SmartFabric Services for OpenManage Network Integration User Guide

Release 1.3

August 2020
Rev. A01

DELL EMC

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

SmartFabric vCenter

Enterprises are adopting the power of automation to transform their IT operations, and enable a more agile and responsive infrastructure in their data center. Network operators must leverage the power of automation within and across their departmental functions, delivering integrated solutions which cater to cloud-based consumption models.

SmartFabric Services

SmartFabric Services (SFS) are an automation framework that is built into the Dell EMC SmartFabric OS10, to integrate converged and hyperconverged infrastructure systems. These solutions deliver autonomous fabric deployment, expansion, and life cycle management.

SFS enables converged infrastructure (CI) and hyperconverged infrastructure (HCI) for system administrators to deploy and operate the network fabric for the infrastructure solution as an extension of the solution being deployed. This integrated network fabric is built using industry-standard protocols adhering to the best practice recommendations for that solution, and is interoperable with customers existing data center networks.

OpenManage Network Integration

Dell EMC OpenManage Network Integration (OMNI) is a management application that is designed to complement SFS, providing a web-based GUI for operating one or more automated network fabrics deployed using SFS (called SmartFabric instances).

OMNI is delivered as a virtual appliance which can be deployed as:

- A stand-alone virtual machine enabling a web portal to manage one or more SmartFabric Instances
- Deployed as an external plug-in for VMware vCenter. OMNI when deployed as a plug-in for VMware vCenter enables:
  - Enables zero-touch automation of physical underlay network fabric running SFS corresponding to changes in the virtual network layer
  - Extends vCenter Host Network Inventory data to include physical switch connectivity details for easy monitoring and troubleshooting
  - Enables single pane of management for one or more SmartFabric instances through the OMNI portal pages that are embedded within vCenter

VxRail SFS integration solution

Dell EMC VxRail integrated with SFS automates and simplifies networking for VxRail hyperconverged infrastructure deployments and ongoing network operations. As hyperconverged domains scale, the network fabric becomes the critical piece of successful deployment. VxRail integration with SFS allows customers to deploy network fabrics for VxRail clusters as an extension of the VxRail clusters without extensive networking knowledge. The network fabric is automatically configured for the VxRail nodes as the operators deploy their VxRail clusters.

Key benefits

- Faster time to production
  - Plug and play fabric formation for VxRail.
  - VxRail Manager automatically creates fabric policies for VxRail nodes.
  - SmartFabric to automate all fabric functions.
- Integrated life cycle
  - Fabric creation, expansion, and maintenance follow the VxRail application model.
  - HCI fabric operations are fully managed through VxRail Manager or vCenter.
- Better infrastructure visibility
  - Tight integration between VxRail appliance and Dell EMC ON-Series PowerSwitches.

- Fabric connectivity extended to PowerSwitches required for VxRail solutions only.
- Improved SLA
  - Fully validated software stack recommendation.
  - Protection from human-error due to predictable and repeatable HCI fabric experience.
- Enhanced support experience
  - World-class Dell EMC HCI and fabric services.
  - Fabric that is integrated into VxRail services and support experience.

Required components

- Dell EMC PowerSwitches supporting SmartFabric Services
  - **Leaf/ToR switches**: 10 GbE—S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON; 25 GbE—S5212F-ON, S5224F-ON, S5248F-ON, and S5296F-ON
  - **Spine switches**: S5232F-ON and Z9264F-ON
- Dell EMC SmartFabric OS10 for PowerSwitch models.
- Dell EMC OpenManage Network Integration (OMNI).
- Dell EMC VxRail hyperconverged nodes when deploying VxRail integrated solution.
- VMware vCenter internal to VxRail cluster or existing vCenter in customer environment.

See the *Dell EMC VxRail Support Matrix* for the latest software releases that support the VxRail SmartFabric Service integrated solution.

More resources

List of more resources you may need:

Table 1. More resources

Path and Links to Documents	Description
Dell EMC Networking OS10 Info Hub > **OS10 User Guides** > **OS10 Dell EMC SmartFabric OS10 User Guide, 10.5.0**	This document contains information to help you understand, configure, and troubleshoot your OS10 networking operating system.
Dell Technologies VxRail Networking Infohub > **Guides**	This page contains reference documents to configuration, deployment, and other guides for VxRail networking solutions.
Support Matrix > **Solutions and SmartFabric Services Validated Versions**	This page contains the various support matrices of SmartFabric OS10 solutions including VxRail, PowerStore, Isilon front-end, PowerEdge ESXi, vSAN Ready Nodes, and PowerEdge MX.
Dell EMC Networking SmartFabric Services Deployment with VxRail	This guide demonstrates the deployment of a leaf-spine fabric using SmartFabric Services and shows how SmartFabric Services simplifies the deployment of a new VxRail cluster.
Dell EMC OpenManage Network Integration for VMware vCenter > **Manuals and documents**	This page lists the OMNI reference manuals from previous versions.

2

SmartFabric Services

SFS offers plug and play data center network fabric deployment, expansion, and management of Dell EMC infrastructure as turnkey solutions. SFS is a component of SmartFabric OS10 network operating system that provides the framework to automatically deploy the network as a single logical entity which enables the integration of Dell EMC infrastructure solutions.

SFS offers turnkey network solution for data center infrastructure using Dell EMC PowerEdge modular system switches (PowerEdge MX), and PowerSwitch data center switches.

This information provides an overview of the SFS solution that is built on an automated data center leaf and spine network fabric using Dell EMC PowerSwitch models.

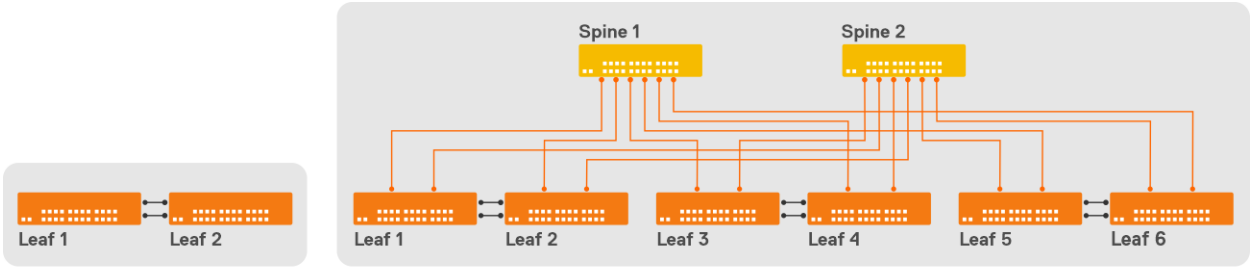
For complete information about SFS for PowerEdge MX fabric, see *Dell EMC PowerEdge MX SmartFabric Configuration and Troubleshooting Guide*.

SFS for data center leaf and spine fabrics

SFS is built on top of modern leaf and spine data center design that is optimized for the increased east-west traffic requirements of modern data center workloads. The entire leaf and spine network fabric is orchestrated and managed as a single object, eliminating the need for box-by-box configuration and management of the switches.

The fabric can start from a single rack deployment with two leaf/top-of-rack (ToR) switches, and expanded to a multi rack leaf and spine network fabric. The fabric is automatically built and expanded using industry-standard Layer 2 and Layer 3 protocols as new switches are connected.

L3 fabric profile



Single Rack Fabric

Multi Rack Fabric

NOTE: SmartFabric Services can be enabled when there are at least two leaf/ToR switches connected as a VLT pair.

SFS initial setup

When PowerSwitch models with SmartFabric OS10 power on, the switches are operating in the normal Full Switch mode. This information explains how to start the automated discovery and fabric creation process.

1. Log in to each switch console.
2. Configure the out-of-band Management IP address.
3. Upgrade SmartFabric OS10 to supported versions based on the *Dell EMC VxRail Support Matrix*.
4. Enable SmartFabric Services on the switches.

For complete information about configuring the out-of-band Management IP address and upgrading the switch operating system, see *Dell EMC SmartFabric OS10 User Guide, Release 10.5.0*.

Enable SFS

This information describes how to enable SmartFabric Services. To enable SFS on a switch from the SmartFabric OS10 command-line interface (CLI), use `smartfabric l3fabric enable` command and set a role. In SmartFabric mode, the two leaf or ToR switches are automatically configured as a VLT pair, and the VLT interconnect link (ICL) ports must be physically connected before enabling SFS.

NOTE: The VLTi ports (ICL ports) cannot be modified once SFS is enabled. It is recommended to select the required number of ports upfront. SFS must be disabled and reenabled again to change the VLTi ports which can result in service interruption.

Once you enable SFS on switches and set a role, the network operating system prompts for configuration to reload, then boots in SFS Fabric mode. To apply the changes, enter Yes to confirm and the switch reloads in Fabric mode. The switch is then placed in Fabric mode, and the CLI is restricted to global switch management features and monitoring. SFS Master controls all network configuration for interfaces and switching or routing functions.

Use these SmartFabric OS10 CLI commands to build a leaf and spine fabric:

- On leaf switches:

  ```
  Leaf1(config)# smartfabric l3fabric enable role LEAF vlti icl_ports
  ```

  Example:

  ```
  Leaf1(config)# smartfabric l3fabric enable role LEAF vlti ethernet 1/1/1-1/1/5
  ```

- On spine switches

  ```
  Spine1(config)# smartfabric l3fabric enable role SPINE
  ```

For complete information about how to use SFS commands, see *SmartFabric commands* in the *Dell EMC SmartFabric OS10 User Guide, Release 10.5.0*.

SFS Graphical User Interface

You can also enable SFS using the SFS Graphical User Interface (GUI). OS10 switches support SFS GUI to set up initial SFS configuration in SFS leaf and spine deployment. The SFS GUI is focused on day zero deployment operations and management of the switches in a Layer 3 SFS fabric. For more information about the SFS and SFS GUI, see SmartFabric Services in the *Dell EMC SmartFabric OS10 User Guide, Release 10.5.0*.

Fabric creation

This information describes switch discovery, SFS Master, Master advertisement, SFS REST services, Master high availability, preferred Master, SmartFabric, rack or VLT fabrics, default fabric settings, reserved VLANs, default client management network, default client control traffic network, and spanning-tree protocol.

Switch discovery

When SFS is enabled on PowerSwitches, the switches boot in Fabric mode, then start discovering each other using LLDP. All discovered switches become part of a single SFS domain, to form a single network domain.

NOTE: For L3 fabric profile, the SFS `Domain ID` is automatically set to 100 and is not configurable in the current release. All directly connected switches join one single domain.

The port where another leaf switch is discovered is configured as a VLT interconnect link (ICL), and the port where another spine switch is discovered is configured as an interswitch link (ISL). A switch operating as a spine can only have ISL links to other leaf switches.

SFS uses reserved VLAN 4000 internally to establish communication between switches in a single network fabric. VLAN 4000 is automatically added to all ICL and ISL ports.

SFS Master

SFS uses Keepalive protocol, running on VLAN 4000, to elect one in the fabric as a Master switch. Only a leaf switch can be elected as a Master.

In a single SFS domain, there is only one Master switch at any given time, and the rest of the leaf switches are designated as the backup. A new Master is elected from the backup switches when the Master fails to provide high-availability to the fabric.

NOTE: Spine switches cannot be elected as a Master node within SFS.

Master advertisement

Once a Master is elected, it initiates all applications to automatically build the network fabric. The Master VIP is advertised using mDNS Avahi services for applications to automatically discover the fabric through inband networks.

SFS REST services

The SFS REST service is started on the Master node. Applications consuming or integrating with SFS use this REST service for fabric operations. Communication is performed with the fabric using the IPv6 VIP assigned to the SFS Master, or using the IPv4 out-of-band Management IP of the Master.

A default REST_USER account is created to authenticate all REST queries. The default password is `admin`, and Dell EMC recommends changing the password through VxRail Manager or OMNI.

NOTE: OMNI communicates with SmartFabric REST Services through REST_USER account only.

Master high availability

SFS uses an internal distributed data store where all fabric configuration is saved. This data is synchronized with all backup switches ensuring the Master, and the backup switches always have the same view of the fabric. With a Master failover, the switch taking over as the Master uses its internal data store to continue fabric operations.

When the fabric is expanded, the newly added switches receive all fabric policies from the SFS Master, once the switches are added to the domain.

Preferred Master

When a Master is elected for a fabric, the switches that are configured as Preferred Master have a higher priority to become the Master switch. If none of the switches are configured as the Preferred Master, any leaf switch can become the Master.

When the fabric is expanded, newly added switches may come up and form a fabric among themselves, and elect a Master before they are connected to the existing fabric. When the new fabric merges with the existing fabric, SmartFabric elects a new Master switch for the combined fabric. If one of the new leaf switches becomes the master, it may overwrite the configuration in the existing fabric. Ensure that the leaf nodes in the existing fabric are set as the Preferred Master before expanding the fabric to prevent the configuration loss.

NOTE: VxRail workflow automatically sets the preferred master during uplink creation as part of Day1 operation. The SFS UI or OMNI checks for the preferred master settings during uplink creation and sets Preferred Master flag automatically on all configured leaf switches in the fabric if not configured already.

SmartFabric or SFS domain

SmartFabric or SFS domain is interchangeable terminology, and the fabric consists of all switches directly connected to form a single logical network. The L3 fabric is automatically assigned ID 100 and this ID cannot be changed. The fabric name and description are automatically assigned, but can be changed through the SFS user interface.

Rack or VLT fabrics

When two leaf switches are discovered on specified VLTi ports, a VLT is automatically created between the two switches to form a network fabric called the VLT fabric. This VLT fabric is automatically assigned with a fabric ID, a universally unique identifier (UUID).

In a single rack deployment, the network fabric and the VLT fabric represent the same set of switches. In a multi rack deployment, each rack has a VLT fabric, and all the VLT fabrics and the spine switches together form the network fabric.

Default fabric settings

SFS automatically builds the network fabric using industry-standard Layer 2 and Layer 3 protocols.

Reserved VLANs

To build fabric, SFS reserves VLANs 4000 to 4094 for internal use. You are not allowed to use these VLANs for general use.

- **VLAN 4000 — SFS control VLAN** SFS automatically configures VLAN 4000 on all switches that are discovered in the fabric, and uses it for all fabric operations internally. When a leaf or spine is switch is discovered, the ICL or ISL ports are automatically added as tagged members.
- **VLAN 4001 to 4079 — leaf and spine connections** SFS automatically sets up the leaf and spine network configuration using eBGP as the underlay routing protocol. SFS uses the reserved VLAN range (4001 to 4079) with automatic IP addressing to set up the peer connections. When a spine switch is connected to the fabric, an ISL is created between the leaf and spine switch. Each ISL link uses a reserved VLAN and the ISL ports that are configured to be the untagged members of this VLAN. IP addresses from the reserved range are used for this VLAN, and an eBGP session is started on the VLAN IP interface.
- **VLAN 4080 — global untagged VxLAN VLAN** SFS automatically sets up VXLAN overlay networks with EVPN to extend networks between racks in a multi rack deployment. SmartFabric OS10 requires an untagged VLAN on leaf switches for VXLAN traffic handling when using VLT. VLAN 4080 with automatic IP addresses from the reserved range is used for leaf-to-leaf interconnect (ICL) links.
- **VLAN 4090 — iBGP peering between leaf switches** SFS automatically sets up iBGP peering between a pair of leaf switches directly connected over ICL links. VLAN 4090 with automatic IP addresses from the reserved range is used for enabling iBGP sessions between the VLT peer switches.
- **VLAN 4094 — VLT control VLAN** SFS automatically creates VLAN 4094 on all leaf switches. VLAN 4094 is used for all VLT control traffic between two VLT peer switches. VLAN 4094 is only added on the VLT interconnect links (ICL ports) on leaf switches.
- **VLAN 4089 — OS10 internal use** In SmartFabric mode, VLAN 4089 is the default VLAN and is reserved for OS10 internal use.

Default client management network

SFS automatically sets up an overlay network that is called a *client management network*. When a device is automatically onboarded on to the network fabric, the device uses the VLAN mapped to this overlay network. This network is a native VLAN unless there is a policy specifying a different native VLAN. VLAN 4091 is used as the default client management VLAN for this VXLAN network.

NOTE: The embedded SFS user interface allows you to change this VLAN to a specified VLAN.

Default client control traffic network

SFS sets up a second overlay network that is called *client control network* specifically for VxRail integrated solutions. When a VxRail node is discovered, it is automatically added as a tagged member of this network. SFS also enables the mDNS Avahi service on this network for master advertisement and fabric discovery by integrated solutions. The SFS Master virtual IP for VXLAN network is advertised. The VIP address is `fde1:53ba:e9a0:cccc:0:5eff:fe00:1100` is fixed and not user configurable.

VLAN 3939 is used as the default client control VLAN for this VxLAN network. Although you can change the VLAN associated with this, it is not recommended to change it for VxRail integrated solution deployments.

Spanning-tree protocol

SFS uses RPVST+ as the default spanning tree protocol to build leaf and spine switches.

Spanning-tree protocol is disabled for VXLAN networks. SFS automatically creates user networks as VXLAN networks inside the fabric. For a Layer 2 uplink from the fabric to the external network, the uplink ports in the fabric are configured as VXLAN access interfaces and spanning-tree BPDUs are not sent to the external network.

SFS support for MSTP on L3 fabric: By default, the STP mode is RPVST+. You can change the mode to MSTP once the fabric is built. When you change the mode, the whole fabric goes through a reboot cycle and the new mode will be set as MSTP.

NOTE: Changing the mode impacts traffic in the SFS as fabric reboots.

The spanning tree behavior for Layer3 fabric is as follows:

- STP is enabled on Cluster control VLAN (VLAN 4000). The spine switches are configured to take over the STP root role.
- STP is disabled on all inter leaf-spine VLANs and leaf-leaf VLAN (4001-4091).
- STP is enabled on all user created VLANs.
- STP is disabled on server facing port.

NOTE: VLANs used for setting up the leaf and spine eBGP peering are automatically set up to prevent loops while having nonblocking connections between the leaf and spine switches.

SFS and OMNI supported solutions

OMNI 1.3 with the latest SmartFabric Services OS10 release supports the following qualified solutions:

Table 2. Qualified solutions

Qualified Solutions	Dynamic discovery	Onboarding type	vCenter/Day 2 automation
VxRail	Yes	Automatic	Yes
PowerStore X (ESXi)	Yes	Import from Fabric or vCenter	Yes
PowerStore T	Yes	Import from Fabric	No
Isilon front-end/PowerScale	No	Manual	No
Other devices running ESXi	No	Import from vCenter or Manual	Yes
Other devices running Windows or Linux-based Operating Systems	No	Manual	No

NOTE: Other devices can be supported provided they meet the industry Ethernet standards and are compatible with SmartFabric-enabled switches.

Dynamic Discovery - Devices that support dynamic discovery send a Dell-specific LLDP TLV. Supported devices are automatically populated in the SFS GUI and OMNI by MAC address, switch, and switch port number for onboarding to the fabric. Devices that do not send the Dell-specific LLDP TLV must be manually added to the fabric.

Onboarding - Onboarding is the process of adding devices to the fabric through the creation of server interface profiles. For VxRail, the SFS and VxRail Manager automates the onboarding process. PowerStore systems support dynamic discovery and may be onboarded using the **Import from Fabric** option in OMNI, see Import SmartFabric discovered server interfaces. Hosts running ESXi may be onboarded using the **Import from vCenter** option in OMNI only if the hosts are already connected to vCenter. For more information, see Import ESXi host profiles from vCenter. Other devices are manually onboarded by specifying the switch and switch port number for each interface, see Create server interface profile.

vCenter/Day 2 Automation - Port groups that are created in vCenter are automatically applied to the applicable host-connected ports on the switch. The host must be running ESXi, added to the vCenter, and have a server profile that is created in OMNI. For the automation to work, register OMNI with the vCenter and ensure to start the respective OMNI vCenter automation services.

NOTE: See the Solutions Support Matrix for the latest supported versions for all the qualified solutions.

SFS integrated personalities

This information describes the two SFS integrated personalities.

