Using the NSX-vRO Plug-In 1.2

vRealize Orchestrator 7.3

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

https://docs.vmware.com/

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

Introduction to the NSX-vRO Plug-In

1

You can use the NSX-vRO Plug-In to automate NSX workflows using the VMware vRealize ™ Orchestrator ™, utilizing the pre-existing workflows that work directly with the NSX REST API.

See the *NSX-vRO Plug-In Release Notes* for installation instructions: http://pubs.vmware.com/Release_Notes/en/nsx/suite/releasenotes_nsx_vro_110.html

Using the NSX-vRO Plug-In

Using the *NSX-vRO Plug-In* provides information and instructions about how to configure and use the NSX-vRO Plug-In for VMware® vRealize Orchestrator. You can use the NSX-vRO Plug-In to automate NSX workflows using the vRealize Orchestrator, utilizing the pre-existing workflows that work directly with the NSX REST API.

Intended Audience

This information is intended for anyone who is installing and configuring the plug-in, using the plug-in API, or using the workflow library. The information in *Using the NSX-vRO Plug-In* is written for experienced users who are familiar with VMware virtual machine technology, with Orchestrator workflow development and with NSX.

For more information about Orchestrator, see
http://www.vmware.com/support/pubs/orchestrator_pubs.html.

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.

Configuration Workflows 2

The Configuration workflows are used to manage NSX endpoints and SSL certificates. You can access the workflows from **Library > NSX > Configuration** on the Workflows view in the Orchestrator client. You can run these workflows from the Run and Design modes.

This chapter includes the following topics:

- Create NSX Endpoint
- Delete all Endpoints
- Sync NSX Endpoint

Create NSX Endpoint

You create an NSX endpoint in order to register an NSX endpoint in vRealize Orchestrator. All other workflows exposed by the plug-in require an NSX endpoint as a mandatory input parameter.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > Configuration > Create NSX endpoint**.

2 Click the green **Start Workflow** icon.

3 Enter a unique name in the **Endpoint name** text box.

4 Enter the NSX Manager user name and password.

5 Enter the URL of the NSX Manager using its IP address of FQDN (Fully Qualified Domain Name).

6 Enter a value for the number of retries that the workflow attempts before stopping.

7 To configure the length of time vRealize Orchestrator waits for a connection or response, enter a timeout value (in seconds) in the **Duration after which operation should timeout** text box.

8 Click **Submit** to start the workflow.

Delete all Endpoints

You can use this workflow to delete all NSX endpoints. This workflow removes all the existing NSX endpoints registered in this vRO.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Configuration > Delete all endpoints**.
2. Click the green **Start Workflow** icon.
3. Enter Yes to confirm that you want to delete all endpoints.
4. Click **Submit**.

Sync NSX Endpoint

Since NSX Manager roles and relationships can change over time, you can run this workflow to synchronize NSX properties (version, role, related NSX Managers, etc.) with the latest configuration of NSX.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Configuration > Sync NSX endpoint**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object. If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Click **Submit**.

Edge Features Workflows

3

The Edge workflows are used to create and manage Edge configurations. You can access the workflows from Library > NSX > Edge Features on the Workflows view in the Orchestrator client. You can run these workflows from the Run and Design modes.

Table 3-1. Edge Features Workflows

Workflow	Description
Add Interface	Use this workflow to add an interface to an NSX Edge. To run this workflow, complete the following parameters: ■ Select the NSX Connection object (NSX endpoint). ■ Select the NSX Edge object. ■ Enter the name of the interface. ■ Enter the index of the router interface. ■ Enter the logical switch or the Network or Portgroup connected to the interface. ■ Enter the IP address specification of the interface. ■ Enter the type of interface (uplink, internal, trunk). ■ Enter the MTU value. ■ Choose whether to indicate if the interface is connected.
Compose Edge	Use this workflow to create a service edge (ESG) on NSX. This workflow completes only after the Edge is successfully created and configured in NSX. To run this workflow, complete the following parameters: ■ Enter the common parameters. ■ Select the appliances. ■ Enter the Edge vNICs. ■ Enter the CLI settings. ■ Enter the default gateway settings. ■ Enter the HA settings. ■ Enter Syslog settings.
Configure Appliance Size	Use this workflow to configure the size of the NSX Edge appliance (or both appliances if HA). Typical sizes are compact, large, x-large and quad-large. To run this workflow, complete the following parameters: ■ NSX Connection object. ■ NSX Edge object. ■ Enter the appliance size (compact, large or x-large).

