IaaS Integration for Multi-Machine Services

vRealize Automation 6.2

vmware®

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

https://docs.vmware.com/

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 Integration for Multi-Machine Services

IaaS Integration for Multi-Machine Services describes how to integrate multi-machine services in an existing VMware vRealize Automation 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*

After the Infrastructure as a Service (IaaS) is set up for a relevant machine type, this documentation guides you through the following processes:

- Preparing for provisioning
- Creating and configuring multi-machine blueprints
- Configuring component machines for network and security virtualization

All of the IaaS configuration tasks that should be completed before 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 vRealize Automation are available in all editions. For a comparison of feature sets in each edition, see https://www.vmware.com/products/vrealize-automation/.

Intended Audience

This information is intended for IaaS administrators, tenant administrators and business group managers, and fabric administrators who want to integrate multi-machine services and network and security virtualization into their vRealize Automation 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.

Updated Information

This *IaaS Integration for Multi-Machine Services* is updated with each release of the product or when necessary.

This table provides the update history of the *IaaS Integration for Multi-Machine Services*.

Revision	Description
001642-03	Added "Troubleshooting a Partially Successful Multi-Machine Deployment Message," on page 50.
001642-02	Updated "Enable App Isolation for Component Machines," on page 46 and Chapter 2, "Configuring Network and Security Integration," on page 11 to include information about load balancing and app isolation.
001642-01	■ Updated "Configure Routed Network Profile IP Ranges," on page 22. ■ Removed an erroneous statement about archive periods from Chapter 4, "Creating Multi-Machine Blueprints," on page 29. ■ Updated "Specifying Scripts for Multi-Machine Service Provisioning," on page 29.
001642-00	Initial 6.2 release.

Using the Goal Navigator

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

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 vRealize Automation 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

With the multi-machine services feature of vRealize Automation, users can provision multi-machine services, and their component machines, in a virtual datacenter based on existing templates.

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

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

This chapter includes the following topics:

Multi-Machine Service Concepts

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 vRealize Automation:

- 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.

These concepts apply to multi-machine services in vRealize Automation.

Component Blueprint	A machine blueprint that is part of a multi-machine 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 multi-machine service.
Component Machine	A machine that is managed as part of a multi-machine service. A multi-machine service might include several component machines.
Multi-machine Blueprint	A blueprint that defines a multi-machine service.
Multi-machine Service	A compound service composed of multiple machines that vRealize Automation can provision and manage as a single entity.

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

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 run during the provisioning process or when powering the multi-machine service on or off. Distributed Execution Manager worker services or agents, not the component machines, run the scripts.

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, vRealize Automation allocates resources for all of the component machines. If the multi-machine service causes 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 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.

Comparing Multi-Machine Services and vApps

You can use vRealize Automation multi-machine services or vApps to group component machines.

Table 1-1. Comparison of Multi-Machine Service and vApp (vCloud) Features

vRealize Automation Multi-Machine Service	vApp (vCloud)
Create a multi-machine blueprint that references individual machine blueprints in vRealize Automation.	Use existing vApp templates created in vCloud Director or vCloud Air.
Provision machines of any type (virtual, physical, or cloud) as part of a service.	Provision virtual machines from vCloud Director or vCloud Air.
Use vRealize Automation to manage component machines of a multi-machine service.	Use vCloud Director or vCloud Air to manage vApp machines.
Application-specific networks can 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.
vRealize Automation defines startup and shutdown order.	The vApp template defines startup and shutdown order.

For both, access to the component portal for Microsoft Remote Desktop Protocol, Virtual Network Computing, and SSH depends on the guest and console and the endpoint.

Configuring IaaS for Multi-Machine Services Checklist

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

For information about how to create the necessary network profiles, fabric groups, business groups, reservation policies, and machine endpoints, see the following documents:

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

The following high-level checklist shows the tasks required to integrate multi-machine services into an existing vRealize Automation deployment.

Table 1-2. Configuring IaaS for multi-machine services checklist

Task	Required Role
❑ Configure vRealize Automation workflows to call vRealize Orchestrator workflows. See "Create a vRealize Orchestrator Endpoint," on page 12.	Outside of vRealize Automation
❑ Create a vSphere endpoint to allow vRealize Automation to interact with a vCloud Networking and Security or NSX instance. See "Create a vSphere Endpoint for Networking and Security Virtualization," on page 14.	IaaS administrator
❑ Create network profiles. To use the vCloud Networking and Security or NSX endpoint you must create a routed network profile. See "Creating a Network Profile," on page 15.	Fabric administrator
❑ Create a reservation to assign networks and security groups. See "Create a Reservation," on page 24.	IaaS administrator

Table 1-2. Configuring IaaS for multi-machine services checklist (Continued)