- **SFS VxRail L2 single rack personality** — enables an automated single rack network fabric (L2 fabric profile) for VxRail clusters. Use the L2 personality for the existing fabric deployments. For more information about configuring VxRail L2 single rack personality, see *VMware Integration for VxRail Fabric Automation SmartFabric User Guide, Release 1.1, September 2019*. For new SmartFabric deployments, it is recommended to use the L3 leaf and spine fabric personality for future expansion.
- **SFS L3 leaf and spine fabric personality** — enables a multi rack data center network fabric offering flexibility to start with a L3 single rack (L3 fabric profile), and expand to a multi rack solution on demand. The L3 personality is integrated with VxRail to enable single-site, multi rack VxRail deployments allowing VxRail nodes to be easily deployed in any rack without complex underlay network configuration.

OpenManage Network Integration (OMNI) enables fabric management and zero-touch automation for:

- SFS L3 leaf and spine fabric personality
- SFS VxRail L2 single rack personality

Table 3. SFS personality comparison

SFS VxRail L2 single rack personality	SFS L3 leaf and spine fabric personality
Network fabric with two ToR switches in a single rack, and cannot be expanded beyond a single rack.	Network fabric with up to 20 switches in a leaf and spine design that can start with a single rack, and extend up to nine racks. If you want to deploy a L3 single rack fabric, enable only leaf switches in the rack without spine. Add spine to the L3 single rack to form a L3 multi rack leaf and spine fabric.
All VxRail SmartFabric deployments prior to SmartFabric OS10 10.5.0.5.	All new SmartFabric deployments with SmartFabric OS10 10.5.0.5 or later.
Enabled through shell commands with fixed parameters.	Enabled through standard SmartFabric OS10 CLI commands with just role and VLTi ports for leaf as fixed parameters. Enable SFS using SmartFabric GUI also. For more information about SFS GUI, see *Dell EMC SmartFabric OS10 User Guide*.
Default uplink and jump box port that is created as part of SmartFabric initialization, and cannot be modified after enabling SFS as part of Day 2 operations.	The network fabric is created as part of SmartFabric initialization. Uplinks and jump box port must be created through the embedded SFS user interface or OMNI. These are fully customizable as part of Day 2 operations.
All networks created during initialization, VxRail deployment and Day 2 operations are VLAN backed network with customer router acting as the gateway.	Networks that are created during initialization and the ones created as part of VxRail deployment and vCenter integration are VxLAN stretched networks for single rack deployments. VLAN-based netwoks in a rack can be created through OMNI.
Existing deployments when upgraded to SmartFabric OS10 10.5.0.5 continue to run in L2 mode. L3 fabric capabilities are not available.	Migration from VxRail L2 personality to L3 fabric personality is not available with SmartFabric OS10 10.5.0.5, and will be available in a future release.

NOTE: We recommend that all new deployments be enabled with L3 leaf and spine fabric personality. VxRail SmartFabric deployments using older VxRail L2 single rack personality cannot be upgraded to the new L3 leaf and spine fabric personality automatically. A migration workflow will be available in a future release to allow existing deployments to expand to a multi rack solution.

3

OpenManage Network Integration

OpenManage Network Integration (OMNI) is a component of SmartFabric Services (SFS) that integrates with VMware vCenter for fabric automation of the physical network infrastructure corresponding to the virtual network operations within vCenter. OMNI also serves as a front-end management application for managing one or more SFS instances, enabling administrators to manage and operate one or more network fabrics that are deployed with SFS.

OMNI virtual appliance

The OMNI virtual appliance is delivered as an open virtual appliance (.ova extension) file. Deploying an OMNI OVA template allows you to add preconfigured OMNI virtual machines to vCenter Server or ESXi inventory.

The OMNI OVA file can be downloaded from the Dell EMC OMNI for VMware vCenter support portal. OMNI virtual machine deployment is tested and supported only on the VMware ESXi hypervisor, even though it is expected that the OVA could be deployed in other x86 hypervisors.

OMNI deployment

Deploying an OVA template is similar to deploying a virtual machine from a template. You can deploy an OVA template from any local file system accessible from the vSphere web client, or from a remote web server.

Table 4. OMNI deployment

OMNI VM system requirements	vCenter Server Network (OMNI VM Network 1 - ens160)	VxRail Management Network (OMNI VM Network 2 - ens192) *Optional in non-VxRail deployment*	OMNI access
• Virtual hardware version: vmx-14 • Compatible: ESXi 6.7 and later • 4 virtual CPUs; 4 GB memory; 40 GB hard disk	Out-of-band (OOB) management network • Provides reachability to DNS, default gateway, and where OMNI obtains the IP/hostname • Provides reachability to Management network (vCenter IP/hostname, SmartFabric Management IP/hostname)	In-band link-local network—Provides reachability to SmartFabric link-local network for IPv6 VIP reachability	• vCenter HTML5 (/ui) plug-in; click OpenManage Network Integration link • OMNI stand-alone user interface: https://*OMNI_IP or hostname*/delawareos10/ using `admin` user • SSH to OMNI VM IP/hostname as `admin` user • OMNI VM console using vCenter/ESXi `admin` or `root` user
	VxRail default: vCenter Server network	VxRail default: VxRail Management network	

NOTE: Even when OMNI is deployed in-band, it is recommended to set up connectivity with the out-of-band Management network of the switches in the network fabric to separate management traffic with user data traffic, and also to enable faster image downloads to the switches.

Create OMNI virtual appliance

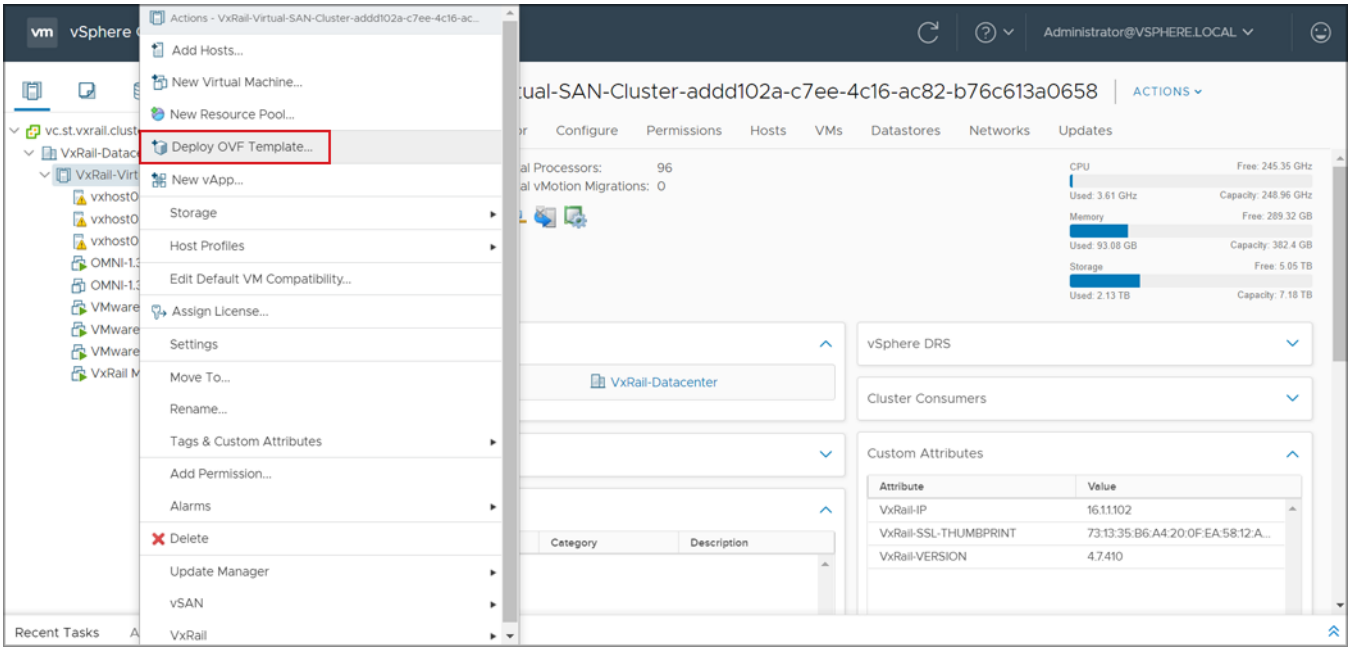
This information describes how to deploy the OMNI appliance on a VMware ESXi hypervisor using the OMNI OVA file, and create a virtual machine (VM).

NOTE: The OMNI portal or SmartFabric Services user interface does not provide localization.

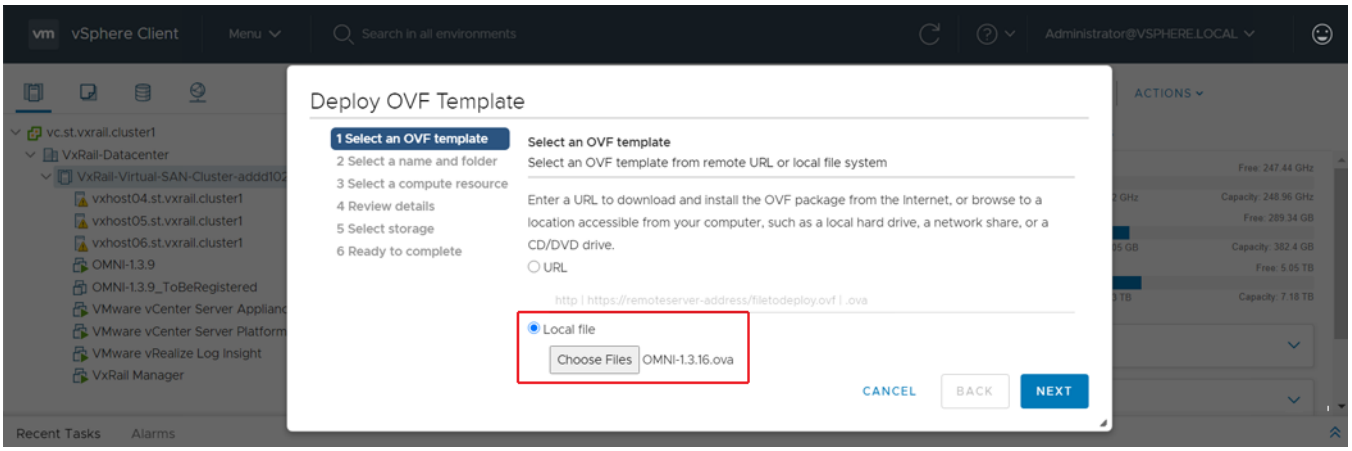
When upgrading from older major version to 1.3, follow the instructions for upgrading major version that is provided in Upgrade OMNI appliance.

Download and install OVA

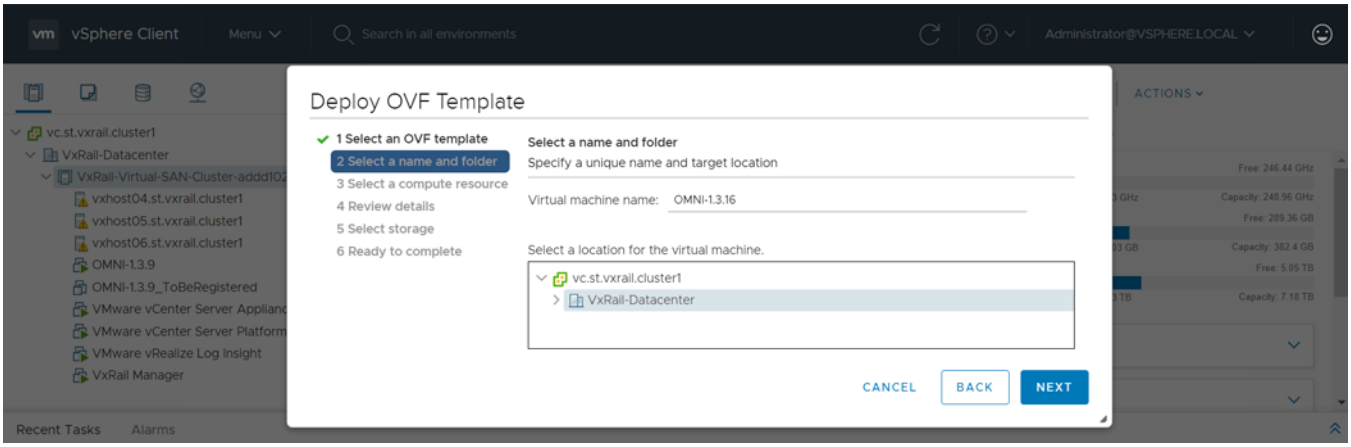
1. Download the OVA from OpenManage Network Integration support, and store the OVA image locally.
2. In the vSphere Client, select **Hosts and Clusters**, right-click the cluster that the plug-in must manage, and select **Deploy OVF Template**.



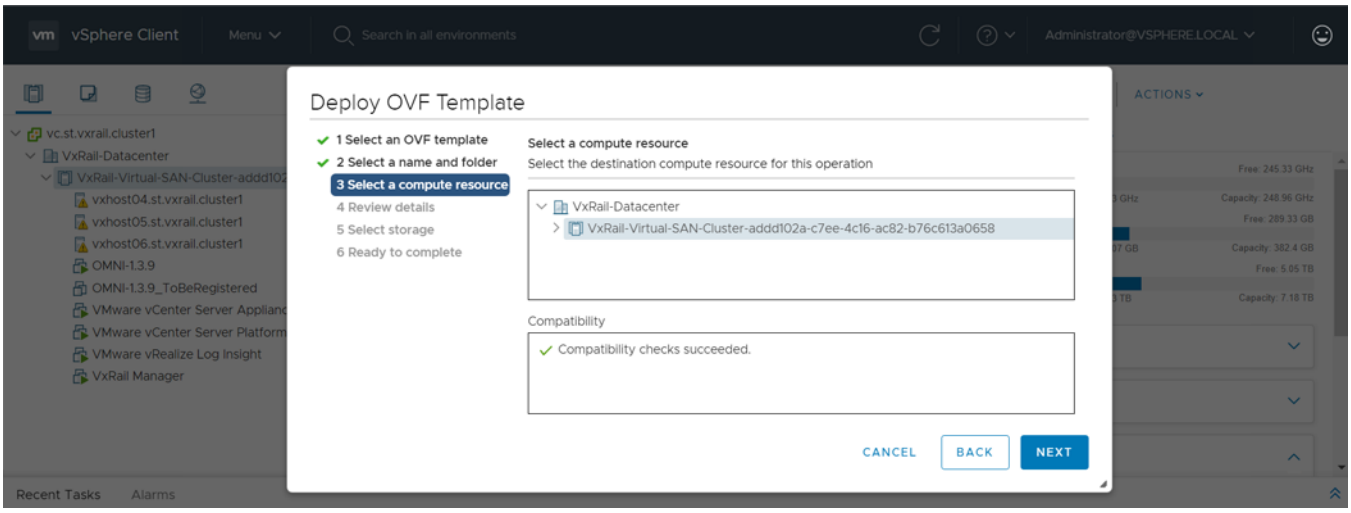
3. Select **Local file**, click **Choose Files**, select the OMNI ova file from a local source, and click **Next**.



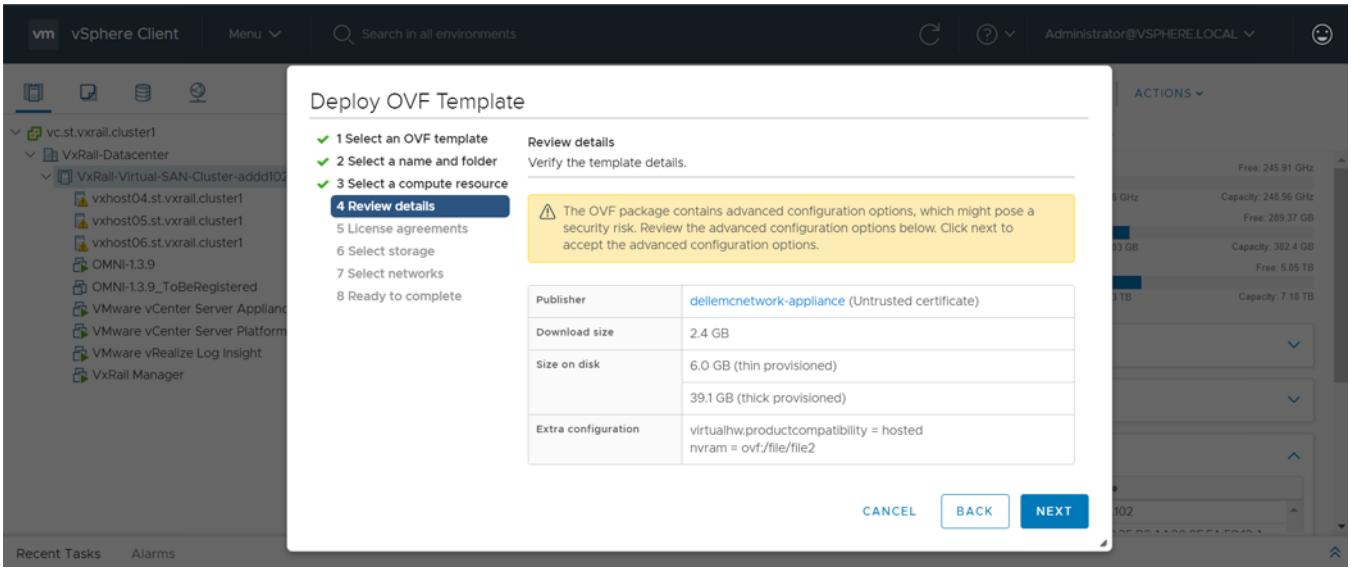
4. Select a name and folder for the VM, and click **Next**.



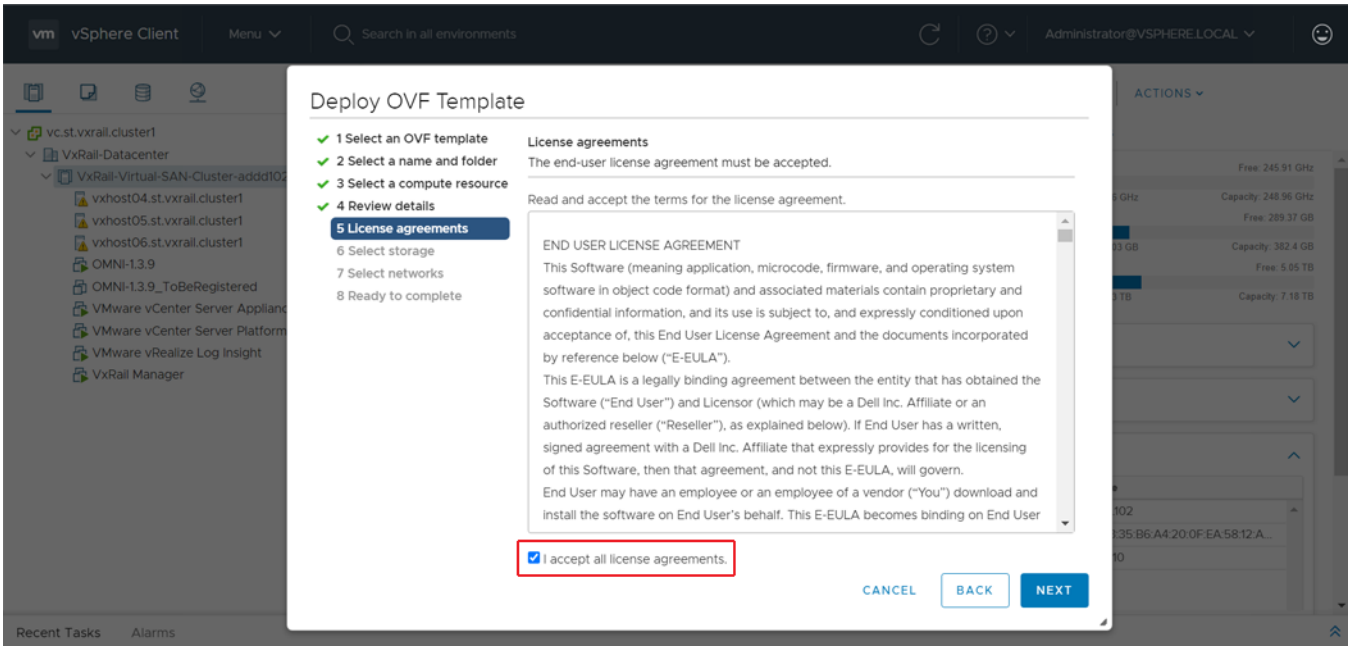
5. Select the destination compute resource, and click **Next**.