Table 3-1. Edge Features Workflows (Continued)

Workflow	Description
Configure Default Gateway	Use this workflow to configure the default gateway. To run this workflow, complete the following parameters: ■ Select the NSX Connection endpoint. ■ Select the NSX Edge object. ■ Enter the NSX Edge vNIC index. ■ Enter the IP address of the gateway. ■ Enter the MTU value. ■ Enter a description of the gateway.
Configure Edge Appliance	Use this workflow to configure the size of the NSX Edge appliance (or both appliances if HA). Typical sizes are compact, large, x-large and quad-large. To run this workflow, complete the following parameters: ■ Choose whether you want to deploy appliances. ■ Enter the HA index. ■ Enter the IDs of the resource pool or cluster, datastore, host and VM folder.
Configure Edge CLI Settings	Use this workflow to configure the CLI settings on the edge. To run this workflow, complete the following parameters: ■ Enter a user name and password for CLI access. ■ Choose whether to enable SSH and auto rule generation. ■ Enter the log level values.
Configure Edge Syslog	Use this workflow to configure syslog servers for an NSX Edge. To run this workflow, complete the following parameters: ■ Enter the protocol. ■ Enter the server IP address of the syslog servers.
Configure HA	Use this workflow to configure HA (High Availability) settings on the NSX Edge. This workflow completes only after the HA is successfully configured on NSX. To run this workflow, complete the following parameters: ■ Select the NSX Connection object. ■ Select NSX Edge object. ■ Choose whether to enable HA. ■ Set a declared dead time (time to listen for a heartbeat). The default value is 15 seconds. ■ Select the management IP addresses (must be in CIDR format with /30 subnet and must not overlap with any vNIC subnets). ■ Choose whether to enable logging. ■ Enter the log level. Typical values are Emergency, Alert, Critical, Error, Warning, Notice and Debug. The default value is Info.

Table 3-1. Edge Features Workflows (Continued)

Workflow	Description
Delete Interface	Use this workflow to delete an NSX Edge interface. To run this workflow, complete the following parameters: ■ Select the NSX Connection object. ■ Select the NSX Edge object. ■ Enter the NSX Edge vNIC or interface to be deleted (inventory selection). ■ Enter the NSX Edge vNIC or interface index to be deleted (user-provided index). **Note** The interface index is ignored if the interface to be deleted is selected.
Get Edge	Use this workflow to return the NSX Edge inventory object. To run this workflow, complete the following parameters: ■ Select the NSX Edge object.
Get Interface	Use this workflow to return an edge interface from inventory. To run this workflow, complete the following parameters: ■ Select the NSX Connection object. ■ Select the NSX Edge object. ■ Select the NSX Edge vNIC (inventory selection). ■ Select the NSX Edge vNIC Index (user-provided index). **Note** The vNIC Index is ignored if the Edge vNIC is selected.
Modify Interface	Use this workflow to modify an interface of an NSX Edge. To run this workflow, complete the following parameters: ■ Select the NSX Connection object. ■ Select the NSX Edge object. ■ Select the NSX Edge Interface to be modified (inventory selection). ■ Select the NSX Edge Interface Index to be modified (user-provided index). **Note** The NSX Edge Interface Index is ignored if NSX Edge Interface is selected. ■ Enter the name of the interface. ■ Enter the logical switch or the Network or Portgroup connected to the interface. ■ Enter the IP address specification for the interface. ■ Enter the type of interface (uplink, internal or trunk). ■ Enter the MTU value. ■ Choose whether to indicate if the interface is connected.

Table 3-1. Edge Features Workflows (Continued)

Workflow	Description
Redeploy Edge	Use this workflow to redeploy an NSX Edge. To run this workflow, complete the following parameters: ■ Select the NSX Connection object. ■ Select the NSX Edge object.
Update Edge	Use this workflow to update a service edge (ESG) on NSX. This workflow completes only after the NSX Edge has been successfully updated and configured in NSX. To run this workflow, complete the following parameters: ■ Enter the common parameters. ■ Select the appliances. ■ Select the interface. ■ Enter the CLI settings. ■ Enter the default gateway settings. ■ Enter the HA settings. ■ Enter the Syslog settings.

Firewall Features Workflows 4

The Firewall Features workflows are used to create and manage a firewall layer 3 section. You can access the workflows from Library > NSX > Firewall on the Workflows view in the Orchestrator client. You can run these workflows from the Run and Design modes.