Task	Required Role
❑ Depending on your customization needs, you can configure scripts, custom properties, and actions for the multi-machine service. See Chapter 4, "Creating Multi-Machine Blueprints," on page 29.	■ Tenant administrator ■ Business group manager
❑ Create multi-machine blueprints. See "Create a Multi-Machine Blueprint," on page 31.	■ Tenant administrator ■ Business group manager
❑ Configure multi-machine blueprints to provision to virtualized networks based on the vCloud Networking and Security or NSX platform. See Chapter 5, "Configuring Multi-Machine Blueprints for Network and Security Virtualization," on page 37.	■ Tenant administrator ■ Business group manager
❑ Publish multi-machine blueprints. See "Publish a Blueprint," on page 36.	■ Tenant administrator ■ Business group manager

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

Configuring Network and Security Integration

2

vRealize Automation supports virtualized networks based on the vCloud Networking and Security and NSX platforms. Network and security virtualization allows virtual machines to communicate with each other over physical and virtual networks securely and efficiently.

To integrate network and security with vRealize Automation an IaaS administrator must install the vCloud Networking and Security or NSX plug-ins in vRealize Orchestrator and create vRealize Orchestrator and vSphere endpoints.

A fabric administrator can create network profiles that specify network settings in reservations and blueprints. External network profiles define existing physical networks. NAT, routed, and private network profiles are templates for configuring network interfaces when you provision virtual machines, and for configuring NSX Edge devices created when you provision multi-machines.

Note When deploying a multi-machine that uses both an NSX Edge load balancer and app isolation, the dynamically provisioned load balancer is not added to the security group with the other multi-machine blueprint components. This prevents the load balancer from communicating with the machines for which it is meant to handle connections. Because Edges are excluded from the NSX distributed firewall, they cannot be added to security groups. To allow load balancing to function properly, use another security group or security policy that allows the required traffic into the component VMs for load balancing.

A tenant administrator or business group manager can configure network adapters, load balancing, and security for all components provisioned from a multi-machine blueprint that uses a routed network profile.

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 can select a transport zone that identifies the vSphere endpoint. A transport zone specifies the hosts and clusters that can be associated with logical switches created within the zone. A transport zone can span multiple vSphere clusters. 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. See *NSX Administration Guide*.

- Configuring vRealize Orchestrator Endpoints on page 12

  If you are using vRealize Automation workflows to call vRealize Orchestrator workflows, you must configure the vRealize Orchestrator instance or server as an endpoint.

- Create a vSphere Endpoint for Networking and Security Virtualization on page 14

  An IaaS administrator creates an instance of a vSphere endpoint to allow vRealize Automation to interact with a vCloud Networking and Security or NSX instance.

- Run the Enable Security Policy Support for Overlapping Subnets Workflow in vRealize Orchestrator on page 15

  Before you use the NSX security policy features from vRealize Automation, an administrator must run the Enable security policy support for overlapping subnets workflow in vRealize Orchestrator.

- Creating a Network Profile on page 15

  A fabric administrator creates external network profiles and templates for network address translation (NAT), routed, and private network profiles.

- Configuring a Reservation for Network and Security Virtualization on page 23

  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.

Configuring vRealize Orchestrator Endpoints

If you are using vRealize Automation workflows to call vRealize Orchestrator workflows, you must configure the vRealize Orchestrator instance or server as an endpoint.

You can associate a vRealize Orchestrator endpoint with a multi-machine blueprint to make sure that all of the vRealize Orchestrator workflows for machines provisioned from that blueprint are run using that endpoint.

vRealize Automation by default includes an embedded vRealize Orchestrator instance. It is recommended that you use this as your vRealize Orchestrator endpoint for running vRealize Automation workflows in a test environment or creating a proof of concept . For more information about managing the embedded vRealize Orchestrator instance, see *Advanced Service Design*.

You can also install a plug-in on an external vRealize Orchestrator server.

It is recommended that you use this vRealize Orchestrator endpoint for running vRealize Automation workflows in a production environment.

To install the plug-in, see the README available with the plug-in installer file from the VMware product download site at http://vmware.com/web/vmware/downloads under the vCloud Networking and Security or NSX links.

Create a vRealize Orchestrator Endpoint

vRealize Automation uses vRealize Orchestrator endpoints to run network and security-related workflows. You can configure multiple endpoints to connect to different vRealize Orchestrator servers. Each endpoint must have a priority.

When executing vRealize Orchestrator workflows, vRealize Automation tries the highest priority vRealize Orchestrator endpoint first. If that endpoint is not reachable, then it proceeds to try the next highest priority endpoint until a vRealize Orchestrator server is available to run the workflow.

Prerequisites

- Log in to the vRealize Automation console as an **IaaS administrator**.
- Verify that the NSX plug-in is installed in vRealize Orchestrator.

  The installation instruction is available in a README file from the VMware product download site at http://vmware.com/web/vmware/downloads under the VMware NSX or VMware vCloud Networking and Security links.