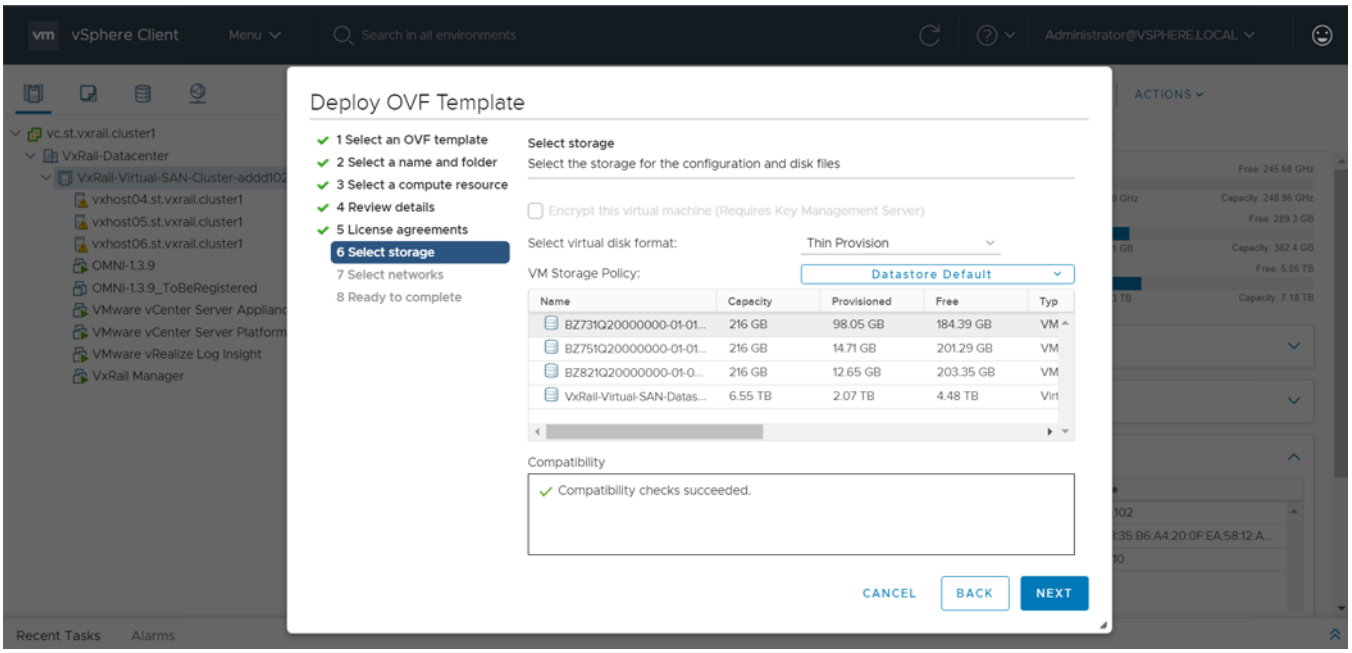
6. Review and verify the template details, and click **Next**.



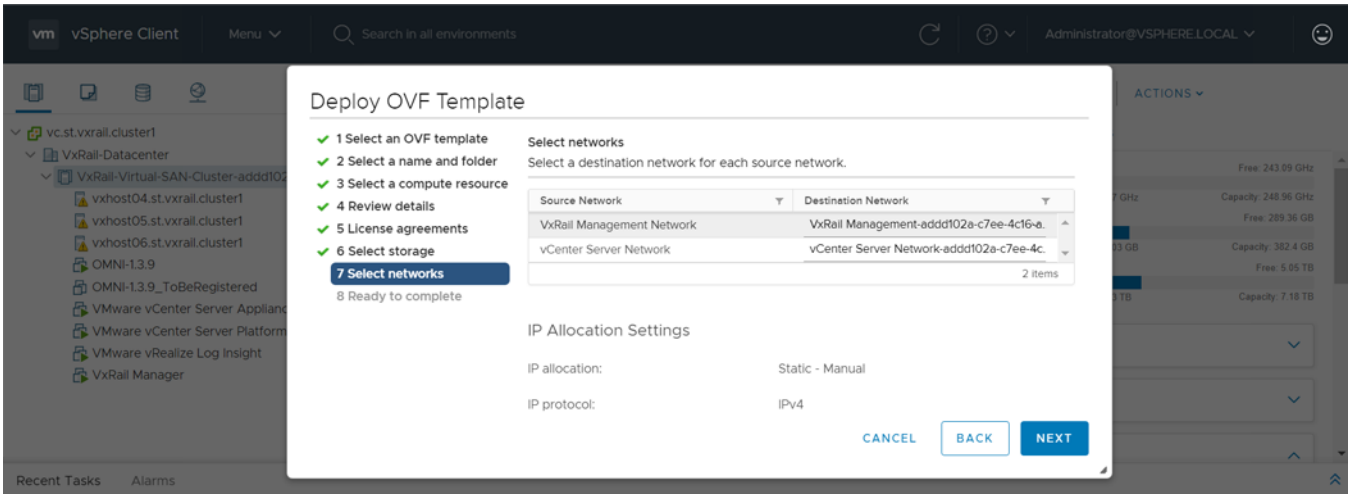
7. Accept the end-user license agreement (EULA), and click **Next**.



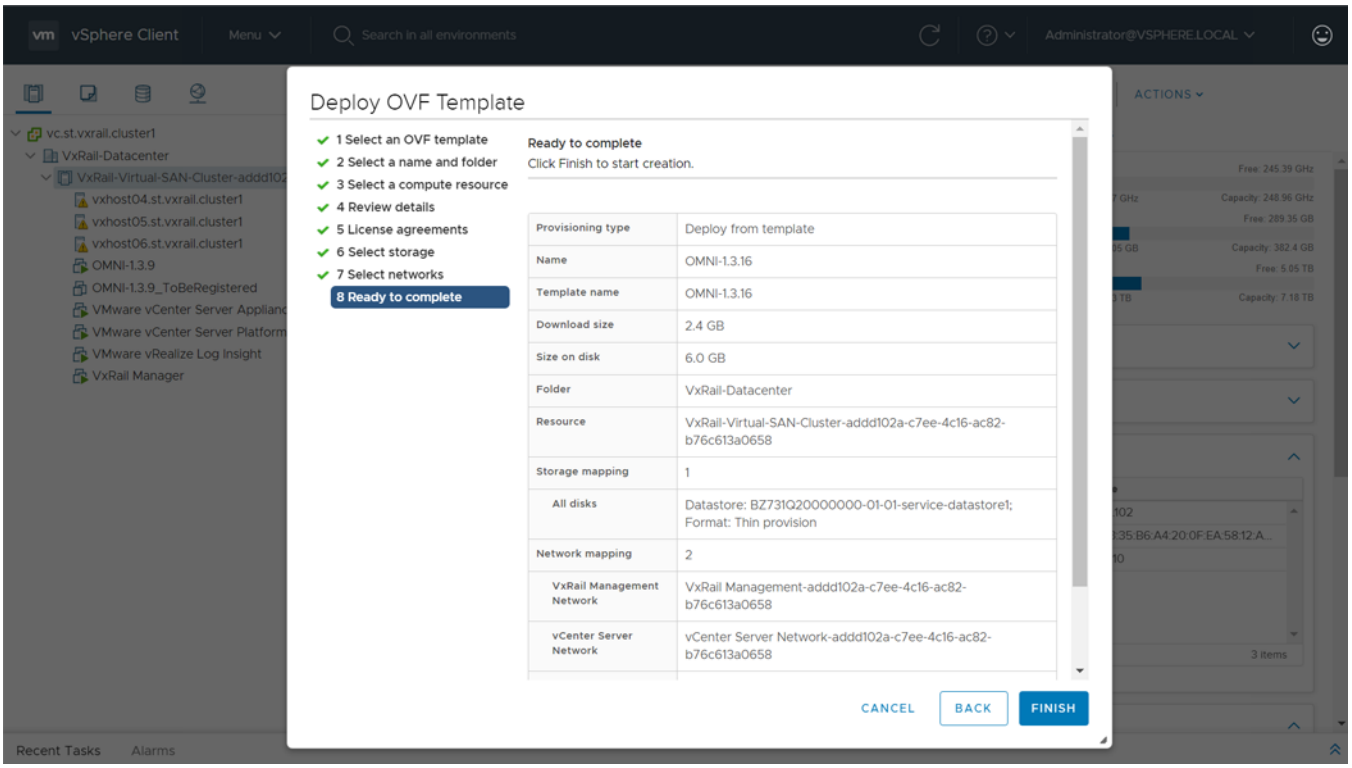
8. Select the VSAN datastore for the configuration and disk files, and click **Next**.



9. Select a destination network for each network source, and click **Next**. The VxRail Management Network must be assigned to the **VxRail internal Management network**. The default VLAN ID for this network is **3939**. The vCenter Server network must be connected to the port group where the vCenter Server is reachable for deployment of the OMNI plug-in. **If you are using a standalone generic ESXi host deployment, you can skip this step.**

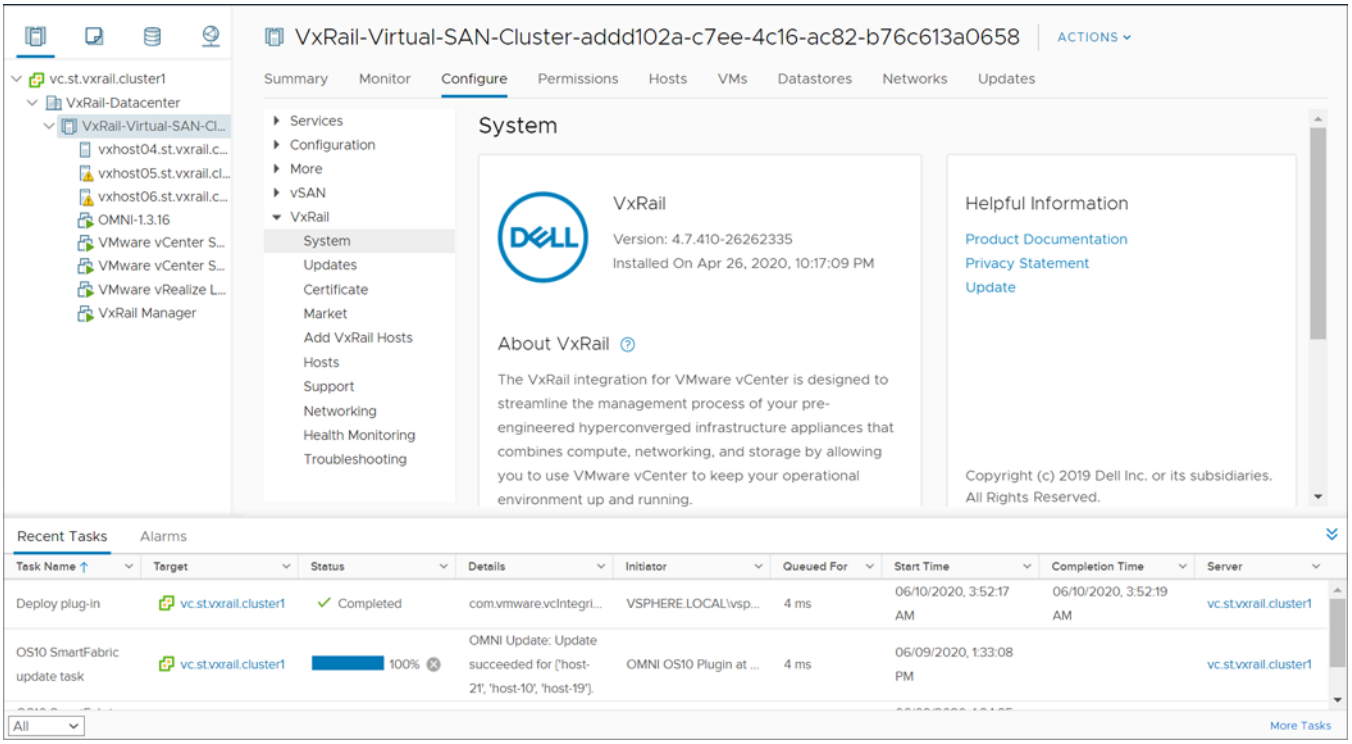


10. Click **Finish** to start creation of the VM.

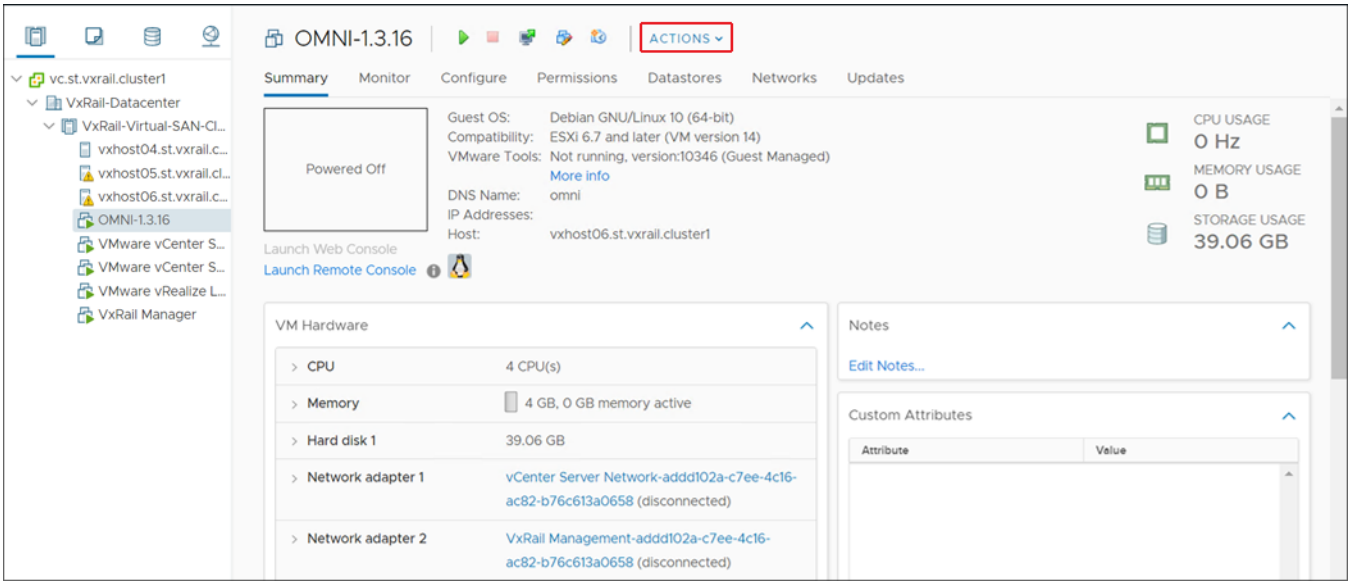


Power on OMNI VM

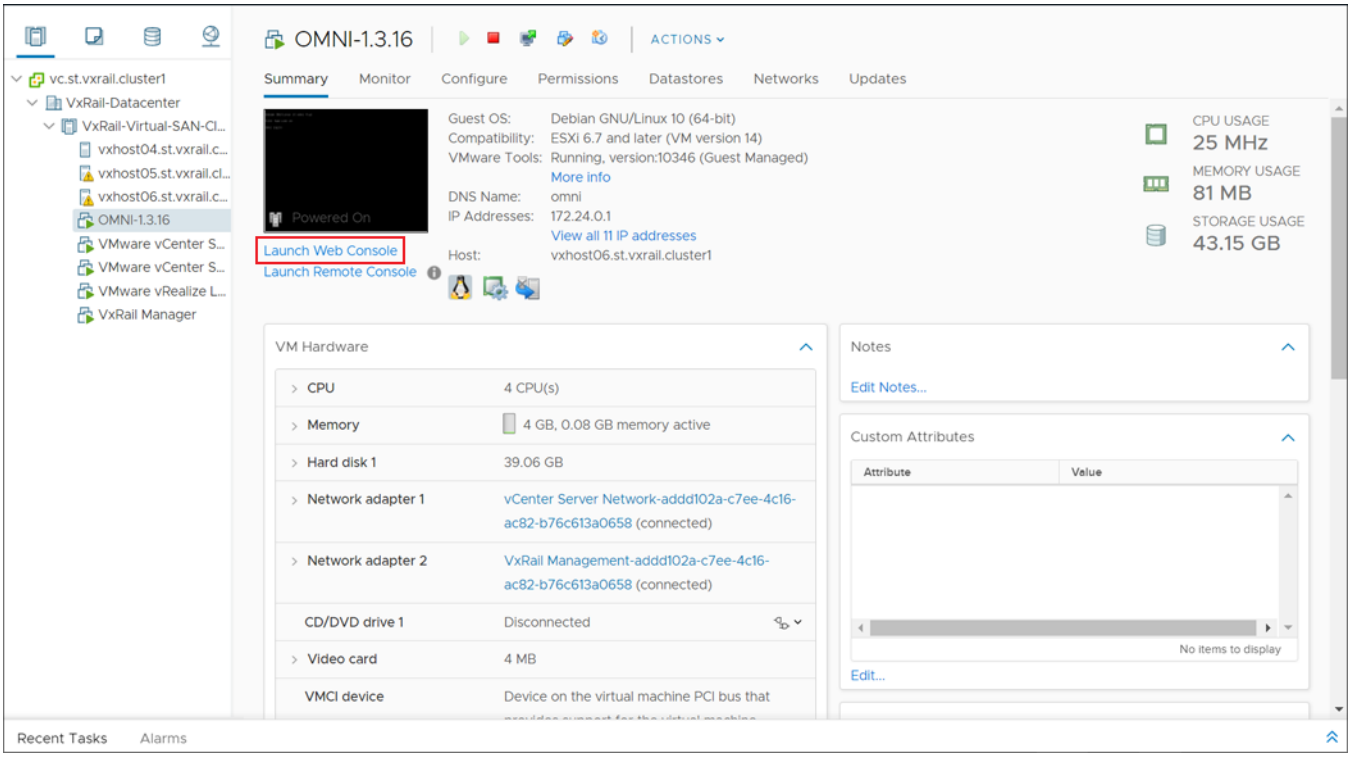
1. Click **Recent Tasks** and scroll to the bottom of the window to view the status, and wait for the deployment to finish.



2. Select the OMNI VM you want to power on, and select **Actions** > **Power** > **Power On**.



3. Select **Launch Web Console**.



Set up OMNI

This information describes how to log in to the VM console, and also explains the OMNI vCenter setup.

Log in to VM console

Configure OMNI through the VM console after completing the authentication step. By default, the VM console automatically closes after 10 minutes, but can be customized.

1. Enter `admin` for both the default username and password.

```
Debian GNU/Linux 10 dellemc-networkappliance tty1

dellemc-networkappliance login: admin
Password:
Linux dellemc-networkappliance 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Updating the password from default value
Changing password for admin.
Current password:
New password:
Retype new password: _
```

2. If it is a first-time login, the system prompts for password change.

After the passwords are successfully updated, self-signed certificates are created. You can change the certificates later with OMNI management menu options.

NOTE: The sudo password is the same as the password set for the `admin` user.

NOTE: Root user is disabled by default. To set the password to enable **root** user, use the OMNI VM console CLI menu. You can only access root user through the console.