Table 4-1. Firewall Feature Workflows

Workflow	Description
Create Firewall Layer 3 Section	Use this workflow to create an application firewall layer 3 section. To run this workflow, complete the following parameters: ■ Select the NSX Connection object. ■ Enter the name of the layer 3 section. ■ Enter the list of firewall rules. ■ Set the operation (for position of section) using the supplied values (insert_after, insert_before, insert_top, insert_before_default). ■ Enter the anchor ID. ■ Specify if you want to auto save the draft.
Delete Firewall Layer 3 Section	Use this workflow to delete a firewall layer 3 section. To run this workflow, complete the following parameters: ■ Select the NSX Connection object. ■ Select the firewall section to delete.
Delete Rules from Firewall Section	Use this workflow to delete rules from a firewall layer 3 section. To run this workflow, complete the following parameters: ■ Select the NSX Connection object. ■ Select the firewall section from which rules are to be deleted. ■ Set the list of rule IDs to be deleted from the firewall section.

Table 4‑1. Firewall Feature Workflows (Continued)

Workflow	Description
Get Firewall Layer 3 Section	Use this workflow to retrieve a firewall layer 3 inventory object. To run this workflow, complete the following parameters: ■ Select the NSX Connection object. ■ Select the Firewall Section Object from inventory.
Update Firewall Layer 3 Section	Use this workflow to update an application firewall layer 3 section. To run this workflow, complete the following parameters: ■ Select the NSX Connection object. ■ Select the section to be updated. ■ Enter the name of the layer 3 section. ■ Enter the list of firewall rules. ■ Set the operation (for position of section) using the supplied values. ■ Enter the anchor ID. ■ Specify if you want to auto save the draft.

Load Balancer Workflows 5

The Load Balancer workflows are used to manage and configure application profiles and rules, monitors, pools and virtual servers. You can access the workflows from **Library > NSX > Load balancer** on the Workflows view in the Orchestrator client. You can run these workflows from the Run and Design modes.

This chapter includes the following topics:

- Get Virtual Server by ID
- Modify Application Profile
- Modify Application Rule
- Modify Monitor
- Modify Pool
- Modify Virtual Server

Configure Global Settings of Load Balancer

You can use this workflow to configure the NSX Edge load balancer global settings, including service insertion profiles, acceleration and logging.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Configure global settings of load balancer**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge.
5. Choose whether you want to enable load balancer on the NSX Edge.
6. Choose whether you want to enable service insertion.
7. Choose whether you want to enable acceleration.
8. Choose whether you want to enable logging.
9. Enter the level of logging to use.
10. Click **Submit**.

Create Application Profile

You can use this workflow to add an application profile to the current set of application profiles.

An application profile is created to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic and makes traffic management tasks easier and more efficient.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Create application profile**.
2. Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Enter the name of the application profile.

6 Enter the type of the application profile.

7 Choose whether to insert forwarded for.

8 Select the persistence.

9 Click **Submit**.

Create Application Rule

You can use this workflow to add an application rule to the current set of application rules. An application rule can be used to directly manipulate and manage IP application traffic.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Create application rule**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Enter the name of the application rule.

6 Enter the ACL script to be pushed to the NSX Edge.

7 Enter a description of the application rule.

8 Click **Submit**.

Create Monitor

You can use this workflow to add a monitor to the current set of service monitors.

A service monitor is created to define health check parameters for a particular type of network traffic. When you associate a service monitor with a pool, the pool members are monitored according to the service monitor parameters.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Create monitor**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Enter the name of the monitor.

6 Enter the type of monitor (HTTP, HTTPS, TCP).

7 Enter the health check interval and health check timeout.

8 Enter the maximum number of retries for the health check.

9 Enter the monitor method and monitor URL.

10 Enter the expected response string.

11 Enter the URL encoded http POST data for the http(s) protocol.

12 Enter the string to expect in the content for the http(s) protocol.

13 Enter the advanced setting for the monitor to fill more customized parameters.

14 Click **Submit**.

Create Pool

You can use this workflow to create a load balancer server pool. A server pool is created to manage and share backend servers flexibly and efficiently. A pool manages load balancer distribution methods and has a service monitor attached to it for health check parameters.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Create Pool**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Enter the name of the backend pool.

6 Enter a description of the backend pool.

7 Enter the load balancing algorithm (round-robin, ip-hash, uri, leastconn). The default is round-robin.

8 Choose whether to enable transparency.

9 Select the load balancer monitor object part of the pool.

10 Select the load balancer pool members.

11 Enter the algorithm parameters. This is required for HTTPHEADER and URL algorithms, but optional for URI.

12 Click **Submit**.

Create Virtual Server

You can use this workflow to create a load balancer virtual server. A virtual server can be an NSX Edge internal or uplink interface.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Create virtual server**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Enter the name of the virtual server.
6. Enter a description of the virtual server.
7. Choose whether to enable the virtual server.
8. Enter the IP address of the virtual server. This should be a valid Edge vNIC IP address.
9. Enter the protocol of the virtual server (HTTP, HTTPS, TCP).
10. Enter the port of the virtual server.
11. Enter the connection limit and connection rate limit.
12. Select the application profile associated with the virtual server.
13. Select the default pool.
14. Select the application profile.
15. Choose whether to enable service insertion.
16. Choose whether to enable acceleration.
17. Click **Submit**.