Procedure

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

2 Select **New Endpoint > Orchestration > vCenter Orchestrator**.

3 Enter a name and, optionally, a description.

4 Type a URL with the fully qualified name or IP address of the vRealize Orchestrator server and the vRealize Orchestrator port number.

The format depends on the version of the vRealize Orchestrator server.

vRealize Orchestrator version	URL format
5.1	https://*hostname*:*port*
5.5	https://*hostname*:*port*/vco

The transport protocol must be HTTPS. If no port is specified, the default port 8281 is used.

To use the default vRealize Orchestrator instance embedded in the vRealize Appliance, type **`https://vrealize-automation-appliance-hostname:8281/vco`**.

5 Specify the credentials to use to connect to this endpoint.

a Click the ellipsis next to the **Credentials** field.

b Select an existing credential from the list or click **New Credentials** to provide your vRealize Orchestrator credentials.

The credentials you use should have Execute permissions for any vRealize Orchestrator workflows to call from IaaS.

To use the default vRealize Orchestrator instance embedded in the vRealize Appliance, the user name is **`administrator@vsphere.local`** and the password is the administrator password that was specified when configuring SSO.

6 Specify the endpoint priority.

a Click **New Property**.

b Type **`VMware.VCenterOrchestrator.Priority`** in the **Name** text box.

The property name is case sensitive.

c Type an integer greater than or equal to 1 in the **Value** text box.

Lower value means higher priority.

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

7 Click **OK**.

8 From the Endpoints column, point to the vRealize Orchestrator endpoint and click **Data Collection** from the drop-down menu.

The data collection process takes 2-3 minutes to check whether the associated NSX plug-in is installed on this endpoint.

9 Verify that you receive a status message that confirms the data collection process for the vRealize Orchestrator endpoint is successful.

What to do next

Create a networking solution endpoint. See "Create a vSphere Endpoint for Networking and Security Virtualization," on page 14.

Create a vSphere Endpoint for Networking and Security Virtualization

An IaaS administrator creates an instance of a vSphere endpoint to allow vRealize Automation to interact with a vCloud Networking and Security or NSX instance.

For a vSphere endpoint in vRealize Automation, all of the NSX related networking operations for that endpoint must be completed on the same vRealize Orchestrator server.

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 traced back to vRealize Automation.

Prerequisites

- Log in to the vRealize Automation console as an **IaaS administrator**.
- Verify that a system administrator installed a vCloud Networking and Security or NSX instance, and that it is accessible.
- Verify that an IaaS administrator 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.
- Verify that an IaaS administrator 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 in 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 to implement networking and security virtualization.

4 Type the URI for the management console of the vCloud Networking and Security or NSX instance in the **Address** text box to register the instance to the vSphere endpoint.

The URL must be of the type: **`https://`*`hostname`*** or **`https://`*`IP_address`***.

For example, **`https://vCNSa`**.

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

6 Click **OK**.

7 Select **Infrastructure > Compute Resources > Compute Resources**.

8 Point to the vSphere compute resource to configure data collection and click **Data Collection** from the drop-down menu.

The data collection process synchronizes the vSphere and the vCloud Networking and Security or NSX inventories to vRealize Automation. This process creates a vCloud Networking and Security or NSX endpoint in vRealize Orchestrator that is used during data collection.

9 Verify that you receive a status message that confirms the data collection process for the vRealize Orchestrator endpoint is successful.

What to do next

If you plan to use the NSX security policy features from vRealize Automation, you must run a workflow. See "Run the Enable Security Policy Support for Overlapping Subnets Workflow in vRealize Orchestrator," on page 15.

Run the Enable Security Policy Support for Overlapping Subnets Workflow in vRealize Orchestrator

Before you use the NSX security policy features from vRealize Automation, an administrator must run the Enable security policy support for overlapping subnets workflow in vRealize Orchestrator.

Security policy support for the overlapping subnets workflow is applicable to a VMware NSX 6.1 and later endpoint. Run this workflow only once to enable this support.

Prerequisites

- Verify that a vSphere endpoint is registered with an NSX endpoint.
- Log in to the vRealize Orchestrator Client as an Administrator.

Procedure

1 Select the **Workflow** tab to navigate through the library to the **NSX > NSX workflows for VCAC** folder.

2 Run the **Enable security policy support for overlapping subnets** workflow.

3 Select the NSX endpoint as the input parameter for the workflow.

Use the IP address you specified when you created the vSphere endpoint to register an NSX instance.

After you run this workflow, the Distributed Firewall rules defined in the security policy are applied only on the vNICs of the security group members to which this security policy is applied.

What to do next

Apply the applicable security features for the multi-machine blueprint.

Creating a Network Profile

A fabric administrator creates external network profiles and templates for network address translation (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 the types of networks.