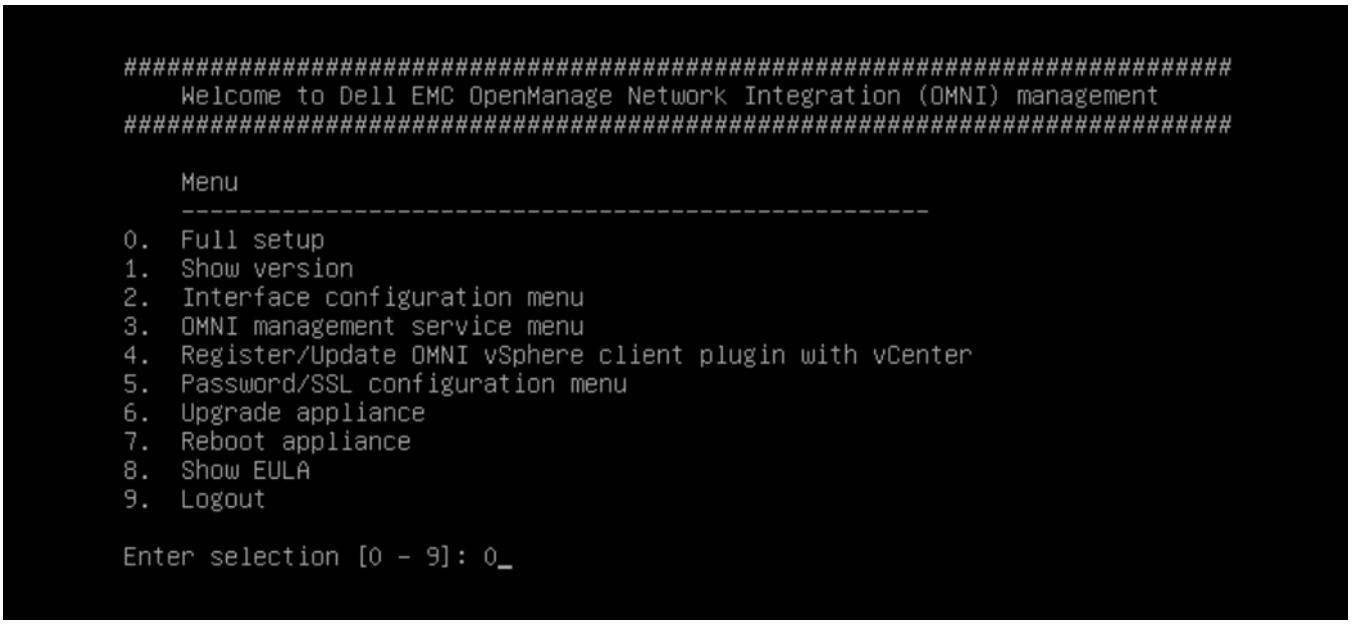
Setup OMNI

This information describes how to set up the appliance with the required network interface configurations, and registration with vCenter and SmartFabric. A single OMNI VM instance supports up to 10 vCenters and 16 SmartFabric domains.

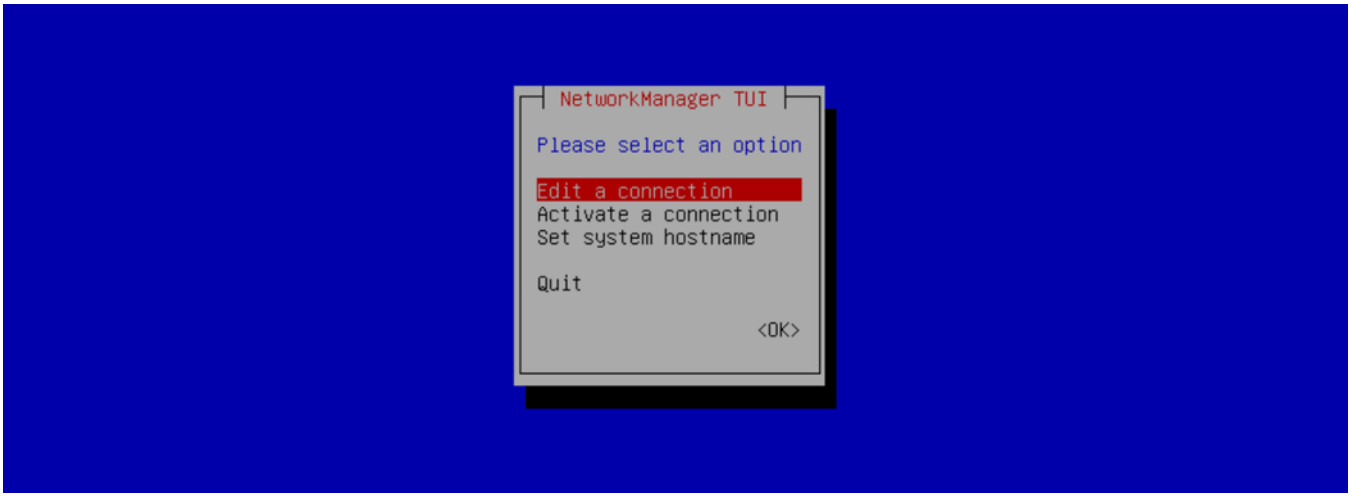
NOTE: The OMNI initial configuration setup can be performed using the vCenter OMNI VM Console only.

Network interface profile configuration

1. Select **0. Full Setup**.

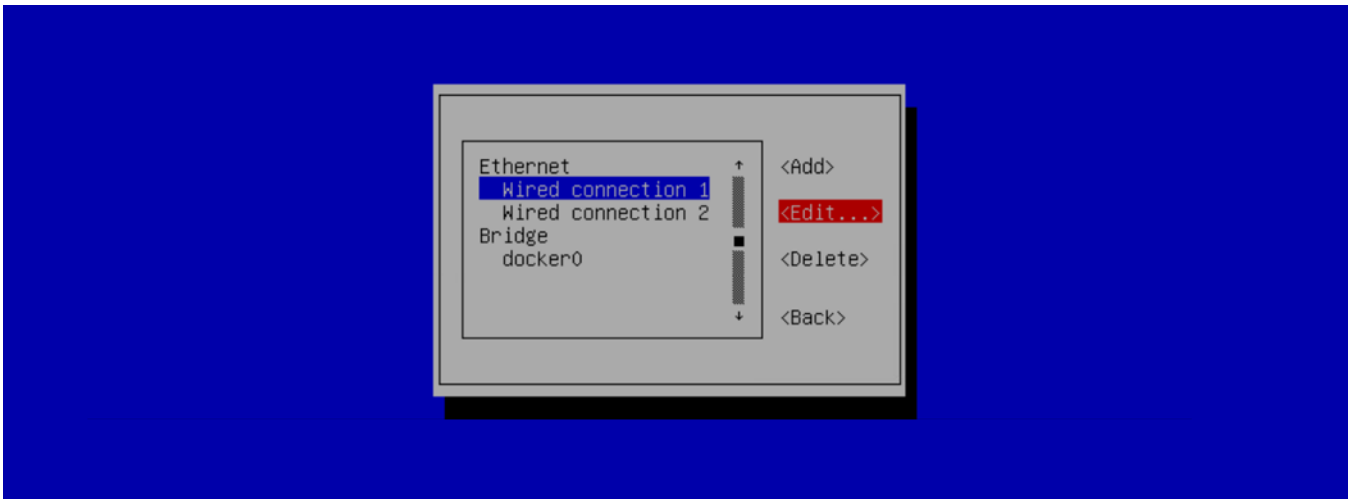


2. Select **Edit a connection**, then click **OK**.

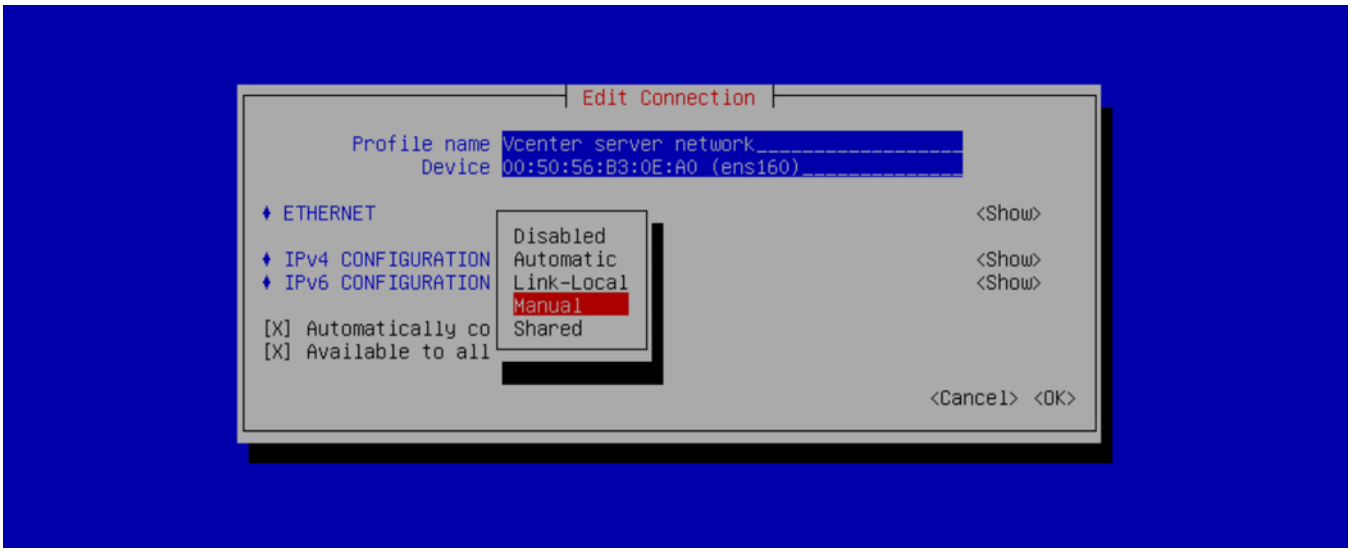


NOTE: **Edit a connection** menu displays edit option of Bridge interface `docker0`. Do not modify any configuration of the `docker0` interface as it can lead to OMNI appliance failure or unexpected OMNI behavior.

3. Select **Wired connection 1**, then click **Edit**.

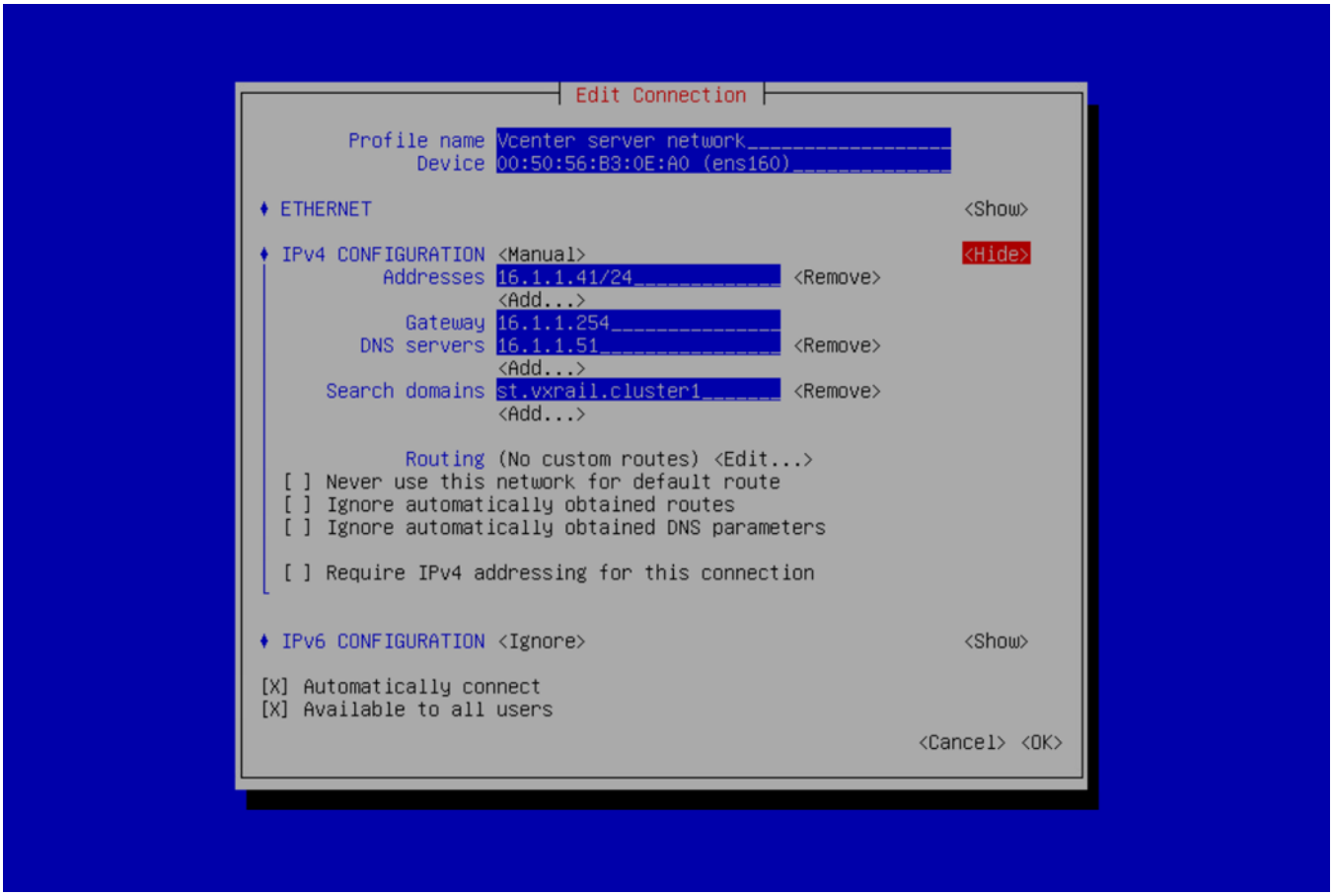


4. Verify Ethernet (ens160) is connected to the vCenter reachable network, then change the Profile name to **vCenter Server Network**.



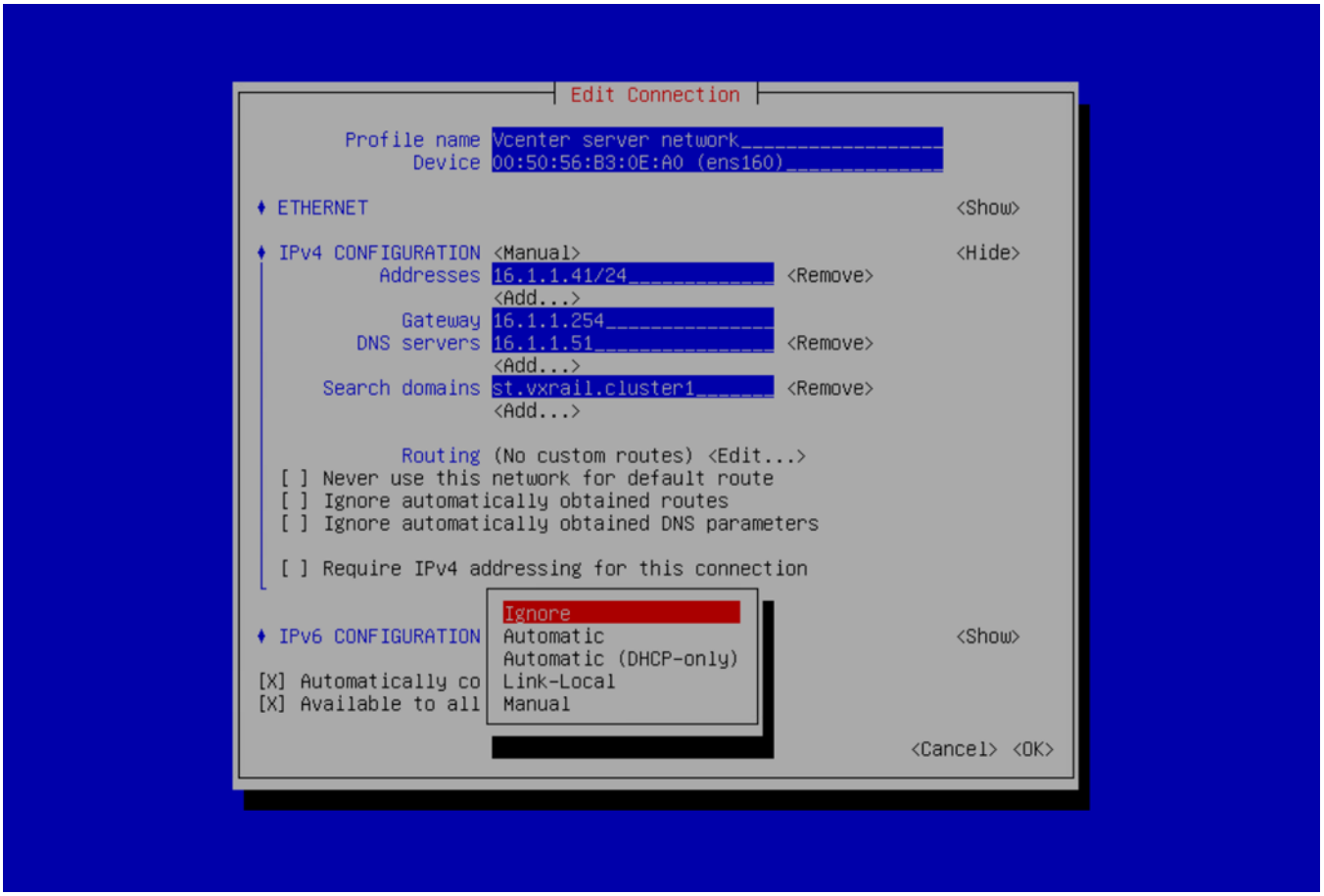
5. Change the IPv4 configuration from Automatic to Manual from the drop-down. You can choose Automatic or Manual IP address configuration.

NOTE: If you are using a stand-alone generic ESXi host deployment and if DHCP services are running on the Management network subnet, use the default IPv4 vCenter server network configuration which uses automatic IP address assignment using DHCP.



6. Click **Show** to the right of IPv4 configuration, then click **Add**.
7. Set the Manual IPv4 address, Gateway address, DNS servers, Search Domains, then click **Edit** to the right of Routing.
8. On IPv6 configuration, select **Ignore** for the IPv6 configuration, then click **OK**.

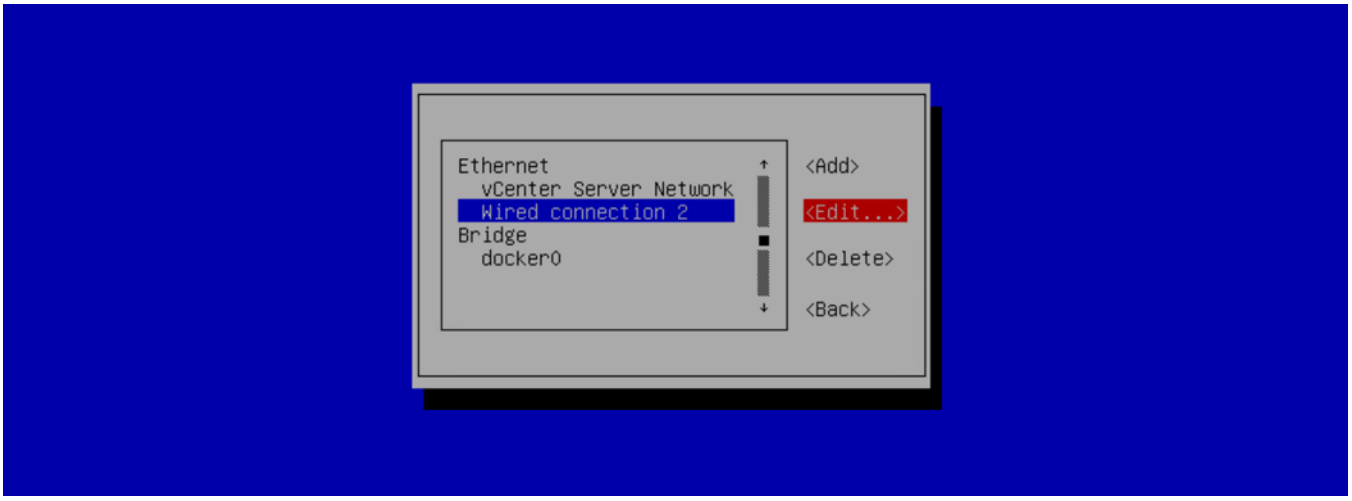
NOTE: IPv6 configuration is only required for an in-band network.