Delete Application Profile

You can use this workflow to delete a load balancer application profile.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Delete application profile**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Select the application profile to delete.

6 Click **Submit**.

Delete Application Rule

You can use this workflow to delete a load balancer application rule.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Delete application rule**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Select the application rule to delete.

6 Click **Submit**.

Delete Monitor

You can use this workflow to delete a load balancer monitor.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Delete monitor**.

2 Click the green **Start Workflows** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Select the load balancer monitor to delete.

6 Click **Submit**.

Delete Pool

You can use this workflow to delete a load balancer backend pool.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Delete pool**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Select the pool to delete.

6 Click **Submit**.

Delete Virtual Server

You can use this workflow to delete a load balancer virtual server.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Delete virtual server**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Select the virtual server to delete.

6 Click **Submit**.

Get Application Profile

You can use this workflow to retrieve a load balancer application profile object.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Get application profile**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Select the application profile to retrieve.

6 Click **Submit**.

Get Application Profile by ID

You can use this workflow to retrieve a load balancer application profile object using its ID.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Get application profile by ID**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Enter the ID of the application profile you want to retrieve.
6. Click **Submit**.

Get Application Rule

You can use this workflow to retrieve a load balancer application rule object from the vRO inventory.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Get application rule**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Select the application rule to retrieve.
6. Click **Submit**.

Get Application Rule by ID

You can use this workflow to retrieve a load balancer application rule object using its ID.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Get application rule by ID**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Enter the application rule ID.
6. Click **Submit**.

Get Monitor

You can use this workflow to retrieve a load balancer monitor object from the vRO inventory.

Procedure

1. Click the Workflows tab and then navigate to **Library > NSX > Load balancer > Get monitor**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Select the load balancer monitor to retrieve.
6. Click **Submit**.

Get Monitor by ID

You can use this workflow to retrieve a load balancer monitor object using its ID.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Get monitor by ID**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Enter the load balancer monitor ID.
6. Click **Submit**.

Get Pool

You can use this workflow to retrieve a load balancer pool from the vRO inventory.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Get Pool**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Select the load balancer pool to retrieve.
6. Click **Submit**.

Get Pool by ID

You can use this workflow to retrieve a load balancer pool using its ID.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Get pool by ID**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Enter the load balancer pool ID.
6. Click **Submit**.

Get Virtual Server

You can use this workflow to retrieve a load balancer virtual server object from the vRO inventory.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Get virtual server**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Select the virtual server to retrieve.
6. Click **Submit**.

Get Virtual Server by ID

You can use this workflow to retrieve a load balancer virtual server using its ID.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Get virtual server by ID**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Enter the load balancer virtual server ID.

6 Click **Submit**.

Modify Application Profile

You can use this workflow to modify a load balancer application profile.

When selecting the application profile to modify, the fields/input parameters are not pre-populated with the existing values, as vRO does not support pre-population of composite type parameters and parameters with custom data.

Whatever values you enter in the modify workflow input parameters replace the existing values of the corresponding NSX entries. This behavior is consistent with the NSX REST API.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Modify application profile**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Select the application profile to be modified.
6. Enter the name of the application profile.
7. Enter the type of application profile (HTTP, HTTPS, TCP, UDP).
8. Choose whether to insert forwarded for.
9. Select the persistence.
10. Click **Submit**.

Modify Application Rule

You can use this workflow to modify a load balancer application rule.

When selecting the application rule to modify, the fields/input parameters are not pre-populated with the existing values, as vRO does not support pre-population of composite type parameters and parameters with custom data.

Whatever values you enter in the modify workflow input parameters replace the existing values of the corresponding NSX entries. This behavior is consistent with the NSX REST API.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Modify application rule**.
2. Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Select the application rule to be modified.

6 Enter the name of the application rule.

7 Enter the ACL script to be pushed to the NSX Edge.

8 Enter a description of the application rule.

9 Click **Submit**.

Modify Monitor

You can use this workflow to modify a load balancer monitor.

When selecting the monitor to modify, the fields/input parameters are not pre-populated with the existing values, as vRO does not support pre-population of composite type parameters and parameters with custom data.

Whatever values you enter in the modify workflow input parameters replace the existing values of the corresponding NSX entries. This behavior is consistent with the NSX REST API.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Modify monitor**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the NSX Edge object.