Table 2-1. Available Network Types for a Network Profile

Network Type	Description
External networks	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 virtual networks	Created during provisioning. 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.

Table 2-1. Available Network Types for a Network Profile (Continued)

Network Type	Description
Routed virtual networks	Created during provisioning. 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 can communicate with each other and the external network. A routed network profile defines a routable space and available subnets.
Private virtual networks	Created during provisioning. 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 VMware Remote Console option in vRealize Automation. A private network profile defines an internal network, ranges of static IP addresses, and a range of DHCP addresses.

In general, vRealize Automation 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 reclaimed for reassignment when the machine is destroyed and the ReclaimDestroyedStaticIPAddresses workflow runs.

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 vRealize Automation console as a **fabric administrator**.

Procedure

1 Specify External 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 External Network Profile IP Ranges on page 17

A fabric administrator can define zero (0) 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 External 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

- Verify that you have a gateway IP address.
- Log in to the vRealize Automation console as a **fabric administrator**.

Procedure

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

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

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

What to do next

You can configure IP ranges for static IP addresses. See "Configure External Network Profile IP Ranges," on page 17.

Configure External Network Profile IP Ranges

A fabric administrator can define zero (0) 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 External 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 Enter a name and, optionally, a description.

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

5 Enter 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.

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 vRealize Automation. 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) Filter IP address entries to only those that match.

a Click in the **Defined IP Addresses** text boxes.

b Type a partial IP address or machine name, or select a date from the Last Modified drop-down calendar.

The IP addresses that match the filter criteria appear.

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 vRealize Automation console as a **fabric administrator**.

Procedure

1 Specify Private Network Profile Information on page 18

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

2 Configure Private Network Profile IP Ranges on page 19

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

Specify Private Network Profile Information

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

Prerequisites

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

Procedure

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

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

3 Enter 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.

The DHCP range cannot overlap the range of static IP addresses.

7 (Optional) Set a lease time to define how long a machine can use an IP address.

What to do next

You can configure IP ranges for static IP addresses. See "Configure Private Network Profile IP Ranges," on page 19.

Configure Private Network Profile IP Ranges

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

Prerequisites

"Specify External 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 Enter a name and, optionally, a description.

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

5 Enter 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.

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 vRealize Automation. 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) Filter IP address entries to only those that match.

a Click in the **Defined IP Addresses** text boxes.

b Type a partial IP address or machine name, or select a date from the Last Modified drop-down calendar.

The IP addresses that match the filter criteria appear.

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 vRealize Automation console as a **fabric administrator**.

Procedure

1 Specify NAT Network Profile Information on page 20

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 NAT Network Profile IP Ranges on page 21

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

Specify NAT 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 vRealize Automation 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 Enter 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.

10 (Optional) Set a lease time to define how long a machine can use an IP address.

What to do next

A NAT network profile requires DHCP information or an IP range. For information about how to create an IP range, see "Configure NAT Network Profile IP Ranges," on page 21.

Configure NAT Network Profile IP Ranges

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

Prerequisites

"Specify External 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 Enter a name and, optionally, a description.

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

5 Enter 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.

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 vRealize Automation. 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) Filter IP address entries to only those that match.

a Click in the **Defined IP Addresses** text boxes.

b Type a partial IP address or machine name, or select a date from the Last Modified drop-down calendar.

The IP addresses that match the filter criteria appear.

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 vRealize Automation console as a **fabric administrator**.

Procedure

1 Specify Routed Network Profile Information on page 22

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

2 Configure Routed Network Profile 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 Routed 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 vRealize Automation console as a **fabric administrator**.
- "Create an External Network Profile," on page 16.
- Verify that the NSX logical router is configured in the vSphere Client to use the routed network profile. See *NSX Administration Guide*.

Procedure

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

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

3 Enter 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 Routed Network Profile IP Ranges," on page 22.

Configure Routed Network Profile 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.

When a multi-machine is deleted, its allocated routed network profile range is released after the next static IP addresses workflow runs.

If a multi-machine blueprint contains a routed network profile but not an assignment for the routed network to component network adapters, a catalog item is created but machine provisioning fails with exception error. IP ranges in the routed network profile are listed as allocated but the IP addresses are in use. Ensure that you assign a routed network profile to multi-machine blueprints.

Prerequisites

"Specify External 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, vRealize Automation generates ranges based on the range subnet mask.

For example, vRealize Automation 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 Enter 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 Enter 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**.

Configuring 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.

When vRealize Automation 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. It also 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, vRealize Automation 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 vRealize Automation. 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 you select 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. For NSX, you must have a working NSX Edge instance before you can configure the default gateway for static routes or dynamic routing details for an Edge Services Gateway or Distributed Router. See *NSX Administration Guide*. Inventory data collection must have run.

Create a Reservation

In a reservation, you can 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.

