT network profile must have the load balancer virtual IP address in its IP range (static for external, static or DHCP for others). A routed network profile does not have a static IP range and so does not have this requirement.

11   For private and NAT network profiles, type the virtual IP address for the load balancer in the **IP Address** text box.

The IP address must be within the IP ranges defined in the network profile.

12   Click **OK**.

Configure Security Groups for Component Machines

A tenant administrator or business group manager can assign one or more security groups to a component machine provisioned with the multi-machine blueprint.

When configuring security groups for a component blueprint, you need to specify a transport zone on the **Network** tab of the multi-machine blueprint to make security groups available for selection. The component is assigned to the selected security group(s) after provisioning.

You can also add security groups on the Network tab of the New or Edit Reservation page. All multi-machine components provisioned through the reservation are assigned to all of the security groups you select. For more information about adding security groups through the reservation, see "Create a Reservation for Network and Security Virtualization," on page 13.

Prerequisites

■   Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

■   This procedure requires that you have already created a multi-machine blueprint that contains at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 27.

Procedure

1   Select **Infrastructure > Blueprints > Blueprints**.

2   Locate a multi-machine blueprint with at least one virtual component blueprint.

3   Click **Edit** in the drop-down menu.

4   (Optional) Verify that a transport zone is selected.

a   Click the **Network** tab on the Edit Blueprint page.

b   Select a transport zone from the **Transport zone** drop-down box.

5   Click the **Build Information** tab.

6   Locate a blueprint in the **Components** table that has editable network settings.

Look for **Edit** in the Network column.

7   Click the **Network** tab.

8   Select one or more security group check boxes in the **Security groups** box under **Advanced Settings**.

Security groups appear for selection only if there is no existing component machine provisioned from this blueprint.

9   Click **OK**.

Configure Reservations for Routed Gateways

A tenant administrator or business group manager can configure reservations for use in provisioning the routed gateway of a multi-machine service.

When vCloud Automation Center provisions a multi-machine service with NAT, routed, or private networking, it provisions a routed gateway as the network router for that service. The routed gateway is a management machine that consumes compute resources like other virtual machines but manages the network communications for the multi-machine components. The reservation used to provision the routed gateway determines the external network used for NAT and load balancer Virtual IP.

Prerequisites

- Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

- You must have created a reservation policy. If reservations already use this policy, they must be intended for use with a routed gateway.

- You must have created a multi-machine blueprint. See "Create a Multi-Machine Blueprint," on page 27.

Procedure

1 Select **Infrastructure > Blueprints > Blueprints**.

2 Locate a multi-machine blueprint, or select **New Blueprint > Multi-Machine** to create one.

3 Click the **Network** tab.

4 Select a transport zone from the **Transport zone** drop-down menu.

The **Reservation policy** drop-down menu becomes selectable.

5 Select a reservation policy from the **Reservation policy** drop-down menu under **Routed Gateway**.

6 Click **OK** to save your changes.

If creating a multi-machine blueprint, you need to complete the required information first.

When you provision a multi-machine service with this blueprint, vCloud Automation Center attempts to use only the reservations associated with the specified reservation policy to provision the routed gateway.

Publish a Blueprint

Blueprints are automatically saved in the draft state and must be manually published before they appear as catalog items.

You only need to publish a blueprint once. Any changes you make to a published blueprint are automatically reflected in the catalog.

Prerequisites

- Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

- Create a blueprint.

Procedure

1 Select **Infrastructure > Blueprints > Blueprints**.

2 Point to the blueprint you want to publish and click **Publish**.

3 Click **OK**.

Your blueprint is now a catalog item.

What to do next

Tenant administrators, business group managers, and service architects configure your catalog item and associate it with a service so that entitled users can request it from the catalog. For information about how to configure and manage the catalog, see *Tenant Administration*.

Configure Network Adapters for Component Machines Using External Network Profiles

A tenant administrator or business group manager can configure a network adapter for a multi-machine component. A network adapter defines a network connection for a component machine. When you select an external network profile for the network adapter, you are specifying an existing external network.