5 Select the load balancer monitor to modify.

6 Enter the name of the monitor.

7 Enter the type of monitor (HTTP, HTTPS, TCP).

8 Enter the health check interval and health check timeout.

9 Enter the maximum number of retries for the health check.

10 Enter the monitor method and monitor URL.

11 Enter the expected response string.

12 Enter the advanced setting for the monitor to fill more customized parameters.

13 Enter the URL encoded http POST data for the http(s) protocol.

14 Enter the string to expect in the content for the http(s) protocol.

15 Click **Submit**.

Modify Pool

You can use this workflow to modify a load balancer backend pool.

When selecting the pool to modify, the fields/input parameters are not pre-populated with the existing values, as vRO does not support pre-population of composite type parameters and parameters with custom data.

Whatever values you enter in the modify workflow input parameters replace the existing values of the corresponding NSX entries. This behavior is consistent with the NSX REST API.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Modify Pool**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Select the pool to modify.
6. Enter the name of the pool.
7. Enter a description of the pool.
8. Enter the load balancing algorithm (round-robin, ip-hash, uri, leastconn). The default is round-robin.
9. Choose whether to enable transparency.
10. Select the load balancer monitor object part of the pool.
11. Select the load balancer pool members.
12. Enter the algorithm parameters. This is required for HTTPHEADER and URL algorithms, but optional for URI.
13. Click **Submit**.

Modify Virtual Server

You can use this workflow to modify a load balancer virtual server.

When selecting the virtual server to modify, the fields/input parameters are not pre-populated with the existing values, as vRO does not support pre-population of composite type parameters and parameters with custom data.

Whatever values you enter in the modify workflow input parameters replace the existing values of the corresponding NSX entries. This behavior is consistent with the NSX REST API.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > Load balancer > Modify virtual server**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Select the virtual server to modify.
6. Enter the name of the virtual server.
7. Enter a description of the virtual server.
8. Choose whether to enable the virtual server.
9. Enter the IP address of the virtual server. This should be a valid Edge vNIC IP address.
10. Enter the protocol of the virtual server (HTTP, HTTPS, TCP).
11. Enter the port of the virtual server.
12. Enter the connection limit and connection rate limit.
13. Select the application profile associated with the virtual server.
14. Select the default pool of the virtual server.
15. Select the list of application rules associated with the virtual server.
16. Choose whether to enable service insertion.
17. Choose whether to enable acceleration.
18. Click **Submit**.

6 NSX Workflows

The NSX workflows are used to configure and manage NSX-specific workflows. You can access the workflows from **Library > NSX > NSX workflows** on the Workflows view in the Orchestrator client. You can run these workflows from the Run and Design modes.

This chapter includes the following topics:

- Delete Edge
- Delete IP Set
- Delete Logical Switch
- Delete NAT Rules
- Delete Security Group
- Delete Security Tags from Security Group
- Delete Static Routes from Edge
- Detach Security Tags from a VM
- Disconnect Router Interface
- Get Edge by ID
- Get IP Set
- Get IP Set by ID
- Get Members of Security Group
- Get Members of Security Tag
- Get NAT Rules
- Get Security Tag by ID
- Modify IP Set
- Remove Secondary IP Addresses Assigned to Edge vNIC
- Remove VMs and IP Sets from Multiple Security Groups
- Remove VMs and Load Balancer Pools
- Set Default Route

Add IP Pools to DHCP

You can use this workflow to add a pool of IP addresses to the NSX Edge DHCP service.

NSX Edge provides DHCP service to bind assigned IP addresses to MAC addresses, helping to prevent MAC spoofing attacks. All virtual machines protected by an NSX Edge can obtain IP addresses dynamically from the NSX Edge DHCP service.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Add IP pools to DHCP**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object. If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the Edge ID.

5 Select the DHCP pool. If not set, specify the IP address range, DNS settings and lease parameters of the DHCP pools.

6 Click **Submit**.

Add Load Balancer to Edge

You can use this workflow to add virtual servers and pools to the NSX Edge load balancer service. Load balancing for various services like HTTP, HTTPS, TCP, etc., can be configured with the desired load balancer algorithm and health checks.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Add load balancer to edge**.

2 Click the green **Start Workflow** icon.

3 Enter the Common parameters:

   a Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

   b Enter the Edge ID.

   c Select whether or not to enable load balancer.

4 Click **Next**.

5 Enter the Pool information:

   a Enter a pool name.

   b Select the pool service profiles.

   c Select the pool members.

6 Click **Next**.

7 Enter the Virtual Server information:

   a Enter the virtual server name.

   b Enter the virtual server vNIC index.

   c Enter the virtual server IP address.

8 Click **Submit**.

Add NAT Rules

You can use this workflow to add Network Address Translation (NAT) rules to an NSX Edge.