Prerequisites

- Log in to the vRealize Automation console as an **IaaS administrator**.
- Verify that a tenant administrator created a business group. For information about how to create a business group, see *IaaS Configuration for Virtual Platforms*.
- Verify that an IaaS administrator created a vCloud Networking and Security or NSX endpoint. See "Create a vSphere Endpoint for Networking and Security Virtualization," on page 14.
- NSX logical routers must be configured for static or dynamic routing. See *NSX Administration Guide*.
- Security groups must be created and resources configured in the vSphere Client. See *NSX Administration Guide*.
- Verify that the vCenter Server administrator prepared transport zones and clusters.

Procedure

1. Select **Infrastructure > Reservations > Reservations**.
2. Select **New Reservation > Virtual > vSphere (vCenter)**.
3. Select a compute resource on which to provision machines from the **Compute resource** drop-down menu.

   The reservation name appears in the **Name** text box.
4. Select a tenant from the **Tenant** drop-down menu.
5. Select a business group from the **Business group** drop-down menu.

   Only users in this business group can provision machines by using this reservation.
6. (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.

7 (Optional) Type a number in the **Machine quota** text box to set the maximum number of machines that can be provisioned on this reservation.

   Only machines that are powered on are counted towards the quota. Leave blank to make the reservation unlimited.

8 Type a number in the **Priority** text box to set the priority for the reservation.

   The priority is used when a business group has more than one reservation. A reservation with priority 1 is used for provisioning over a reservation with priority 2.

9 (Optional) Deselect the **Enable this reservation** check box if you do not want this reservation active.

10 Click the **Network** tab and assign an external network profile to an external, physical network.

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

      You can select more than one network path on a reservation, but only one network is selected when provisioning a machine.

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

      This option requires additional configuration to configure network profiles.

   c Repeat to enable additional physical networks on this reservation.

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

   A transport zone defines which clusters the multi-machine networks span. The transport zones in a reservation and a multi-machine blueprint must match for provisioning to occur.

12 Select a security group check box in the Security groups list to assign to the reservation.

   Any multi-machine service that is created on this reservation belongs to the selected security group.

13 Select a routed gateway.

   a Select the check box of a routed gateway in the Routed Gateways table to connect to an NSX logical router.

      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 to select more routed gateways.

14 Click **OK**.

Optional Configurations for Multi-Machine Services 3

You can create and configure optional cost profiles to give you more control over computing the cost of the multi-machine services.

For information about how to create and configure cost profiles for the component machines, see the following documents:

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

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

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 3-1. 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 was provisioned.

How Cost Is Displayed

The multi-machine service cost appears 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 3-2. 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. ■ More than one reservation can be available for provisioning the component machines. If these reservations have different compute resources, different cost profiles can apply. ■ More than one datastore can be available for provisioning the component machines, either on the same reservation or on different reservations, that have different storage cost profiles. ■ If either more than one reservation or datastore is available, the daily cost appears 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 use multiplied by the highest cost. If the multi-machine blueprint specifies a value for lease duration, the lease cost appears 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 more than one reservation is available for provisioning the component machines and these reservations have different compute resources that vary in cost. Alternatively, more than one datastore can be 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 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 more than one reservation is 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 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 use 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 the multi-machine as a whole and its component machines.

Creating Multi-Machine Blueprints 4

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 to include in the multi-machine service. A multi-machine blueprint contains references to component blueprints. The component blueprints must be available to the same business 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.

For information about what you can edit in multi-machine blueprints, and their component blueprints, see "Editing Multi-Machine Blueprints," on page 49.

This chapter includes the following topics:

Specifying Scripts for Multi-Machine Service Provisioning

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

For information about how to specify custom logic to run at each stage, see "Specify Scripting Information for a Multi-Machine Blueprint," on page 34.

PowerShell scripts can use the following parameters:

- `VirtualMachine`
- `VirtualMachineProperties`
- `DataContext`

The following PowerShell script is provided as a sample:

```
# Script to Test InvokePowerShell functions
      $VirtualMachine.Notes = "Test";

      foreach ($i in $VirtualMachineProperties)
      {
      $i.PropertyValue = $i.PropertyName;
      }
```

A PowerShell script can modify some `VirtualMachine` fields and property values. Not all `VirtualMachine` parameter fields can be modified.

For related information, see *Import Custom PowerShell Scripts* in *IaaS Configuration for Physical Machines*.

Table 4-1. Script Execution Stages in the Multi-Machine Life Cycle

Stage	Description
Pre-provisioning	Runs after all necessary approvals are complete, but before provisioning any machines.
Post-provisioning	Runs after all component machines are provisioned and powered on.
Pre-startup	Runs before powering on the multi-machine service and all its component machines.
Post-startup	Runs 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 run.
Pre-shutdown	Runs immediately before powering off the multi-machine service and its component machines.
Post-shutdown	Runs after 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 run only during the initial provisioning of a multi-machine service. The startup and shutdown scripts are run 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, vRealize Automation follows a specific order of precedence 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 is 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.