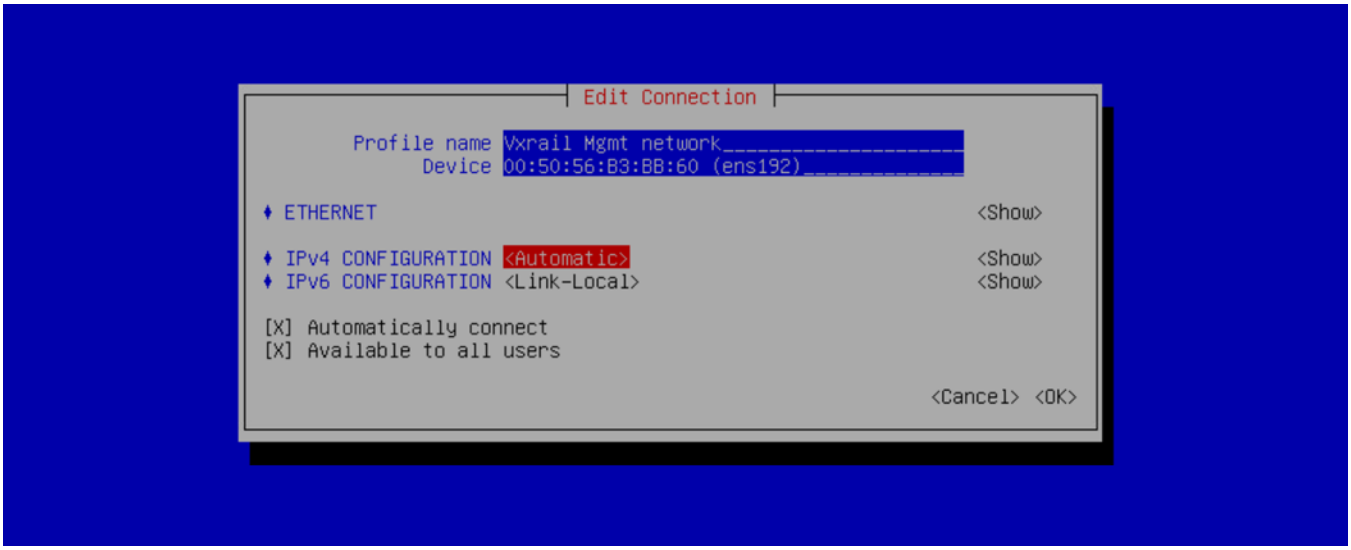
You are now ready to continue configuration.

NOTE: If you are not connecting the OMNI VM to a SmartFabric local-link, ignore this part as it not applicable and you are ready to activate the connection profile.

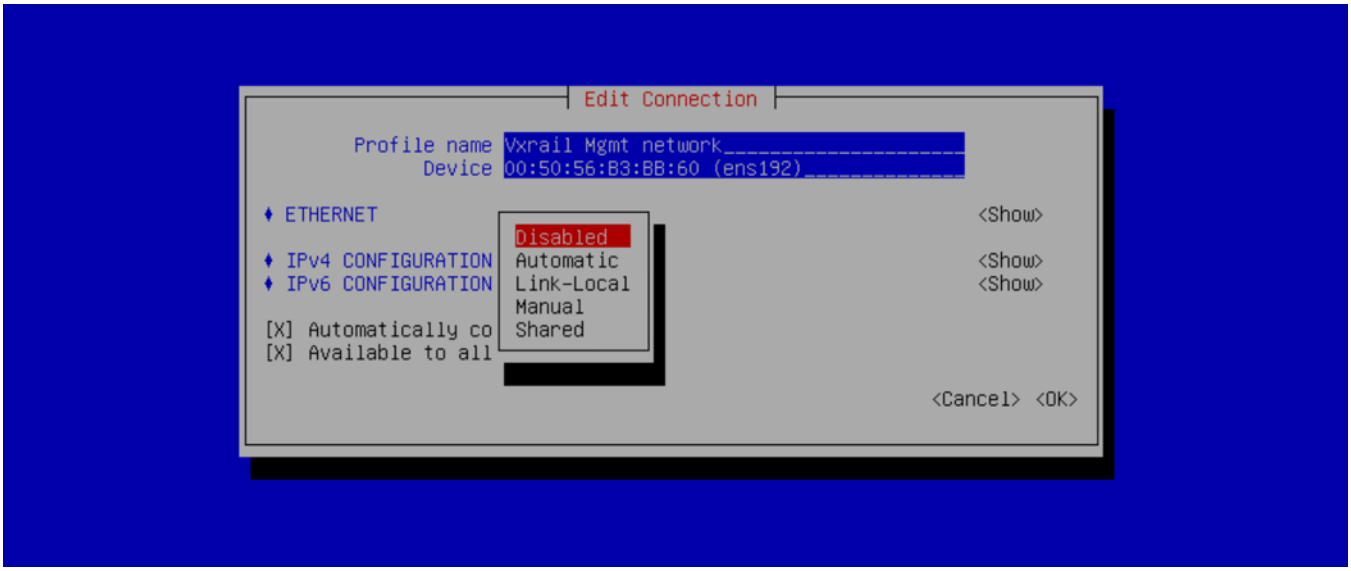
1. Select **Wired connection 2**, and click **Edit**.



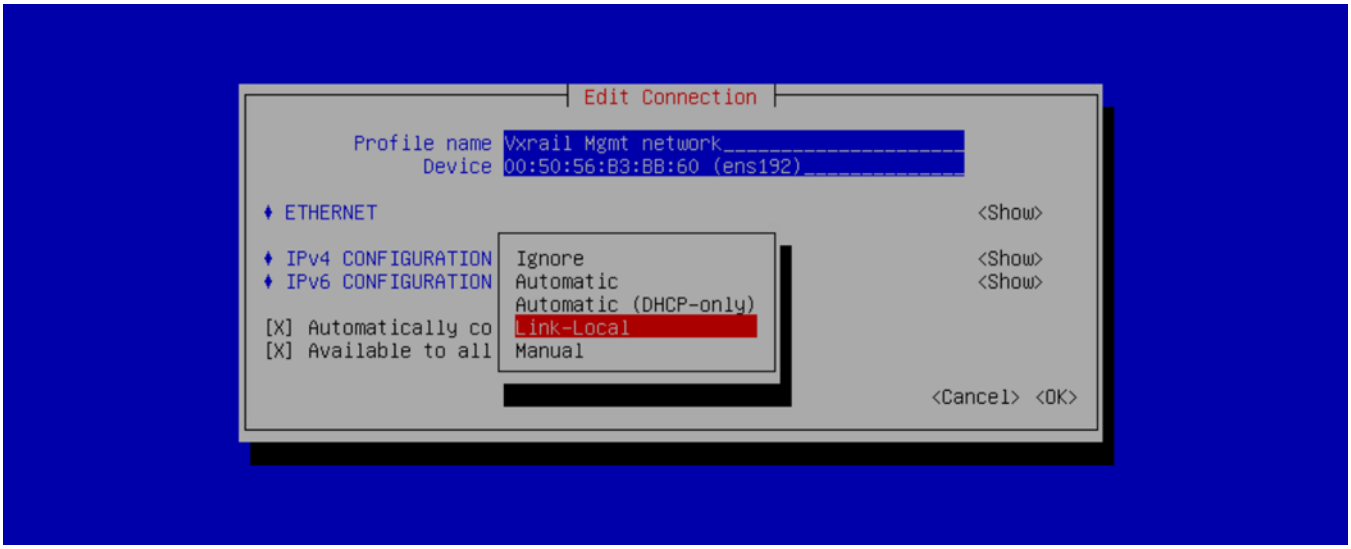
2. Rename Profile name to **VxRail Mgmt Network**.



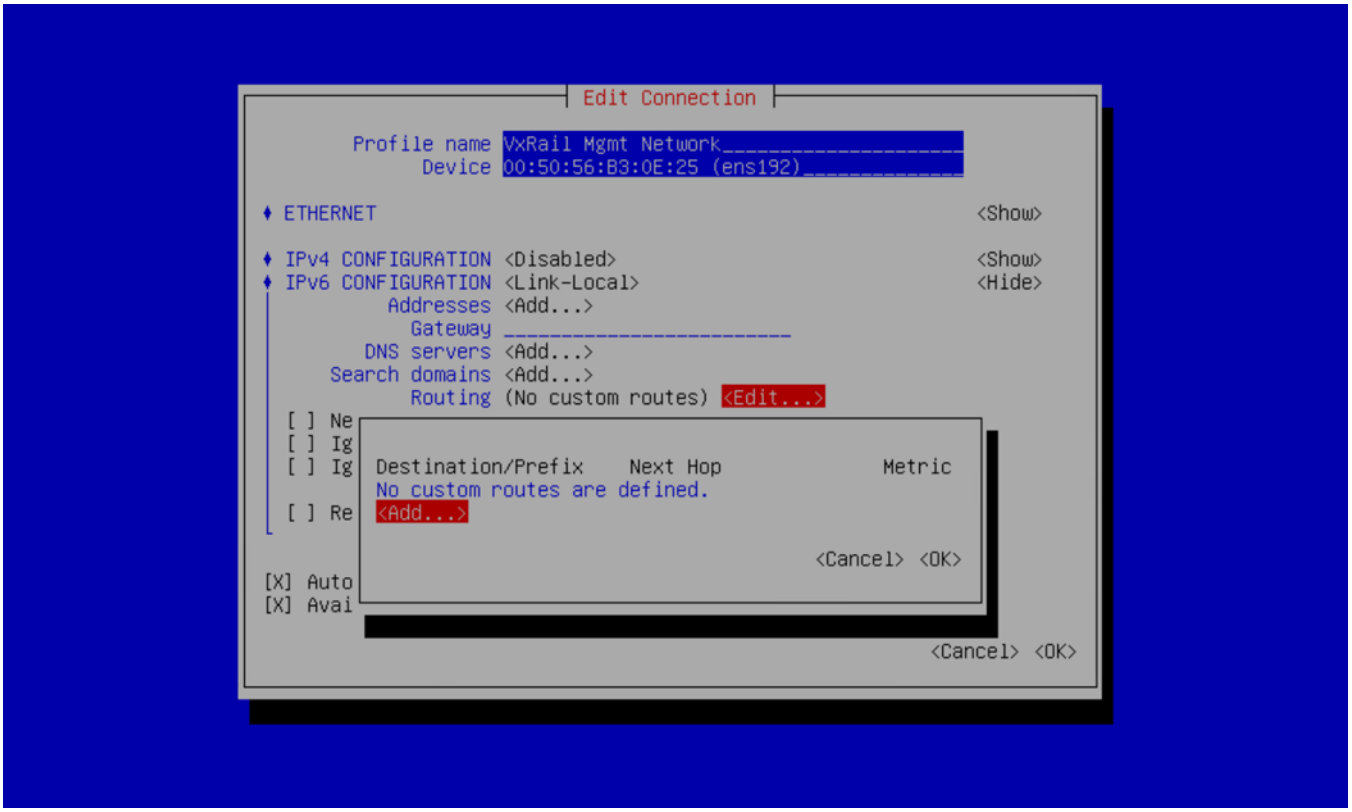
3. Select **Disabled** for the IPv4 configuration.



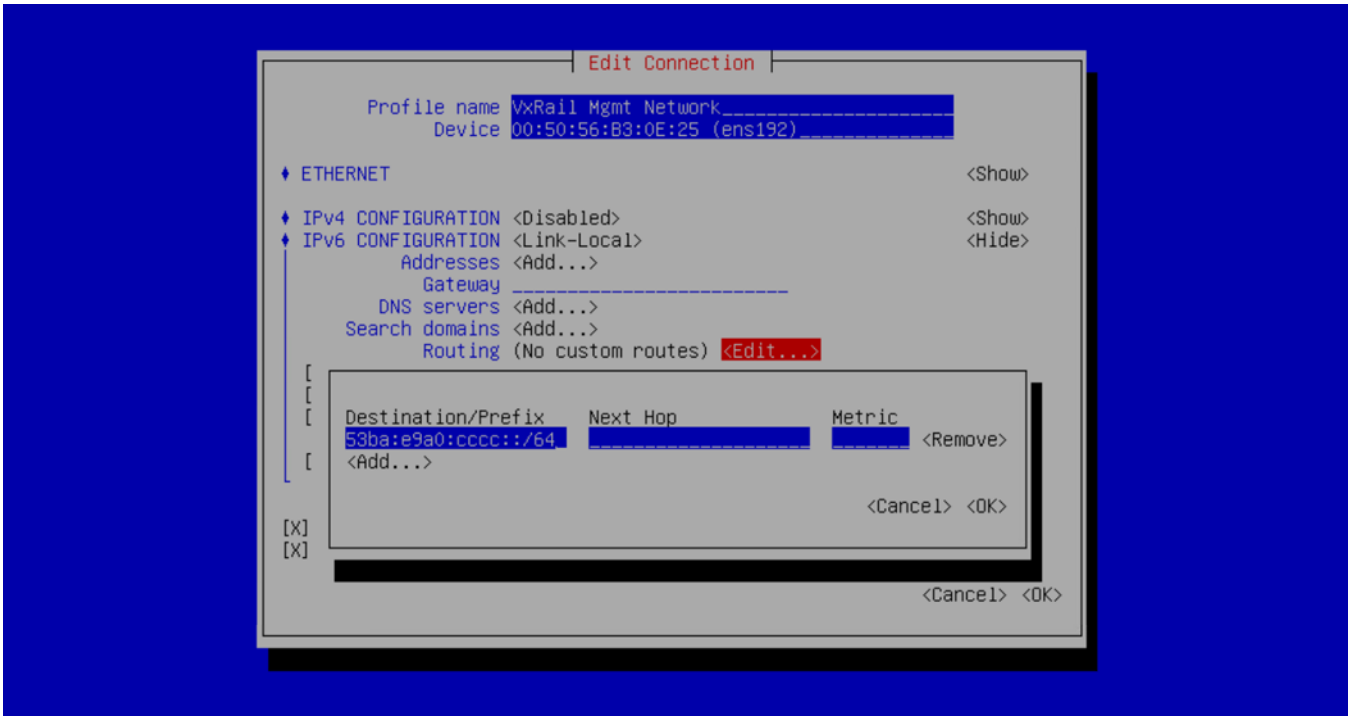
4. Select **Link-Local** for the IPv6 configuration.



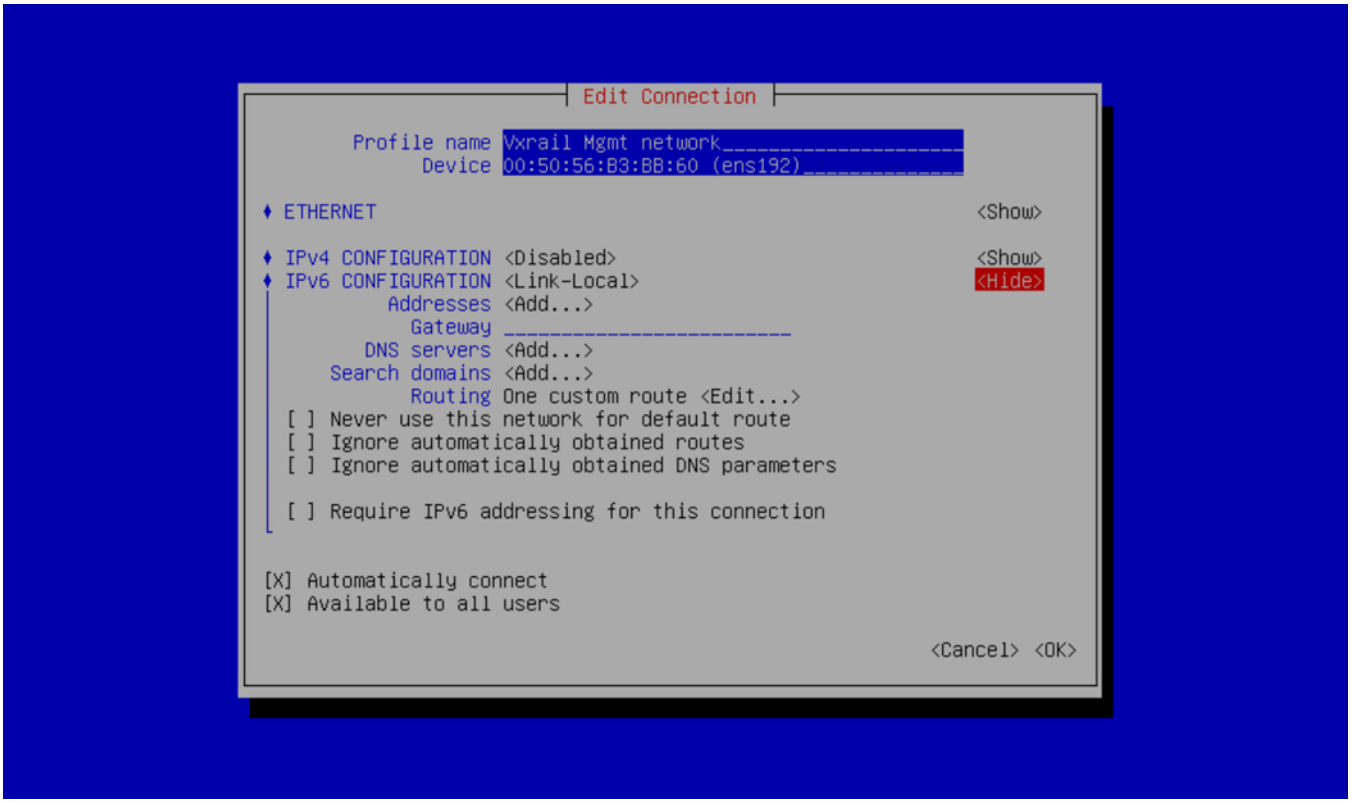
5. Click **Edit** to the right of Routing, and click **Add**.



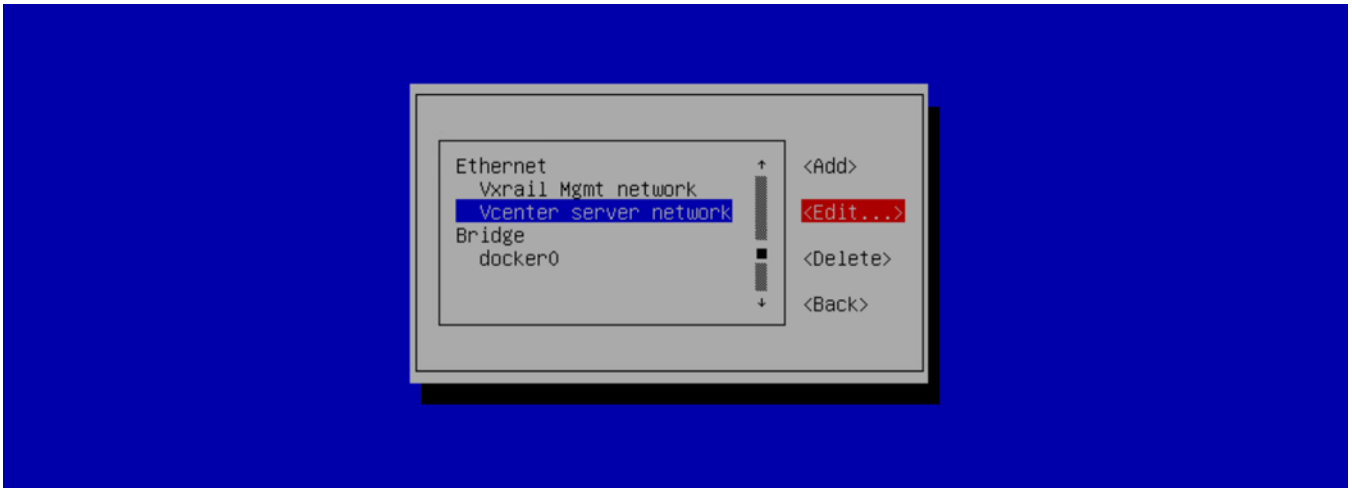
6. Enter the custom route as **fde1:53ba:e9a0:cccc::/64**, and click **OK**.