NSX Edge provides NAT service to protect the IP address of internal (private) networks from the public network. You can configure NAT rules to provide access to services running on privately addressed virtual networks.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Add NAT rules**.
2. Click the **Start Workflow** icon.
3. Select the NSX endpoint:
   a. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
   b. Enter the Edge ID.
4. Click **Next**.
5. Set the NAT rules.
6. Click **Submit**.

Add Secondary IP Addresses to Edge vNIC

You can use this workflow to add secondary IP addresses to Edge vNICs (virtual network interfaces). These secondary IP addresses can be used for NAT or load balancer virtual servers (VIPs).

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Add secondary IP addresses to edge vNIC**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the Edge ID.
5. Enter the vNIC index.
6. Enter the list of IP addresses.
7. Click **Submit**.

Add Security Tags to Security Group

You can use this workflow to add security tags to a security group.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX Workflows > Add Security Tags to Security Group**.
2. Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select a Security Group object.

5 Select a Security Tags object.

6 Click **Submit**.

Add Static Routes

You can use this workflow to add static routes to an Edge.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Add static routes**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the Edge ID.

5 Set the static routes.

6 Click **Submit**.

Add VMs and IP Sets to Multiple Security Groups

You can use this workflow to add virtual machines (VMs) and IP Sets to multiple security groups. A security group is a collection of assets or grouping objects from your vSphere inventory.

Global and universal security groups are supported. However, for universal security groups, only universal IP Sets can be added as members. Similarly, for global security groups, global scope IP Sets are supported.

This workflow does best effort in maintaining a transactional behavior. In case any update to a security group fails, this workflow reverts previous security group updates and the workflow fails. However, there are chances that the roll back might fail. In such cases, you should sync with the latest security group memberships.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Add VMs and IP Sets to multiple security groups**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the security groups from the NSX inventory from the vRO inventory view.

4 Select the security groups. If not set, select the connection from the NSX inventory from the vRO inventory view.

5 (Optional) Select the security group IDs as an alternative to security group inventory objects.

   This field is ignored if security group objects are selected from the inventory.

6 Select the list of VMs.

7 Select the list of IP Sets. If not set, select the IP Set objects from the NSX inventory from the vRO inventory view.

8 (Optional) Select the IP Set IDs as an alternative to IP Set inventory objects.

   This field is ignored if IP Set objects are selected.

9 Click **Submit**.

Add VMs and IP Set to Security Group

You can use this workflow to add VMs and IP addresses to security groups.

For IPs, an IP set is created internally and the IP addresses specified in the workflow are added to the IP set. The IP set is added as a member of the security group.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Add VMs and IP set to security group**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the security group ID.

5 Enter or set the virtual machine managed object reference.

6 Enter or set the list of IP addresses.

7 Click **Submit**.

Add VMs to Existing Load Balancer Pools

You can use this workflow to add VMs to existing load balancer pools.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Add VMs to existing load balancer pools**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the Edge ID.

5 Enter the pool members.

6 Click **Submit**.

Add VMs to Security Group

You can use this workflow to add VMs to security groups.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Add VMs to security group**.

2 Click the green **Start Workflow** icon.

3 Select the NSX endpoint.

4 Enter the security group.

5 Enter the virtual machine managed object reference.

6 Click **Submit**.

Apply NAT Configuration

You can use this workflow to configure NAT on an NSX Edge. This workflow can be used to add new NAT rules or modify or delete existing NAT rules.

When adding NAT rules, rule ID is not specified. When modifying NAT rules, rule ID must be specified. For deleting NAT rules, action should be specified as delete.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Add NAT Configuration**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the NSX Edge.

5 Enter the NAT rule specification.

6 Click **Submit**.

Apply Security Policies on Security Group

You can use this workflow to apply multiple security policies on a security group.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Apply security policies on security group**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the security group ID.

5 Enter the security group policy IDs.

6 Click **Submit**.

Apply Security Policy on Security Group

You can use this workflow to apply a security group policy on a security group. A security policy is a collection of the following service configurations.

Service	Description	Applies to
Firewall rules	Rules that define the traffic to be allowed to, from or within the security group.	vNIC
Endpoint service	Data Security or third party solution provider services such as anti-virus or vulnerability management services.	virtual machines
Network introspection services	Services that monitor your network, such as IPS.	virtual machines

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Apply security policy on security group**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the security group ID.

5 Enter the security policy ID.

6 Click **Submit**.

Apply Security Tags on VM

You can use this workflow to apply security tags to a VM. Security tags are labels that can be applied to workflows to define certain characteristics and how the workflow is flagged and categorized.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Apply security tags on VM**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the security tag IDs.