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.

Blueprint Action Settings for Multi-Machine Services

Tenant administrators and business group managers use blueprints to control which actions are available 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 vRealize Automation console as a **tenant administrator** or **business group manager**.

Procedure

1 Specify Blueprint Information for a Multi-Machine Blueprint on page 32

You can configure who can provision machines, how many machines they can provision, and the daily cost of machines.

2 Specify Build Information for a Multi-Machine Blueprint on page 33

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 34

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 34

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

5 Add Multi-Machine Blueprint Custom Properties on page 35

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 Specify Actions for Multi-Machine Blueprints on page 35

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

What to do next

Publish your blueprint to make it available as a catalog item. See "Publish a Blueprint," on page 36.

Specify Blueprint Information for a Multi-Machine Blueprint

You can configure who can provision machines, how many machines they can provision, and the daily cost of machines.

Prerequisites

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

Procedure

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

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

3 Enter 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.

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) Enter 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 plus 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 32.

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

5 Enter a blueprint display name in the **Name** text box.

6 Enter 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.

7 Enter 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.

8 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.

9 If available, type a component blueprint description in the **Description** text box.

This text box might be read-only.

10 Click **Edit** in the Network column to configure network information for the component blueprint.

11 Repeat the steps to edit your component machines as necessary.

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

a Enter 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) Enter 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.

Specify Network Information for a Multi-Machine Blueprint

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

Note If your multi-machine service consists of an NSX logical router that includes routed and private networks, machines on the routed networks cannot access machines on the private networks and vice-versa within that multi-machine service. If you require connectivity between the machines on the routed and private network, add a second virtual network adapter (NIC) to the machines on the routed network and also connect the second adapter to the private network.

See *NSX Administration Guide*.

Prerequisites

- "Specify Build Information for a Multi-Machine Blueprint," on page 33.
- Verify that a fabric administrator created at least one external network profile. See "Create an External Network Profile," on page 16.
- Verify that a vCenter Server administrator prepared transport zones and clusters.

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 span.

3 Choose a network profile.

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

This option requires additional configuration by a fabric administrator to create a reservation policy.

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 34.

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**, enter 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

"Specify Scripting Information for a Multi-Machine Blueprint," on page 34.

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 Add any custom properties to your blueprint.

a Click **New Property**.

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

c Enter the value of the custom property in the **Value** text box.

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

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 users for a value, any value you provide for the custom property is presented to them as the default. If you do not provide a default, users 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 vRealize Automation instance.

Prerequisites

"Add Multi-Machine Blueprint Custom Properties," on page 35.

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 in draft state.

What to do next

Publish your blueprint to make it available as a catalog item. See "Publish a Blueprint," on page 36.

Publish a Blueprint

Blueprints are saved in the draft state and must be manually published before you can configure them as catalog items.

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

Prerequisites

- Log in to the vRealize Automation console as a **tenant administrator** or **business group manager**.
- Create a blueprint.

Procedure

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

2 Point to the blueprint to publish and click **Publish** from the drop-down menu.

3 Click **OK**.

Your blueprint is now ready for tenant administrators, business group managers, and service architects to associate it with a catalog service and entitle users to request it from the catalog.

What to do next

For information about how to configure and manage the catalog, see *Tenant Administration*.

Configuring Multi-Machine Blueprints for Network and Security Virtualization

5

When you provision a multi-machine service in vRealize Automation, 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, external network profiles, and 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 applicable security policies, security groups, and security tags to 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 that fabric administrators create. 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 can connect to existing logical network objects such as routers and switches, or these objects might 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 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. Users can connect to the application through console access only.

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

When you create 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. 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 18.

Prerequisites

- Log in to the vRealize Automation console as a **tenant administrator** or **business group manager**.
- Create a multi-machine blueprint that contains at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 31.

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 > Private**.

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

vRealize Automation 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

Select the new profile when you create a network adapter. See "Configure Network Adapters for Component Machines," on page 41.

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 must 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. Users can connect to the application through network and console access.

The most common use 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.

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 vRealize Automation console as a **tenant administrator** or **business group manager**.
- Verify that a fabric administrator created at least one routed network profile template. See "Create a Routed Network Profile," on page 21.
- Create a multi-machine blueprint that contains at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 31.

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**.

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

vRealize Automation 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. See "Configure Network Adapters for Component Machines," on page 41.

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. 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 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. The application and database tiers have private network profiles and the Web tier has a NAT network profile.

Another use 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, masked 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.

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 vRealize Automation console as a **tenant administrator** or **business group manager**.
- A fabric administrator created at least one NAT network profile template. See "Create a NAT Network Profile," on page 19.
- Create a multi-machine blueprint that contains at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 31.

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**.

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

vRealize Automation 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 required.