7. One custom route is now configured, click **OK**.



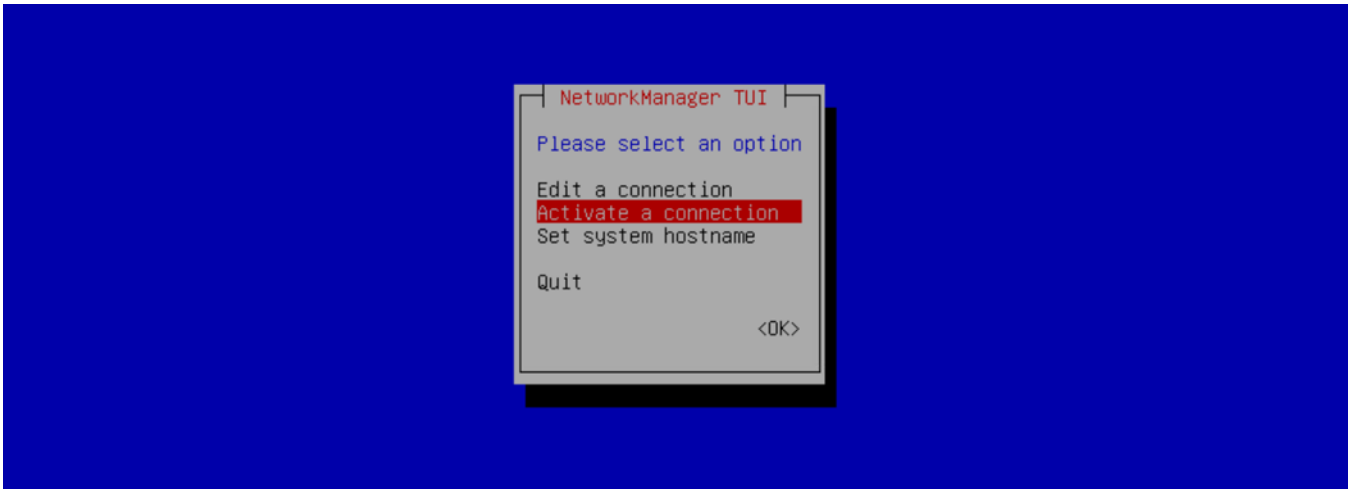
8. Click **Back** to activate the connection profiles.



Activate connection profiles

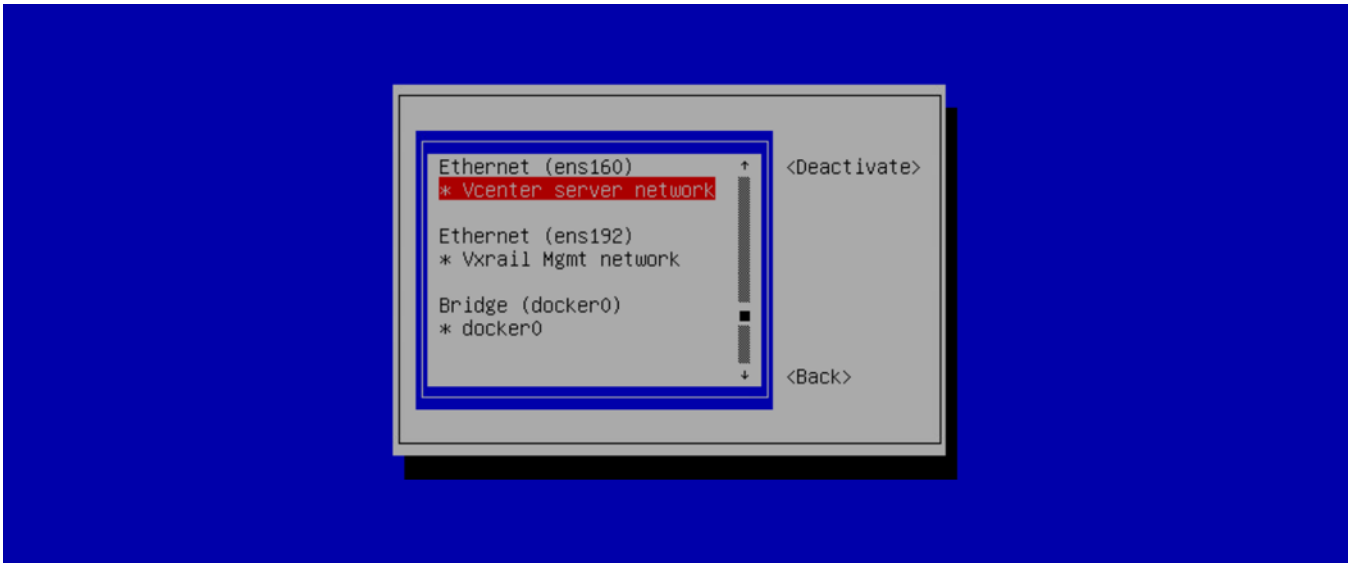
NOTE: To populate DNS entries automatically, deactivate and active each profile.

1. Select **Activate a Connection**, and click **OK**.

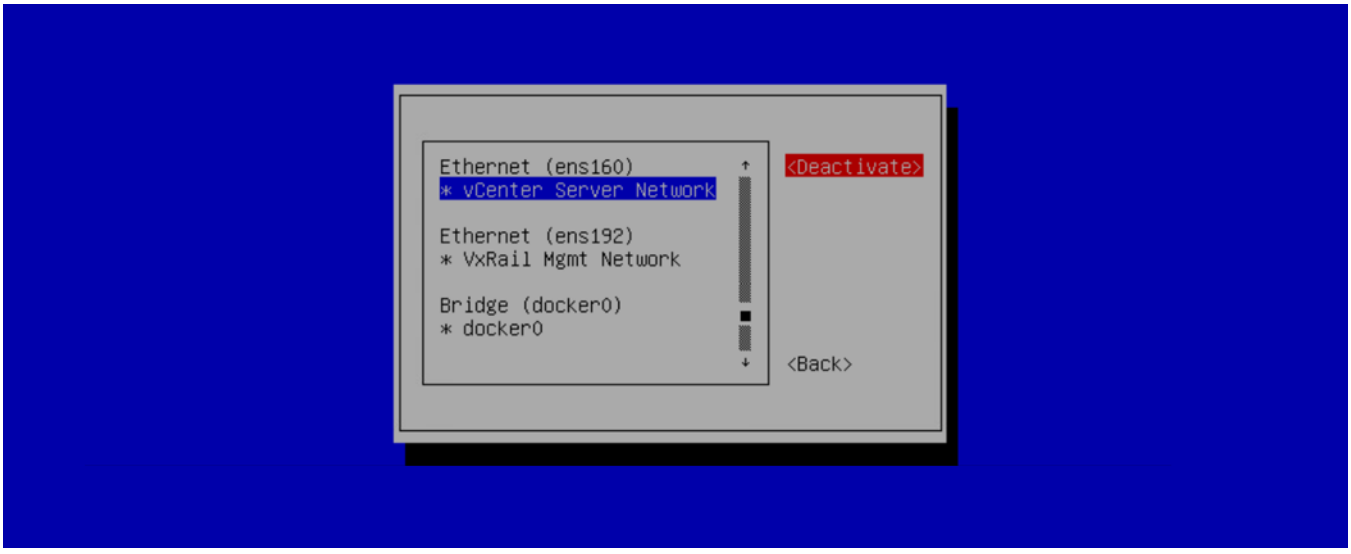


NOTE: If you change while editing a connection, you must deactivate then activate the connection for the respective interface profile.

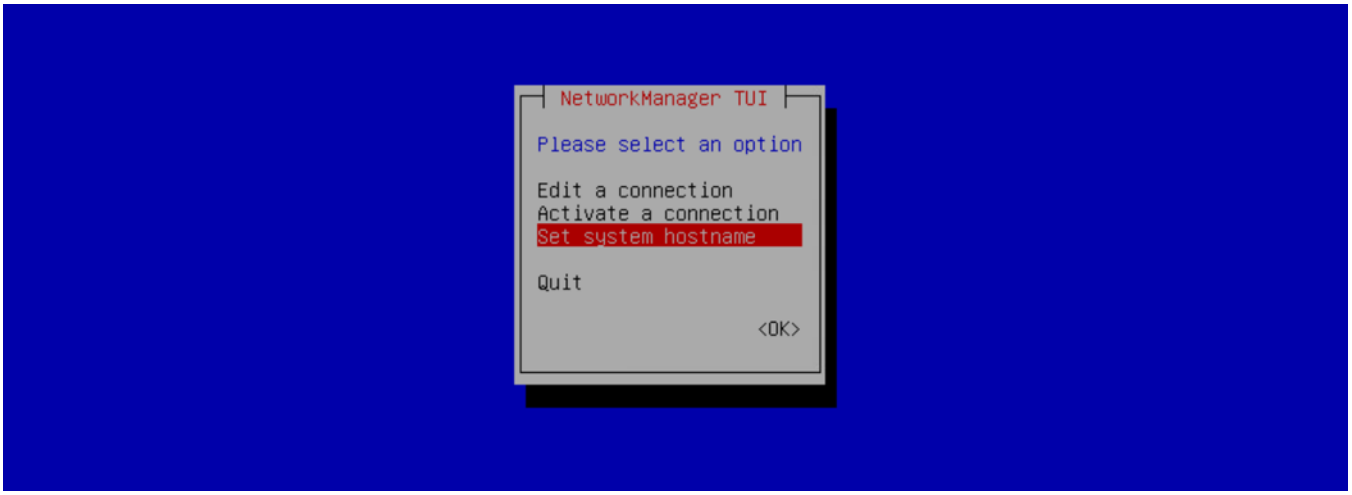
2. Select the **vCenter Server Network** profile, and click **Deactivate**. Repeat for **VxRail Mgmt Network**.



3. Select the **vCenter Server Network** profile, and click **Activate**. Repeat for **VxRail Mgmt Network**.

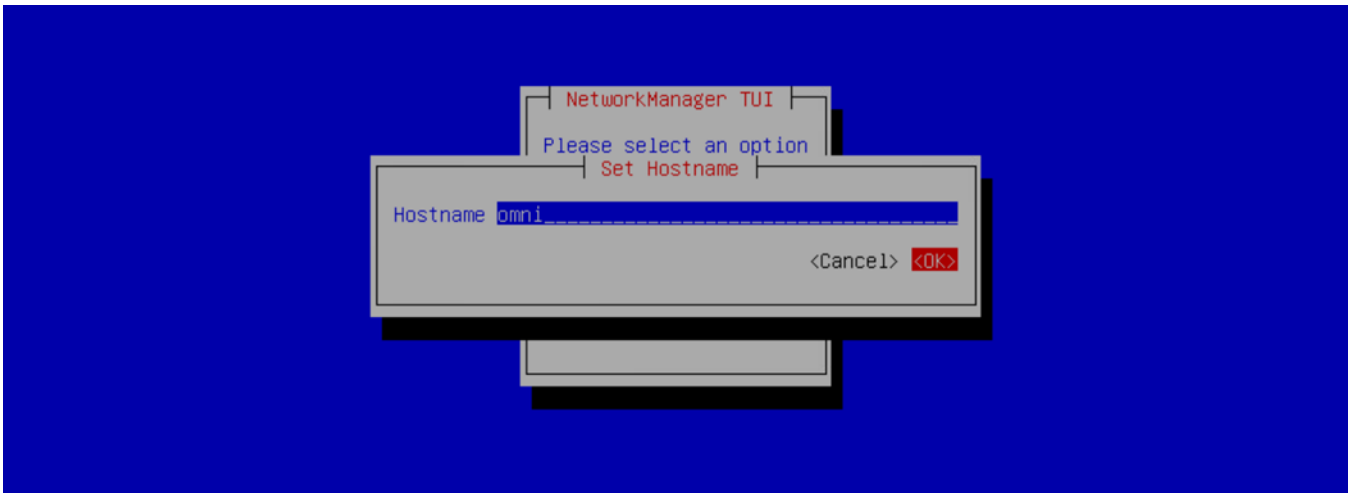


4. Click **Back**, select **Set system hostname**, and click **OK**.

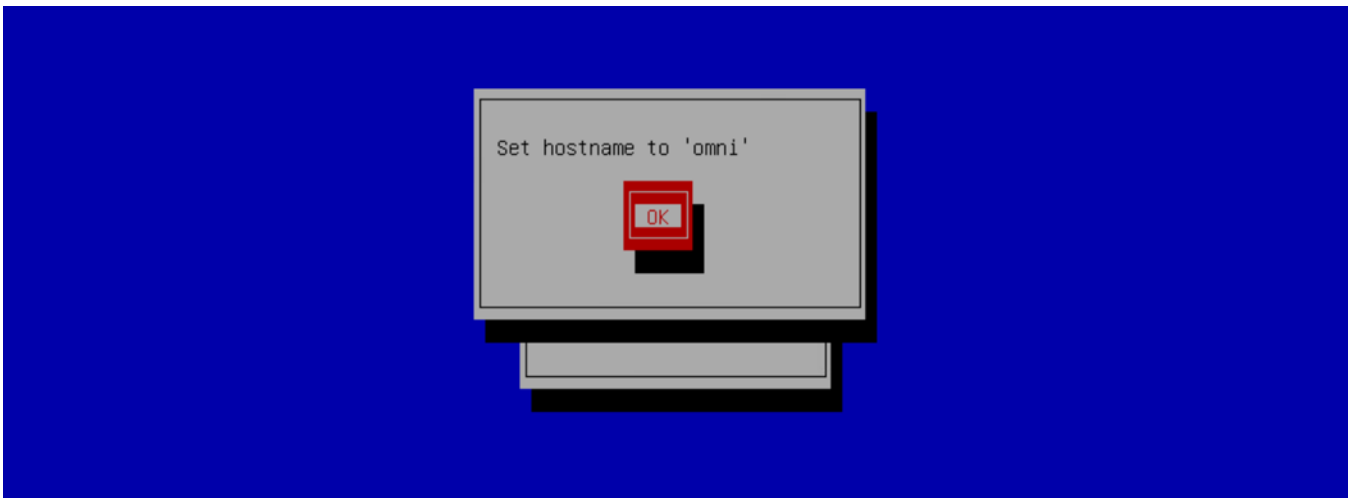


NOTE: If you are setting the hostname of OMNI, ensure you have the DNS entry of the OMNI hostname.

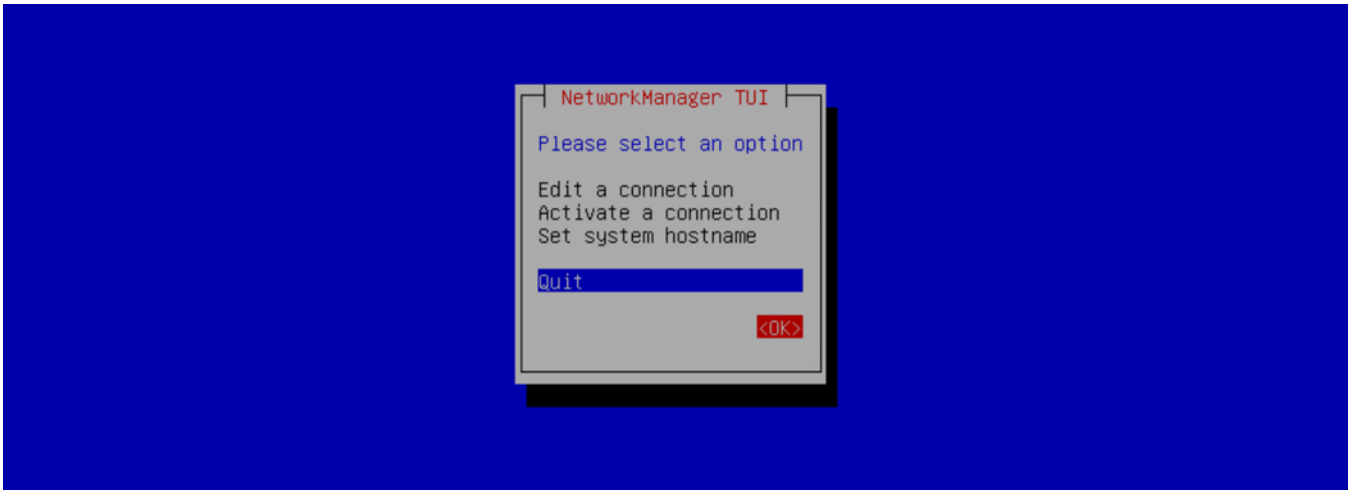
5. Enter **omni** for the hostname, and click **OK**.



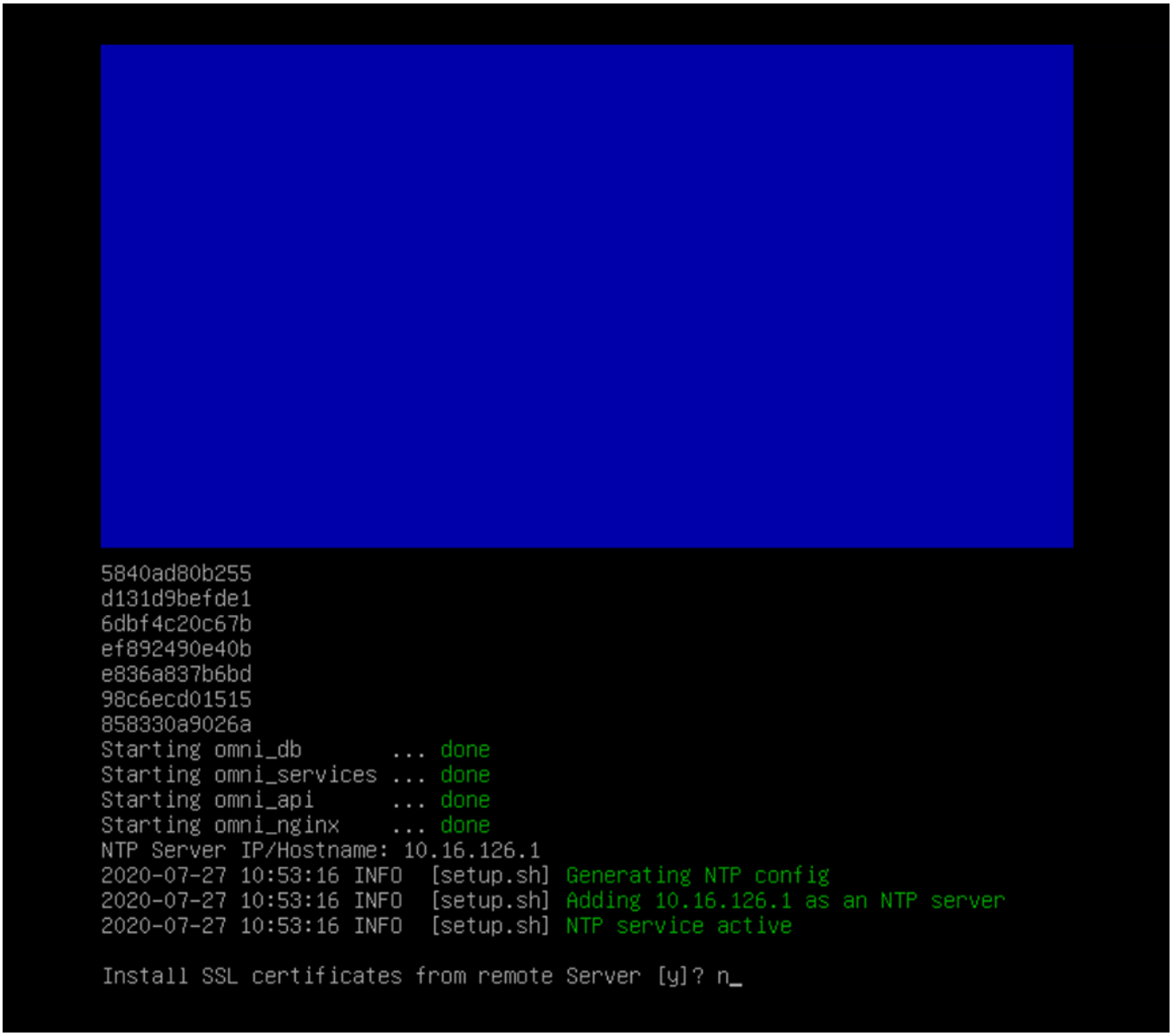
6. The hostname is now set. Click **OK**.