5 Enter the virtual machine managed object reference.

6 Click **Submit**.

Configure Firewall Rules Between Interfaces

You can use this workflow to configure firewall rules between interfaces.

Specify the source, destination and action of the firewall rules. Other fields of the firewall tuple default to "any." Source and destination are typically Edge vNIC interfaces indices.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Configure firewall rules between interfaces**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the Edge ID.

5 Enter the firewall rules, specifying the source, destination and action.

6 Click **Submit**.

Connect Logical Switch to Router

You can use this workflow to connect a logical switch to a router.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Connect logical switch to router**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the virtual router ID.

5 Enter the logical switch ID.

6 Enter the IP address to be assigned to the router interface.

7 Enter the subnet mask.

8 Enter the index of the router interface to connect to.

9 Enter the type of interface (internal or uplink).

10 Click **Submit**.

Create Edge

You can use this workflow to create an NSX Edge. An NSX Edge provides routing services and connectivity to networks that are external to the NSX deployment.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Create Edge**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the Edge name.
5. Enter a description of the Edge.
6. Enter the datacenter ID.
7. Enter the tenant.
8. Enter the Edge vNICs, specifying the NIC index, portgroup and IP address specification.
9. Enter the Edge appliances, specifying the placement parameters of resource pool, datastore and host.
10. Click **Submit**.

Create IP Set

You can use this workflow to create an IP Set grouping object in NSX. An IP Set is a group of individual IP addresses, IP ranges and subnets used as sources and destination in firewall rules.

This workflow can be used to create a set of IP addresses, IP ranges and CIDR blocks. IP Sets can contain any combination of individual IP addresses, IP ranges and/or subnets to be used as sources and destinations for firewall rules or as members of Security groups.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Create IP Set**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the name of the IP set.
5. Enter a description of the IP set.
6. Enter the list of IP addresses, IP ranges and CIDR blocks, separated by commas.
7. Choose whether you want to create a universal IP set.
8. Click **Submit**.

Create Logical Switch

You can use this workflow to create a logical switch. An NSX logical switch creates logical broadcast domains or segments to which an application or tenant virtual machine can be logically wired.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Create logical switch**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the transport zone ID.
5. Enter the logical switch name.
6. Enter a description of the logical switch.
7. Enter the tenant ID.
8. Click **Submit**.

Create Security Group

You can use this workflow to create a security group with VMs and IP Sets (optional) as members. A security group is a collection of assets or grouping objects from your vSphere inventory.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Create security group**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the security group name.
5. Enter a description of the security group.
6. Enter the virtual machine managed object references.
7. Enter the IP Sets.
8. Choose whether you want to create a universal security group.
9. Click **Submit**.

Delete Edge

You can use this workflow to delete an Edge.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Delete edge**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the Edge ID.
5. Click **Submit**.

Delete IP Set

You can use this workflow to delete an IP Set in NSX.

With a forced delete, the object is deleted even if used in other places, such as firewall rules, causing invalid referrals. For an unforced delete, the object is deleted only if it is not used by other configurations. Otherwise, the delete fails.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Delete IP Set**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the IP set.
5. Choose whether you want to force delete the IP set.
6. Click **Submit**.

Delete Logical Switch

You can use this workflow to delete a logical switch.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Delete logical switch**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the logical switch ID.
5. Click **Submit**.

Delete NAT Rules

You can use this workflow to delete NAT rules.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Delete NAT rules**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the Edge ID.
5. Enter the NAT rule IDs.
6. Click **Submit**.

Delete Security Group

You can use this workflow to delete a security group.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Delete security group**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the security group ID.
5. Click **Submit**.

Delete Security Tags from Security Group

You can use this workflow to delete security tags from a security group.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX Workflows > Delect Security Tags from Security Group**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select a Security Group object.
5. Select a Security Tags object.

Delete Static Routes from Edge

You can use this workflow to delete static routes from an Edge.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Delete static routes from Edge**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the Edge ID.
5. Enter the static routes to delete.
6. Click **Submit**.

Detach Security Tags from a VM

You can use this workflow to detach security tags from a VM.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Detach security tags from VM**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the security tags to detach.
5. Enter the virtual machine managed object reference.
6. Click **Submit**.

Disconnect Router Interface

You can use this workflow to disconnect a router interface.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Disconnect router interface**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the router ID.

5 Enter the index of the router interface to disconnect.

6 Click **Submit**.

Get Edge by ID

You can use this workflow to retrieve an NSX Edge object using its ID.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Get Edge by ID**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the ID of the Edge to retrieve.

5 Click **Submit**.

Get IP Set

You can use this workflow to retrieve an IP Set from inventory.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Get IP Set**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Select the IP Set to retrieve.