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. See "Configure Network Adapters for Component Machines," on page 41.

Configure Network Adapters for Component Machines

A network adapter defines a network connection for a component machine. A tenant administrator or business group manager can configure a network adapter for a multi-machine blueprint, and apply the network adapter to one or more component blueprints in that multi-machine blueprint.

When you request the multi-machine service, vRealize Automation provisions the component machines with the network connection that the network adapter defines. During configuration, when you select an external network profile for the network adapter, you specify an existing external network.

Prerequisites

- Log in to the vRealize Automation 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 31.
- Verify that a fabric administrator created all necessary external network profiles and templates for other types of network profiles. See "Creating a Network Profile," on page 15.
- Verify that a tenant administrator or business group manager created all necessary NAT, routed, and private network profiles. See "Adding Network Profiles to a Multi-Machine Blueprint," on page 38.
- Verify that a fabric administrator created at least one external network profile. 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**.

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.

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

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

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

10 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. Static IP is the only assignment type allowed for routed and one-to-one NAT network profiles. You can only type a static IP address in the **Address** text box for private and NAT network profiles. 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.

11 Click the **Save** icon () to save the network adapter.

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

13 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 you configure a load balancer, you specify a network adapter and select an external, private, NAT, or Routed network profile for the virtual IP address. The network profile you select for the virtual IP address must be the same one that the network adapter uses.

Prerequisites

- Log in to the vRealize Automation console as a **tenant administrator** or **business group manager**.
- Create a multi-machine blueprint that contains at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 31.
- Verify that a tenant administrator added a network profile to the multi-machine blueprint. See "Adding Network Profiles to a Multi-Machine Blueprint," on page 38.
- Verify that a tenant administrator added a network adapter with a Static IP assignment type to the component machine. See "Configure Network Adapters for Component Machines," on page 41.
- Select 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 not editable 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.

vRealize Automation populates the text boxes with typical values.

c Click the **Save** icon () to save the values and select the service.

Selecting a service enables the text boxes for that service.

d (Optional) Repeat to add other services.

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

For vCloud Networking and Security 5.5.2, do not leave this option blank even if disabled. Type **/** as the default value to avoid a load balancer data path error.

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 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**.

Applying Security on a Component Machine

From the Security tab the tenant administrator or business group manager can enable the App isolation and assign security groups, security tags, and security policies to a multi-machine blueprint.

Security policies, security groups, and security tags are defined in the NSX environment. See *NSX Administration Guide*.

Security Group Collection of assets or grouping objects from the vSphere inventory. The grouping feature enables you to create custom containers to which you can assign resources, such as virtual machines and network adapters, for distributed firewall protection. After a group is defined, you can add the group as source or destination to a firewall rule for protection.

	The dynamic mapping capability of security groups let you define the criteria that an object must meet for it to be added to the security group you are creating. This gives you the ability to include virtual machines by defining a filter criteria with a number of parameters supported to match the search criteria. For example, you might include a criteria to add all virtual machines that run a specific operating system such as Microsoft Windows 2003 to the security group.
Security Tag	Include a criteria to add all of the virtual machines tagged with a specified security tag to a security group. Security tags are case sensitive.
Security Policy	During data collection the security policies that have been defined in NSX appear in the Security tab. The tenant administrator or business group manager can assign security policies on selected component machines. For example, for a Web component you can apply a Web security policy. A security policy is a set of endpoint, firewall, and network introspection services that can be applied to a security group.
App Isolation	Use the logical firewall to prevent all of the inbound and outbound traffic to the applications in the multi-machine blueprint. The component machines in the multi-machine blueprints can communicate with each other but cannot connect outside the firewall. The vRealize Automation App Isolation security policy has a precedence value of 3456. If the 3456 precedence value is applied to another component, the deployment fails.

Specify Security Policy, Groups, and Tags for Component Machines

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

When you configure security groups for a component machine, 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 groups 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," on page 24.

Security policies, security groups, and security tags appear for selection only if there are no existing component machines provisioned from this multi-machine blueprint. If a component machine is provisioned, then you cannot edit the security settings of the machine.

Familiarize yourself with the security features that can be applied to a multi-machine blueprint. See "Applying Security on a Component Machine," on page 43.

Prerequisites

- Log in to the vRealize Automation console as a **tenant administrator** or **business group manager**.
- Create a multi-machine blueprint that contains at least one virtual component blueprint. See "Create a Multi-Machine Blueprint," on page 31.
- Verify that the supported version of VMware Tools is installed on the component machines. See *NSX Installation and Upgrade Guide*.

- Verify that the NSX endpoint is configured to use the vRealize Automation security policy. See "Run the Enable Security Policy Support for Overlapping Subnets Workflow in vRealize Orchestrator," on page 15.
- Verify that the security policies, security groups, and security tags are defined in the NSX environment. See *NSX Administration Guide*.