7. Click **Back**, and **OK** to exit the network management UI.



8. Enter a valid NTP Server IP address or hostname, and click **Enter**.
9. Enter **n** to not install the SSL certificate from remote server. When you enter **n**, the self-signed certificate that is created locally is installed.



NOTE: To install a new certificate, see Generate and install SSL certificate.

NOTE: If the NTP Server is not configured, the OMNI appliance VM synchronizes with the ESXi server time zone.

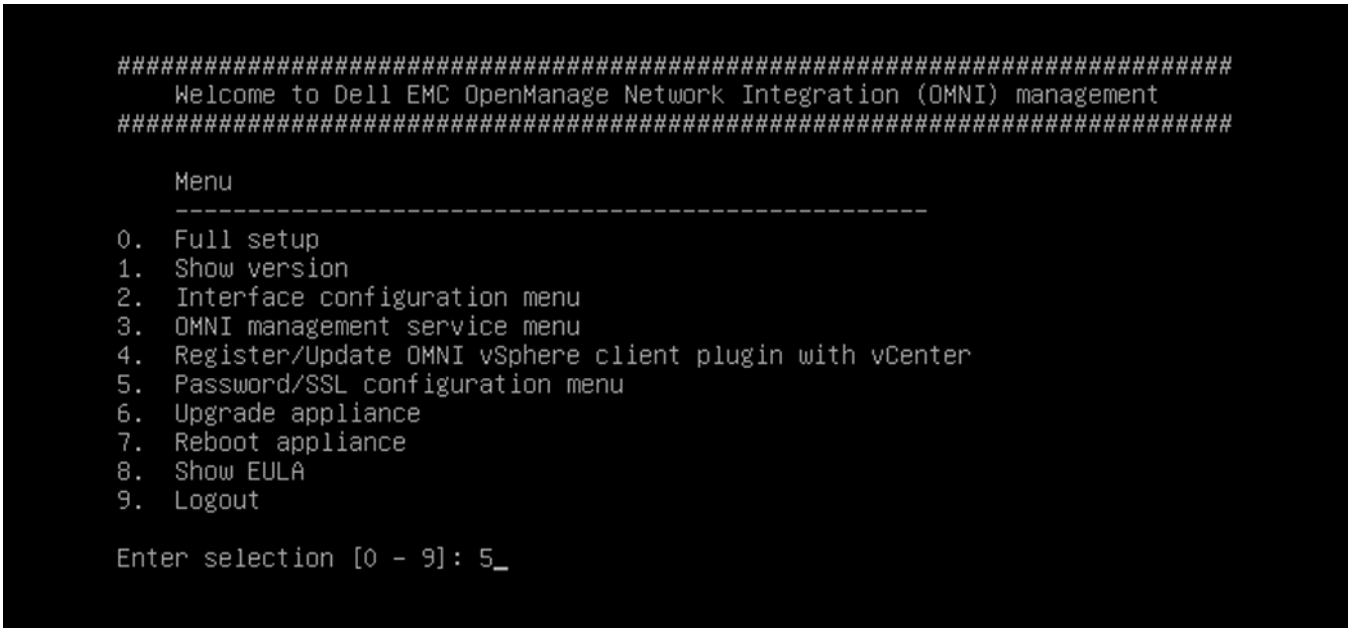
Generate and install SSL certificate

OMNI Management menu has options to generate self-signed SSL certificates or install SSL certificates from remote server.

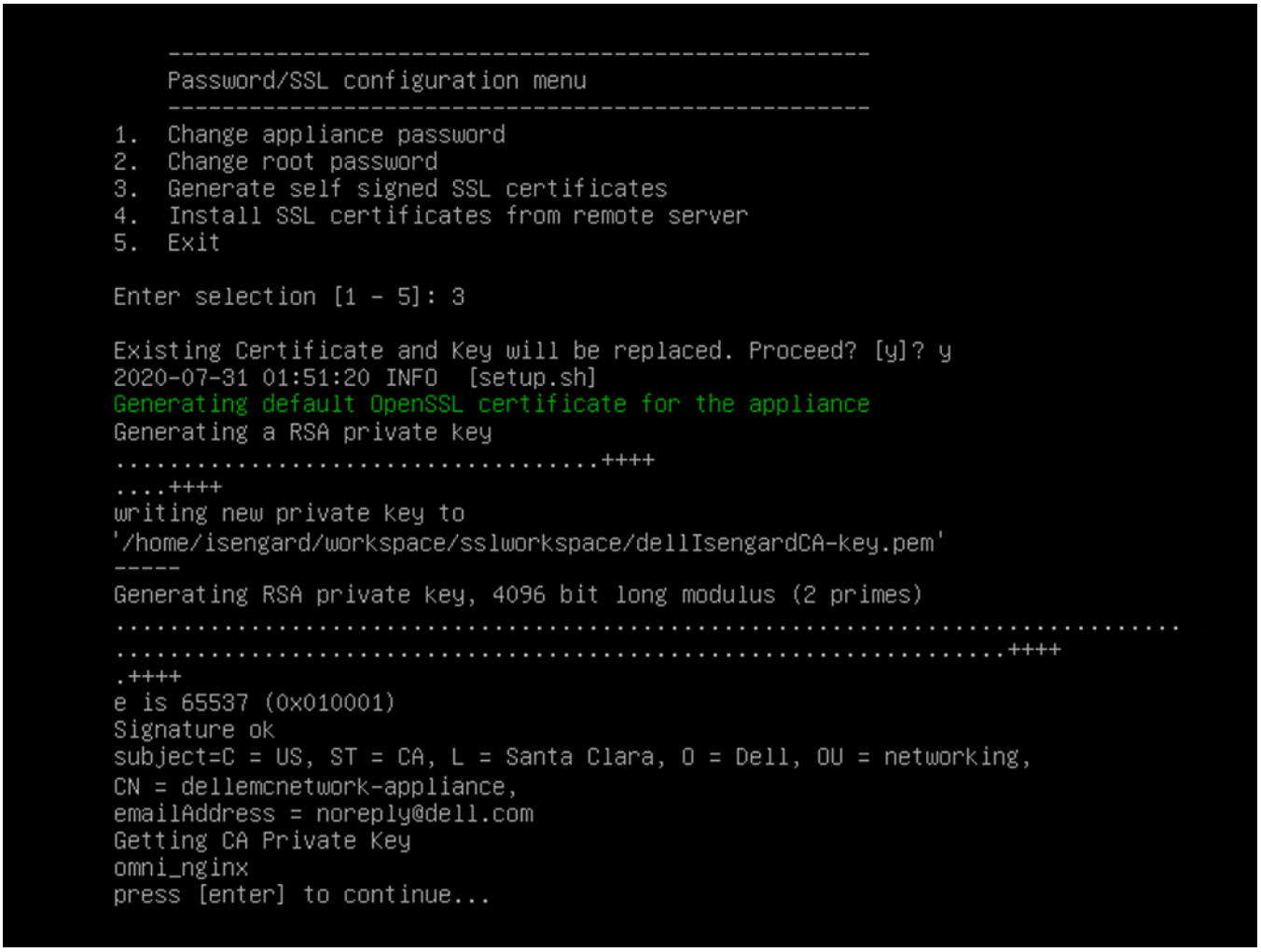
Generate self-signed SSL certificate

To generate a self-signed SSL certificate:

1. From the OMNI management menu, select **5. Password/SSL configuration menu**.

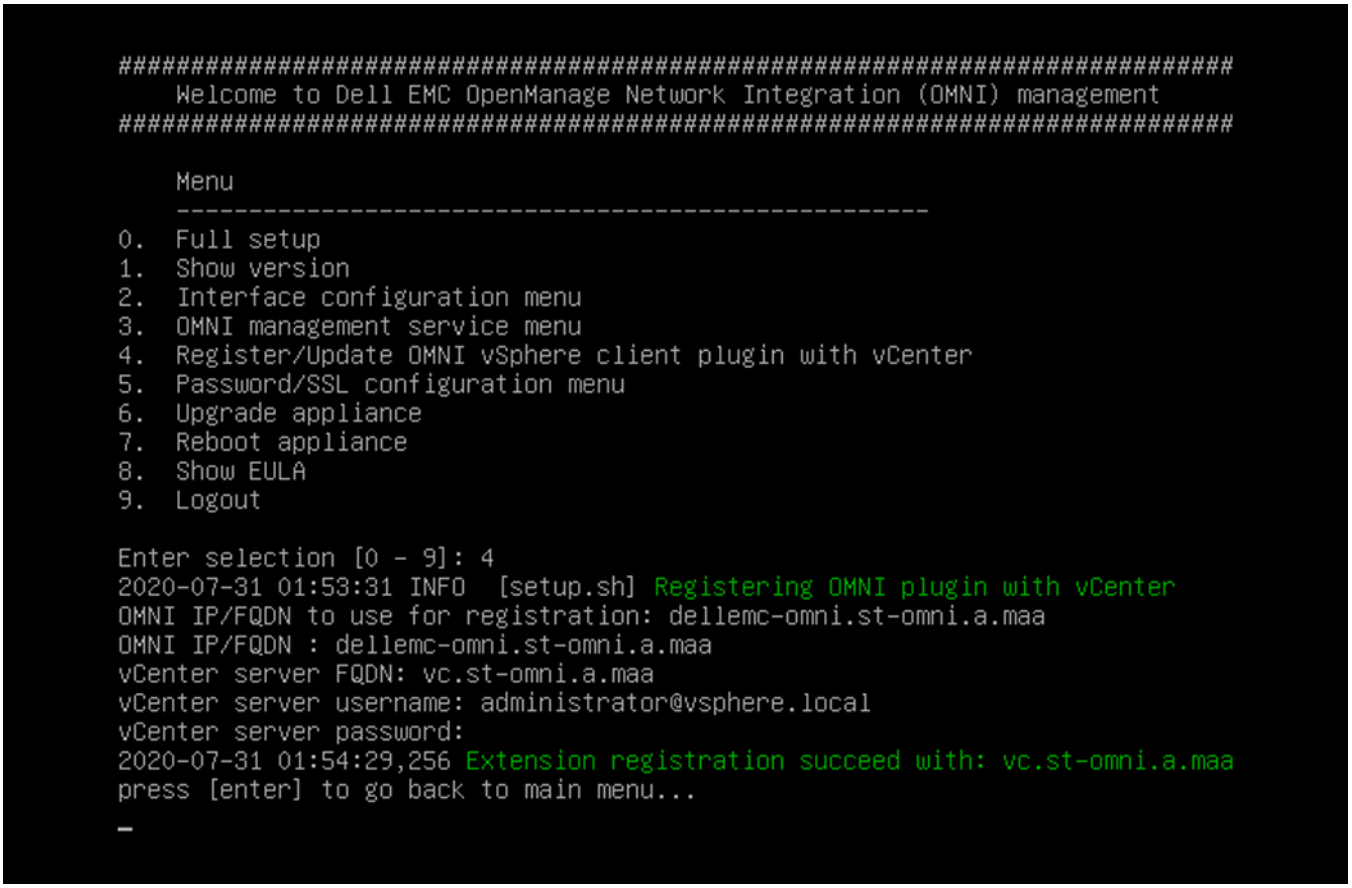


2. Enter the selection as **3. Generate self signed SSL certificates**. OMNI VM displays confirmation for replacing the existing certificate and key with the newly created certificates and keys.



3. Register or update the OMNI appliance with vCenter for applying the new SSL certificate. From the OMNI management menu, select **4.Register/update OMNI vSphere client plug-in with vCenter**.

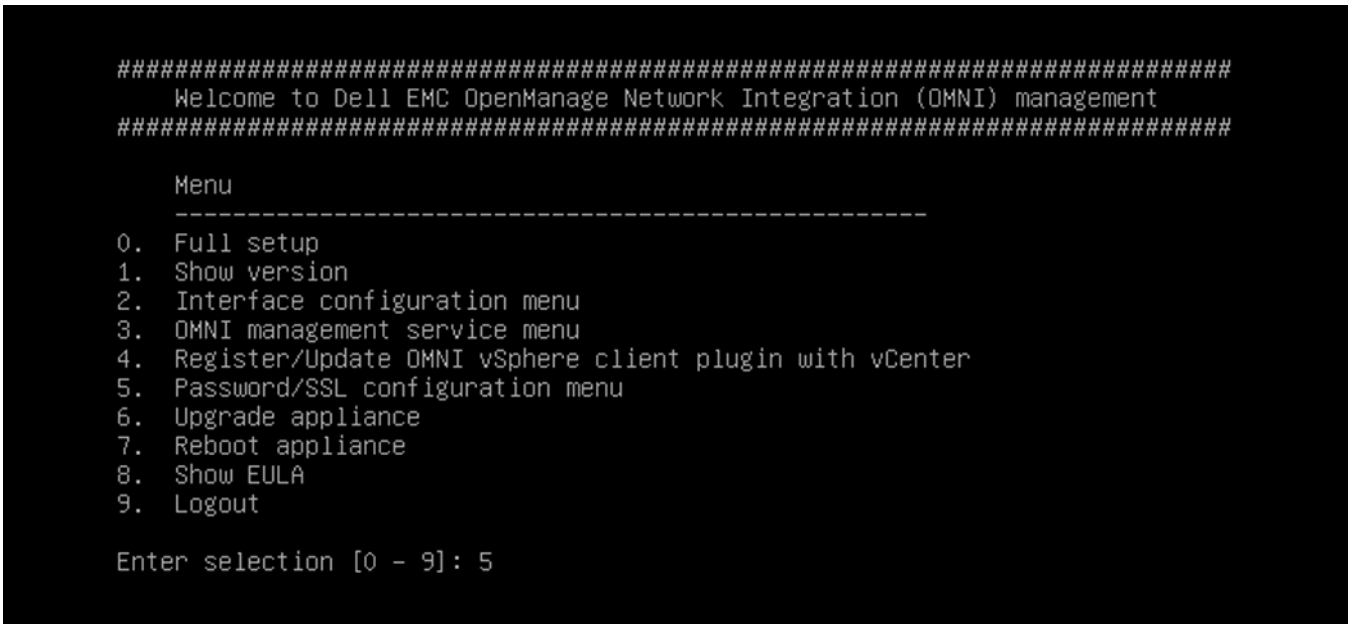
NOTE: Refresh the browser to view the OMNI UI plug-in from the vCenter when you register or unregister OMNI 1.3 VM appliance with vCenter 7.0. For older versions of vCenter, log out and log in to access the plug-in from the vCenter.



Install SSL certificate from remote server

To install SSL certificate from remote server:

1. Generate SSL certificate using a standard method in .pem or .crt formats.
2. Copy the generated files to the remote SCP server.
3. From the OMNI management menu, select **5. Password/SSL configuration menu**.

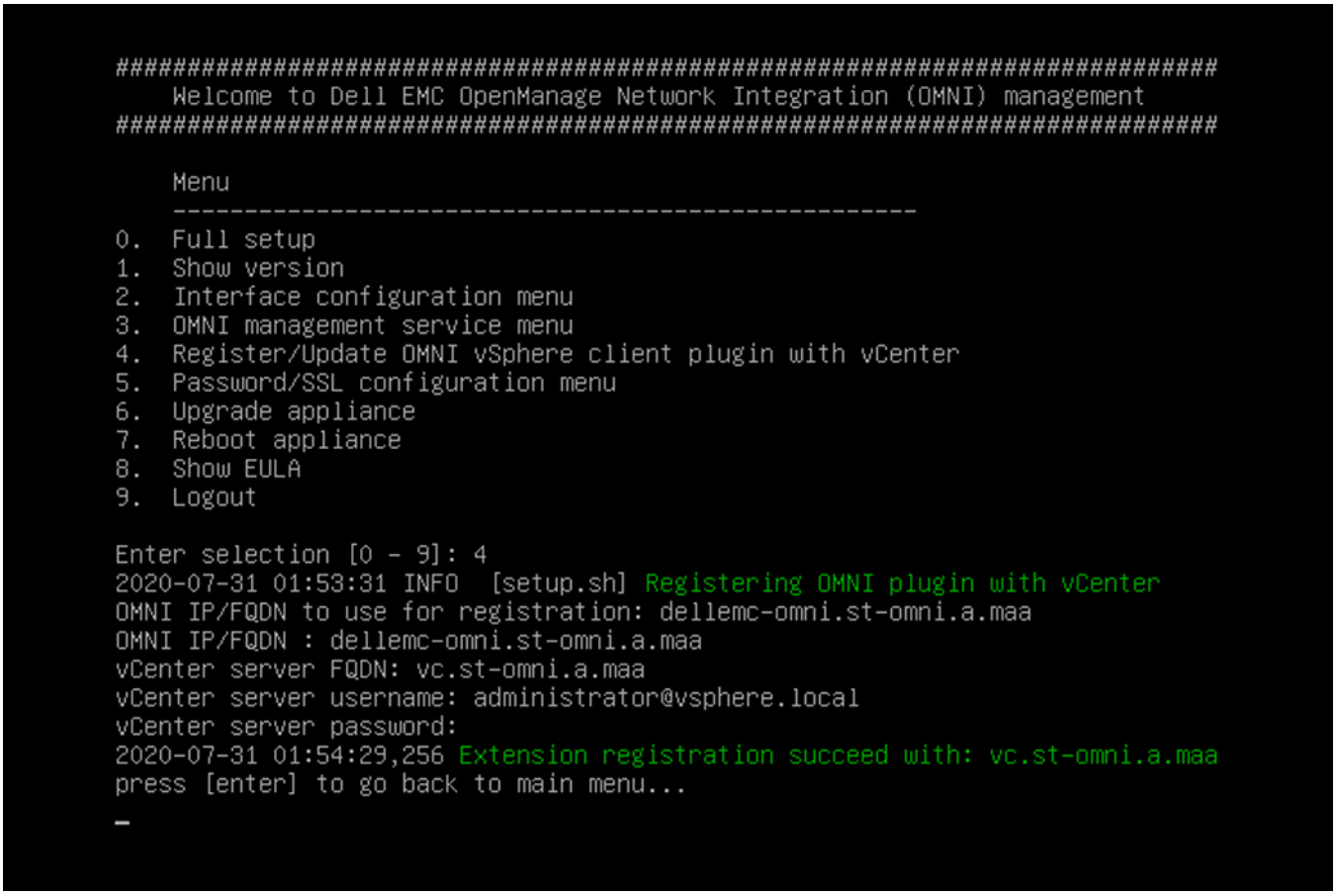


4. Enter the selection as **4. Install SSL certificate from remote server** to install the certificate. Enter the remote SCP server IP address or hostname and login to the SCP server. Provide the path to the certificate and private key in the server. The files are copied to the OMNI VM.

```
    ------------------------------------------------
    Password/SSL configuration menu
    ------------------------------------------------
1.  Change appliance password
2.  Change root password
3.  Generate self signed SSL certificates
4.  Install SSL certificates from remote server
5.  Exit

Enter selection [1 - 5]: 4
2020-07-31 02:07:57 INFO  [setup.sh]
Setting up server certificate for HTTPS service
Remote SCP server IP/hostname: 192.168.101.32
Username: admin
File path [certificate file format(.crt/.pem)]: /tmp/omni-cert.pem
The authenticity of host '192.168.101.32 (192.168.101.32)' can't be established.
ECDSA key fingerprint is SHA256:Hxik4YrYfZfrEbR5r5oegH8XivUdGdHHTL/+F29hiQQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.101.32' (ECDSA) to the list of known hosts.
admin@192.168.101.32's password:
omni-cert.pem                                 100% 1034     5.2MB/s   00:00
2020-07-31 02:08:44 INFO  [setup.sh]
File successfully copied to /home/isengard/workspace/sslworkspace/tempcertfile
2020-07-31 02:08:44 INFO  [setup.sh]
Setting up server private key for HTTPS service
Remote SCP server IP/hostname [192.168.101.32]:
Username [admin]:
File path [must be private key format(.pem)]: /tmp/omni-key.pem
admin@192.168.101.32's password:
omni-key.pem                                  100% 1675     7.1MB/s   00:00
2020-07-31 02:09:11 INFO  [setup.sh]
File successfully copied to /home/isengard/workspace/sslworkspace/tempprivkeyfile

Installing new keys will restart the service. Proceed? [y]? _
```

5. Enter **y** to install the SSL certificate.
6. Register or update the OMNI appliance with vCenter for applying the SSL certificate. From the OMNI management menu, select **4.Register/update OMNI vSphere client plugin with vCenter**.