For related information, see "Configuring Multi-Machine Blueprints for Network and Security Virtualization," on page 33.

Prerequisites

- Log in to the vCloud Automation Center console as a **tenant administrator** or **business group manager**.

- "Create a Multi-Machine Blueprint," on page 27 with at least one virtual component blueprint.

- A fabric administrator must have created at least one external network profile. For more information, see "Create an External Network Profile," on page 16.

Procedure

1 Select **Infrastructure > Blueprints > Blueprints**.

2 Locate a multi-machine blueprint with at least one virtual component blueprint.

3 Click **Edit** in the drop-down menu.

4 Click the **Build Information** tab.

5 Locate a blueprint in the **Components** table that has **Edit** in the Network column.

6 Click **Edit**.

   The **Edit Network** dialog box appears.

7 Click **New Network Adapter**.

   An editable network adapter row appears.

8 Select an external network profile from the **Network Profile** drop-down menu.

9 Select an assignment type from the **Assignment Type** drop-down menu.

   - Static IP

   - DHCP

10 Click ☑ to save the network adapter.

11 (Optional) Click **Edit** in the Custom Properties column to create or edit a custom property for the network adapter. For more information, see "Add Multi-Machine Blueprint Custom Properties," on page 31.

12 Click **OK**.

Managing Multi-Machine Blueprints

<div style="text-align: right; font-size: 2em;">**4**</div>

You can edit certain aspects of an existing blueprint.

There are restrictions to the configuration of component machines if existing multi-machine services were provisioned by the blueprint:

- When editing component types, the Minimum field is read-only.

- You cannot add new component types to the multi-machine service.

- You cannot delete component blueprints from the multi-machine service.

- You cannot change the business groups associated with the multi-machine blueprint or the component blueprint.

These restrictions prevent an existing multi-machine service from reaching an unhealthy state due to changes in the blueprint. To make any of these changes to the component machine configuration in a multi-machine blueprint, either decommission all existing services that use the blueprint or create a copy of the blueprint and update the configuration in the copy.

If you change the maximum value for a component type, existing services that have more component machines of that type than the new maximum do not become invalid. Users cannot add any more machines of that component type until the number of machines falls below the maximum.

When you change custom properties on a multi-machine blueprint, the new properties are applied to new multi-machine services that are provisioned from this blueprint. They are also inherited by component machines that are added to existing multi-machine services that are provisioned from this blueprint.

Monitoring Workflows and Viewing Logs

5

Depending on your role, you can monitor workflows and view activity logs.

The following table outlines the possible monitoring and log display options available to administrators.

Table 5-1. Monitoring and Log Display Options

Objective	Role	Menu Sequence and Description
Display information about actions that have occurred, such as the action type, date and time of the action, and so on.	IaaS administrator	Display default log information or control display content using column and filter options. Click **Infrastructure > Monitoring > Audit Logs**. The audit log provides details on the status of managed virtual machines and activities performed on these machines during reconfiguration. It also displays information about Amazon machine provisioning. The log includes Amazon machine provisioning, multi-machine, vCloud Networking and Security, reclamation, and reconfigure actions.
View the status of scheduled and available Distributed Execution Manager and other workflows.	IaaS administrator	Display workflow status and optionally open a specific workflow to display its details. Click **Infrastructure > Monitoring > Distributed Execution Status**.
View and optionally export log data.	IaaS administrator	Display default log information or control display content using column and filter options. Click **Infrastructure > Monitoring > Log**.
View the status and history of executed Distributed Execution Manager and other workflows.	IaaS administrator	Display workflow history and optionally open a specific workflow to display its execution details. Click **Infrastructure > Monitoring > Workflow History**.
Display a list of events, including event type, time, user ID, and so on and optionally display an event details page.	System administrator	View a list of events and their associated attributes, such as execution time, event description, tenant name, target type and ID, and other characteristics. Click **Administration > Event Logs**.
Monitor the status of your requests and view request details.	Tenant administrator or business group manager	Display the status of requests that you are responsible for or have ownership of. Click **Requests**.

Index