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 **Security** tab.

8 Select one or more security policies check boxes in the Security policies list.

9 Select one or more security group check boxes in the Security groups list.

10 Select one or more security tags check boxes in the Security tags list.

11 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 vRealize Automation 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 addresses.

Prerequisites

- Log in to the vRealize Automation console as a **tenant administrator** or **business group manager**.
- Create a reservation policy. If reservations already use this policy, they must be intended for use with a routed gateway.
- Create a multi-machine blueprint. See "Create a Multi-Machine Blueprint," on page 31.

Procedure

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

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

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**.

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

Enable App Isolation for Component Machines

When App Isolation is enabled for a vRealize Automation multi-machine blueprint, the firewall blocks all inbound and outbound traffic to the component machines of the blueprint. The component machines of the multi-machine blueprint can communicate with each other but cannot connect outside the firewall.

When a multi-machine service is provisioned with App isolation, vRealize Automation creates a security group corresponding to the multi-machine service and assigns the component machines as members of that security group. The security policy called vRealize Automation App Isolation policy in NSX is created and applied to the security group. The firewall rules are defined in the security policy to allow only internal traffic.

Note When deploying a multi-machine that uses both an NSX Edge load balancer and the App Isolation checkbox option, the dynamically provisioned load balancer is not added to the security group with the other multi-machine blueprint components. This prevents the load balancer from communicating with the machines for which it is meant to handle connections. Because Edges are excluded from the NSX distributed firewall, they cannot be added to security groups. To allow load balancing to function properly, use another security group or security policy that allows the required traffic into the component VMs for load balancing.

The vRealize Automation App Isolation policy has a lower precedence compared to other security policies in NSX. For example, if a multi-machine service contains a Web component machine and an App component machine and the Web component machine hosts a Web service, then the service must allow inbound traffic on ports 80 and 443. In this case, users must create a Web security policy in NSX with firewall rules defined to allow incoming traffic to these ports. In vRealize Automation, users must apply the Web security policy on the Web component of the multi-machine blueprint.

If the Web component machine needs access to the App component machine using a load balancer on ports 8080 and 8443, the Web security policy should also include firewall rules to allow outbound traffic to these ports in addition to the existing firewall rules that allow inbound traffic to ports 80 and 443.

Familiarize yourself with the security features that can be applied to a multi-machine blueprint. See "Applying Security on a Component Machine," on page 43.

Prerequisites

- Log in to the vRealize Automation console as a **tenant administrator** or **business group manager**.
- Create a multi-machine blueprint. See "Create a Multi-Machine Blueprint," on page 31.
- Verify that an IaaS administrator created a vCloud Networking and Security or NSX endpoint. See "Create a vSphere Endpoint for Networking and Security Virtualization," on page 14.
- Verify that the supported version of VMware Tools is installed on the component machines. See NSX product documentation

Procedure

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

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

3 Click the **Network** tab.

4 Click the App Isolation check box under Security to enable the option.

5 Click **OK**.

What to do next

Publish your blueprint to make it available as a catalog item. See "Publish a Blueprint," on page 36.

Managing Multi-Machine Services 6

After you create and configure a multi-machine service you can perform several management tasks such as edit an existing multi-machine blueprint, view the status of scheduled and completed workflows, or display the default log information.

This chapter includes the following topics:

Editing Multi-Machine Blueprints

You can edit certain aspects of an existing multi-machine blueprint.

Restrictions exist for configuring component machines if the blueprint provisioned existing multi-machine services:

- 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 because of 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 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

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

Table 6-1. 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. Select **Infrastructure > Monitoring > Audit Logs**. The audit log provides details about 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. Select **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. Select **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. Select **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 run time, event description, tenant name, target type and ID, and other characteristics. Select **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 own. Click **Requests**.

Troubleshooting a Partially Successful Multi-Machine Deployment Message

A multi-machine blueprint request is reported as partially succeeded even though provisioning succeeded fully and deployments are accessible from the Items and Managed Machines tabs in vRealize Automation.

Problem

vRealize Automation indicates that a multi-machine blueprint provisioning request was only partially successful when in fact it was fully successful.

Cause

The incorrect message is caused by a synchronization issue that has since been resolved by a workaround procedure. The procedure requires an additional custom property. The workaround is fully documented in the VMware Knowledge Base.

Solution

1 Navigate to Knowledge Base article *Multi-Machine Blueprint Reported as Partially Succeeded But All the Components Provisioned Correctly (2132084)* at http://kb.vmware.com/kb/2132084.

2 Follow the procedure as documented in the KB.

For vRealize Automation 6.2.5, you only need to obtain and add the `AppService.SyncMachines.MachineProvisioned` custom property to your blueprint to avoid this issue. vRealize Automation 6.2.5 users do not need to perform the rest of the procedure documented in the KB article.

Index