5 Click **Submit**.

Get IP Set by ID

You can use this workflow to retrieve an IP Set using its ID.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Get IP Set by ID**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the ID of the IP Set to retrieve.

5 Click **Submit**.

Get Members of Security Group

You can use this workflow to retrieve members of a security group.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Get members of security group**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the security group object for which you want to retrieve members.
5. Click **Submit**.

Get Members of Security Tag

You can use this workflow to retrieve members of a security tag.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Get members of security tag**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the security tag object from which you want to retrieve members.
5. Click **Submit**.

Get NAT Rules

You can use this workflow to retrieve rules configured on a specific Edge.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Get NAT rules**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the NSX Edge object.
5. Click **Submit**.

Get Security Tag by ID

You can use this workflow to retrieve the security tag object using the security tag ID.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Get security tag by ID**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the ID of the security tag.
5. Click **Submit**.

Modify IP Set

You can use this workflow to modify an IP Set.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Modify IP Set**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the IP set object.
5. Enter the name of the IP set.
6. Enter a description of the IP set.
7. Enter the list of IP addresses, IP ranges and CIDR blocks, separated by commas.
8. Click **Submit**.

Remove Secondary IP Addresses Assigned to Edge vNIC

You can use this workflow to remove secondary IP addresses assigned to an Edge vNIC.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Remove secondary IP addresses assigned to Edge vNIC**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the Edge ID.

5 Enter the vNIC index.

6 Enter the list of IP addresses to remove.

7 Click **Submit**.

Remove VMs and IP Sets from Multiple Security Groups

You can use this workflow to remove VMs and IP sets from multiple security groups. Global and universal security groups are supported.

This workflow does best effort in maintaining a transactional behavior. In case any update to a security group fails, this workflow reverts to previous security group updates and the workflow fails. However, there are changes that the roll back might fail. In such cases, you should synchronize with the latest security group memberships.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Remove VMs and IP sets from multiple security groups**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Select the security groups. If not set, select the security group from the NSX inventory from the vRO inventory view.
5. (Optional) Select the security group IDs as an alternative to security group inventory objects.

   This field is ignored if security group objects are selected from the inventory.
6. Select the list of VMs.
7. Select the list of IP sets. If not set, select the IP Sets from the NSX inventory from the vRO inventory view.
8. (Optional) Select the IPSet IDs as an alternative to IPSet inventory objects.

   This field is ignored if IP set objects are selected.
9. Click **Submit**.

Remove VMs and Load Balancer Pools

You can use this workflow to remove VMs from load balancer pools.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Remove VMs from load balancer pools**.
2. Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the Edge ID.

5 Enter the Pool IDs.

6 Enter the members of the pool to remove.

7 Click **Submit**.

Set Default Route

You can use this workflow to add a default route to an Edge.

Procedure

1 Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows > Set default route**.

2 Click the green **Start Workflow** icon.

3 Select the NSX Connection object (NSX endpoint). If not set, select the connection from the NSX inventory from the vRO inventory view.

4 Enter the Edge ID.

5 Enter the vNIC index for the default route.

6 Enter the Gateway IP address for the default route.

7 Click **Submit**.

NSX Workflows for vCAC

7

The NSX workflows for vCAC are used to create and manage security policies. You can access these workflows from **Library > NSX > NSX Workflows for VCAC** on the Workflows view in the Orchestrator client. You can run the workflows from the Run and Design modes.

Note This workflow folder is called NSX Workflows for vCAC (vCloud Automation Center) for backward compatibility. vCAC has been renamed vRealize Automation (vRA).

This chapter includes the following topics:

Create App Isolation Security Policy

You can run this workflow to create an app isolation security policy. An NSX app isolation security policy acts as a firewall to block all inbound and outbound traffic to and from the provisioned machines in the deployment.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows for VCAC > Create app isolation security policy**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Endpoint - NSX Connection object. If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Enter the ID of the NSX endpoint returned by the Create NSX endpoint workflow.
5. Click **Submit**.

Enable Security Policy Support for Overlapping Subnets

You can run this workflow to enable enforcement of firewall rules defined in security policies only on the members of the security group to which the security policy is applied. Running this workflow is a prerequisite for supporting overlapping subnets when consuming service composer/security policy features from vRealize Automation.

Procedure

1. Click the **Workflows** tab and then navigate to **Library > NSX > NSX workflows for VCAC > Enable security policy support for overlapping subnets**.
2. Click the green **Start Workflow** icon.
3. Select the NSX Endpoint - NSX Connection object. If not set, select the connection from the NSX inventory from the vRO inventory view.
4. Click **Submit**.