   NOTE: Refresh the browser to view the OMNI UI plug-in from the vCenter when you register or unregister OMNI 1.3 VM appliance with vCenter 7.0. For older versions of vCenter, log out and log in to access the plug-in from the vCenter.



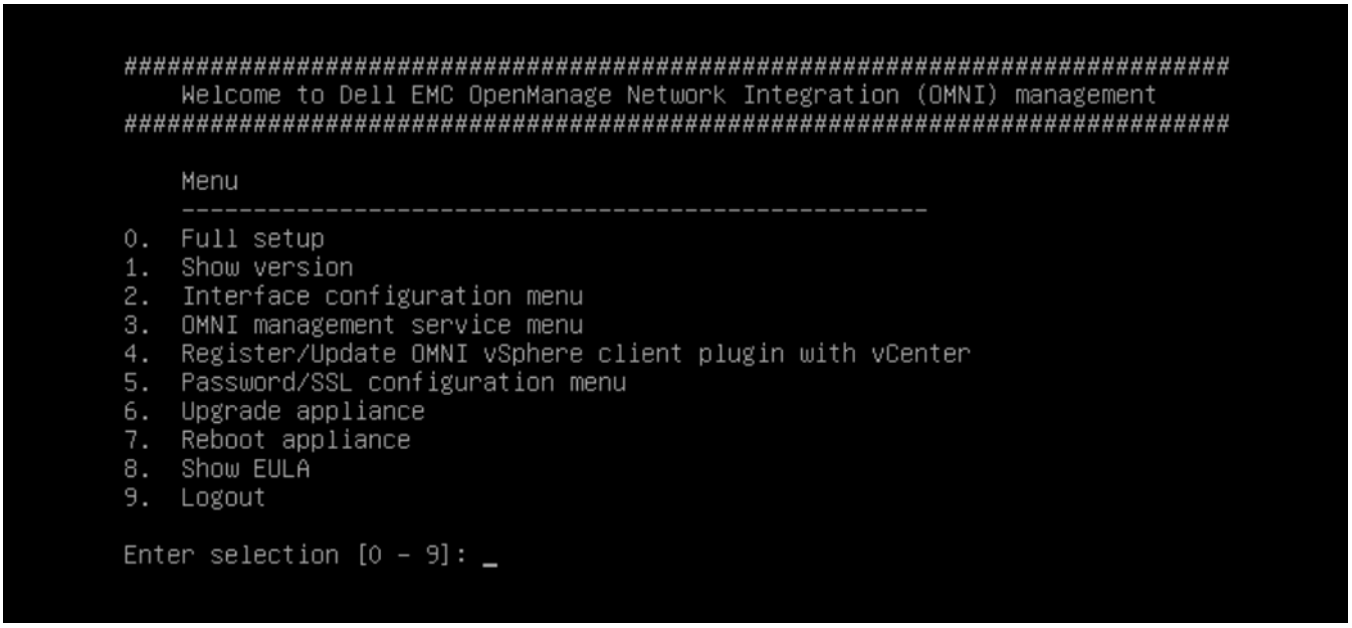
OMNI vCenter client plug-in registration

This information describes how to register the vCenter plug-in. SSL certificates have been automatically generated after the password is successfully updated. For more information, see Log into VM console.

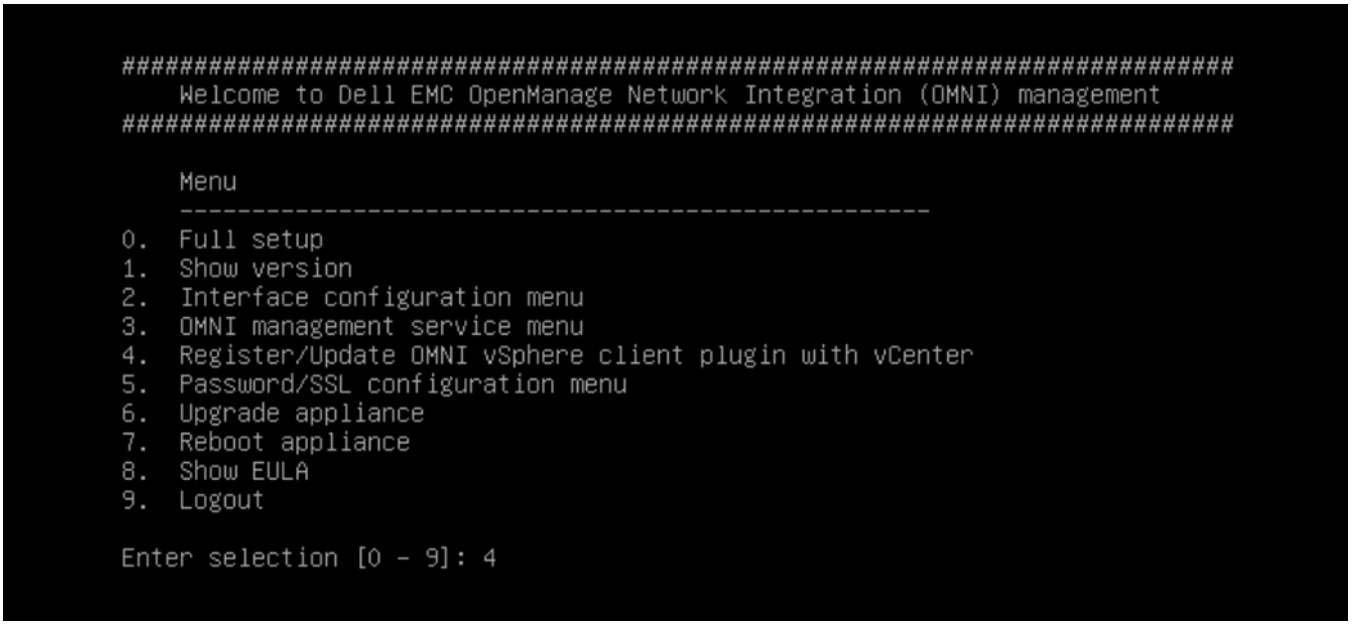
NOTE: Multiple OMNI instances cannot be mapped to a single vCenter instance. If a situation where multiple VxRail clusters exist with their own respective fabric instances, it is recommended to map these fabric instances to a single vCenter instance. For example, VxRail cluster1 ideally has its own vCenter-1 VM instance, and the same is true for VxRail cluster 2 with its own vCenter-2 VM instance. In this case, OMNI-1 maps to vCenter-1, and OMNI-2 maps to vCenter-2.

If you do not want to create individual OMNI to vCenter mappings, you do have the option of mapping multiple fabric instances to a single OMNI mapped to a single or primary vCenter instance.

1. Login to the OMNI management console.



2. Select **4. Register/Update OMNI vSphere client plugin with vCenter**.



3. Enter the OMNI IP or FQDN for registration with the vCenter instance.

NOTE: The recommendation is to use FQDN instead of the IP address of OMNI.

```
################################################################################
    Welcome to Dell EMC OpenManage Network Integration (OMNI) management
################################################################################

    Menu
    ------------------------------------------------
0.  Full setup
1.  Show version
2.  Interface configuration menu
3.  OMNI management service menu
4.  Register/Update OMNI vSphere client plugin with vCenter
5.  Password/SSL configuration menu
6.  Upgrade appliance
7.  Reboot appliance
8.  Show EULA
9.  Logout

Enter selection [0 - 9]: 4
2020-06-08 02:25:43 INFO  [setup.sh] Registering OMNI plugin with vCenter
OMNI IP/FQDN to use for registration: omni.st02.omni.vxrail
OMNI IP/FQDN : omni.st02.omni.vxrail
vCenter server FQDN:
```

4. Enter the vCenter Server FQDN, vCenter Server username, and vCenter Server password. Repeat this step to register each vCenter instance (up to 10).

```
################################################################################
    Welcome to Dell EMC OpenManage Network Integration (OMNI) management
################################################################################

    Menu
    ------------------------------------------------
0.  Full setup
1.  Show version
2.  Interface configuration menu
3.  OMNI management service menu
4.  Register/Update OMNI vSphere client plugin with vCenter
5.  Password/SSL configuration menu
6.  Upgrade appliance
7.  Reboot appliance
8.  Show EULA
9.  Logout

Enter selection [0 - 9]: 4
2020-06-08 02:25:43 INFO  [setup.sh] Registering OMNI plugin with vCenter
OMNI IP/FQDN to use for registration: omni.st02.omni.vxrail
OMNI IP/FQDN : omni.st02.omni.vxrail
vCenter server FQDN: internal-vc.st02.omni.vxrail
vCenter server username: administrator@vsphere.local
vCenter server password: _
```

5. The OMNI application server services start successful; press **[enter]** to continue.

```
################################################################################
    Welcome to Dell EMC OpenManage Network Integration (OMNI) management
################################################################################

    Menu
    ------------------------------------------------
0.  Full setup
1.  Show version
2.  Interface configuration menu
3.  OMNI management service menu
4.  Register/Update OMNI vSphere client plugin with vCenter
5.  Password/SSL configuration menu
6.  Upgrade appliance
7.  Reboot appliance
8.  Show EULA
9.  Logout

Enter selection [0 - 9]: 4
2020-06-08 02:25:43 INFO  [setup.sh] Registering OMNI plugin with vCenter
OMNI IP/FQDN to use for registration: omni.st02.omni.vxrail
OMNI IP/FQDN : omni.st02.omni.vxrail
vCenter server FQDN: internal-vc.st02.omni.vxrail
vCenter server username: administrator@vsphere.local
vCenter server password:
2020-06-08 02:28:14,662 Extension registration succeed with:
internal-vc.st02.omni.vxrail
press [enter] to go back to main menu...
_
```

6. Select **9. Logout**.

```
################################################################################
    Welcome to Dell EMC OpenManage Network Integration (OMNI) management
################################################################################

    Menu
    ------------------------------------------------
0.  Full setup
1.  Show version
2.  Interface configuration menu
3.  OMNI management service menu
4.  Register/Update OMNI vSphere client plugin with vCenter
5.  Password/SSL configuration menu
6.  Upgrade appliance
7.  Reboot appliance
8.  Show EULA
9.  Logout

Enter selection [0 - 9]: 9
```

NOTE: You cannot register the same vCenter instance from another OMNI plug-in.

For more information about how to unregister OMNI with vCenter, see Manage vCenter with OMNI.

4

OMNI vCenter integration

This information describes the OMNI vCenter integration to automate vCenter PortGroup VLANs.

vCenter VSS and DVS PortGroups

When you configure PortGroups of a virtual standard switch (VSS) with VLANs and distributed virtual switch (DVS) with VLANs on the OMNI registered vCenter, the respective active and standby physical adapter interfaces are automatically configured by OMNI on the SmartFabric ServerInterfaces. This is shown as tasks on the registered vCenter tasks pane.

NOTE: You cannot delete PortGroups on a VSS/DVS, or delete the VSS/DSS entirely as it clears all unused networks from the SmartFabric ServerInterfaces.

DVS provides an option to change the VLAN of uplink PortGroups. OMNI ignores PortGroup configuration if the VLAN type PortGroup is set to VLAN trunking or private VLAN.

We recommend keeping the DVS uplink in Trunking mode and configure the virtual PortGroups with VLANs for each network. OMNI configures the respective VLANs on the ToRs and SmartFabric uplinks.

OMNI automates the vCenter PortGroup VLAN and manages the registered vCenter by identifying the relation between the SmartFabric ServerInterface and the ESXi host PNIC MAC.

Identification of vCenter ESXi Host by OMNI

OMNI collects the PNIC MACs of all ESXi hosts in registered vCenters. If OMNI identifies the ServerInterface ID as a collected PNIC MAC (Id=MAC without ':') of the host, OMNI identifies that host to belong to an OMNI registered SmartFabric instance.

Table 5. vCenter PortGroup VLAN automation of identified ESXi host

vCenter action	SmartFabric action by OMNI
Add/update PortGroup: VLAN of VSS/DVS	• Create network of PortGroup VLAN and set Network Originator to Auto • Add network to SmartFabric ServerInterface
Remove PortGroup from VSS/DVS	Remove unused networks from SmartFabric ServerInterface

NOTE: OMNI automation is not designed to delete unused ServerInterfaces of SmartFabric.

SmartFabric networks consolidation by OMNI

1. Collect all networks of registered SmartFabric.
2. Collect networks of ServerInterface of registered SmartFabric.
3. Identify SmartFabric networks created by the OMNI user interface, and SmartFabric networks that are not created by the OMNI user interface.

   OMNI distinguish the origin of the network configured through vCenter or OMNI user by setting the Network Originator parameter.

   a. OMNI sets Network Originator to Manual when an user creates a network using OMNI UI.
   b. OMNI sets Network Originator to Auto when OMNI vCenter PortGroup automation creates a network.

4. Append networks that are not created by the OMNI user interface (all networks except the one that has `Network Originator` set to `Manual`) to SmartFabric uplink of the type `Default` or `CreateOnly`.

   OMNI automates network addition on one of the fabric uplinks. If you edit the network on the uplink using the OMNI UI and add or edit Network of Originator type `Auto`, the automation process may remove that network.

5. Find unused networks; SmartFabric networks not created by the OMNI user interface, and not used by the SmartFabric `ServerInterface` and SmartFabric uplinks.
6. Delete unused networks from the SmartFabric.

NOTE: The `Default` or `CreateOnly` uplink can be configured on the SmartFabric through the OMNI Uplink configuration page. For more information, see Configure and manage uplinks.

5

OMNI appliance console CLI menu

This information describes the menus available to the admin SSH user through the console.

Table 6. OMNI appliance console CLI menu

Menu option	Submenu option	Description
1. Show version	—	Display OMNI virtual appliance and plug-in version.
2. Interface configuration menu	1. Show interfaces	Display OMNI network interface configuration.
	2. Show connection status	Display OMNI network interface connection status.
	3. Configure interfaces	Configure OMNI network interfaces using Network Manager user interface (nmtui) including OMNI Management IP, gateway, DNS entries, search domains, routes, OMNI hostname, and so on.
	4. Show NTP status.	Display OMNI network time protocol (NTP) server status.
	5. Configure NTP server.	Configure OMNI NTP server. Enter remote NTP server IP or hostname. **It is recommended that you use the server hostname**.
	6. Unconfigure NTP server.	Unconfigure OMNI NTP server.
	7. Start NTP server.	Start OMNI NTP service, and enable NTP service.
	8. Stop NTP server.	Stop OMNI NTP service.
	9. Exit	—
3. OMNI management service menu	1. Start OMNI management service.	Start OMNI web and database essential services.
	2. View OMNI management service	Display status of OMNI essential services.
	3. Stop OMNI management service.	Stop OMNI essential services.
	4. Restart OMNI management service.	Restart OMNI essential services.
	5. Create support bundle.	Create OMNI support bundle archive and save to download location. **It is recommended that you use the OMNI appliance management user interface to generate and download support bundle**.
	6. Change application log level	Display current log-levels, and configure DEBUG or ERROR log-levels. **It is recommended that you use the OMNI appliance management user interface to change log level of needed services**.

Table 6. OMNI appliance console CLI menu (continued)

Menu option	Submenu option	Description
	7. Exit	—
4. Register or update OMNI vSphere client plug-in with vCenter	—	Register OMNI with vCenter; enter OMNI IP or hostname, vCenter IP or hostname, vCenter administrator user (administrator @vsphere.local), and vCenter password. **It is recommended that you register OMNI appliance user interface with one or multiple vCenters**.
5. Password or SSL configuration	1. Change appliance password	Change appliance `admin` user password.
	2. Change root password	Assign password of application root user; root user is disabled by default, and is required to set the password first to access the root user. **Root user is only accessible using the vCenter OMNI VM console**. **CAUTION: Changing the system state from the Linux shell can result in undesired and unpredictable system behavior. Only use Linux shell commands to display system state and variables, or as instructed by Dell EMC Support.**
	3. Generate self-signed SSL certificates.	Replace existing OMNI appliance self-sign certificate. **After SSL certificate installation completes, you need to re-register OMNI with the vCenter**.
	4. Install SSL certificates from remote server.	Replace OMNI certificates with the certificate that is on the remote server using SCP or FTP. **After SSL certificate installation completes, you need to re-register OMNI with the vCenter**.
	5. Exit	—
6. Upgrade appliance	—	Upgrade the OMNI appliance.
7. Reboot appliance	—	Reboot the OMNI appliance.
8. Show EULA	—	Display the OMNI end user license agreement (EULA).
9. Logout	—	Log out as the `admin` user.

OMNI appliance page displays links to launch the OMNI Appliance Management UI, OMNI Fabric Management Portal, and OMNI Documentation. Open a browser session, **https://*OMNI_IP*/** with the IP address or FQDN of the OMNI VM.

OMNI Appliance Management user interface

From OMNI 1.3 release, manage all the system, web, and automation services running in the OMNI using a new UI—OMNI Appliance Management.

OMNI Appliance Management provides flexibility to manage each of the automation services running in the OMNI appliance, by allowing you to start, stop, and restart the OMNI services individually. See Related videos section for more information.

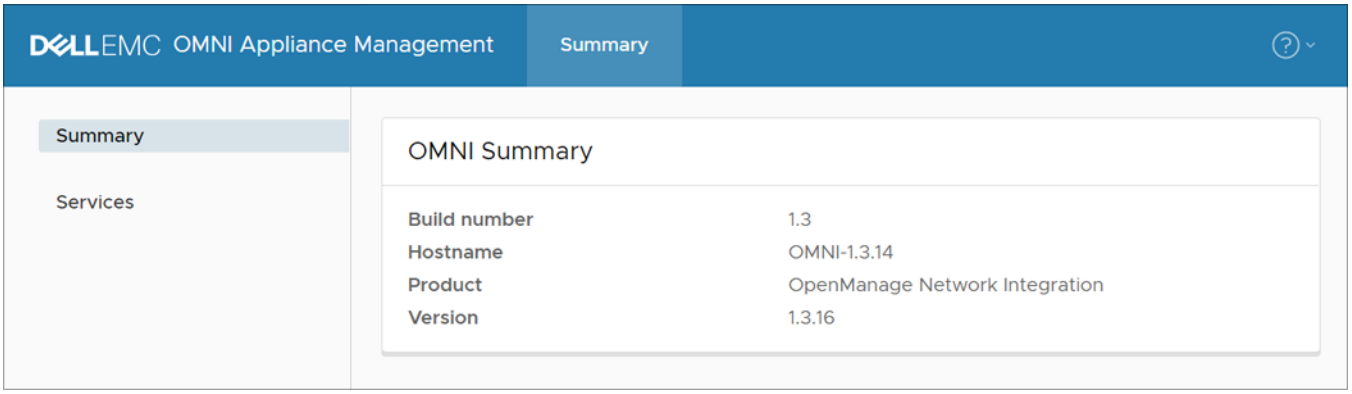
After you create the OMNI virtual appliance and complete the virtual appliance setup, launch the OMNI appliance management UI.

To access the OMNI Appliance Management UI:

Open a browser session, go to **https://*OMNI_IP*/omni** with the IP address or hostname of the OMNI VM that is configured during the initial setup.

NOTE: Access OMNI Appliance Management UI only with OMNI VM appliance administrator credentials.

View OMNI Appliance Management summary



Summary displays:

- Build number—Displays the OMNI build number information.
- Hostname—Displays the hostname configure during OMNI setup.
- Product—Displays the name of the VM appliance that is registered with the vCenter.
- Version—Displays the version of the OMNI VM build.

Manage OMNI services

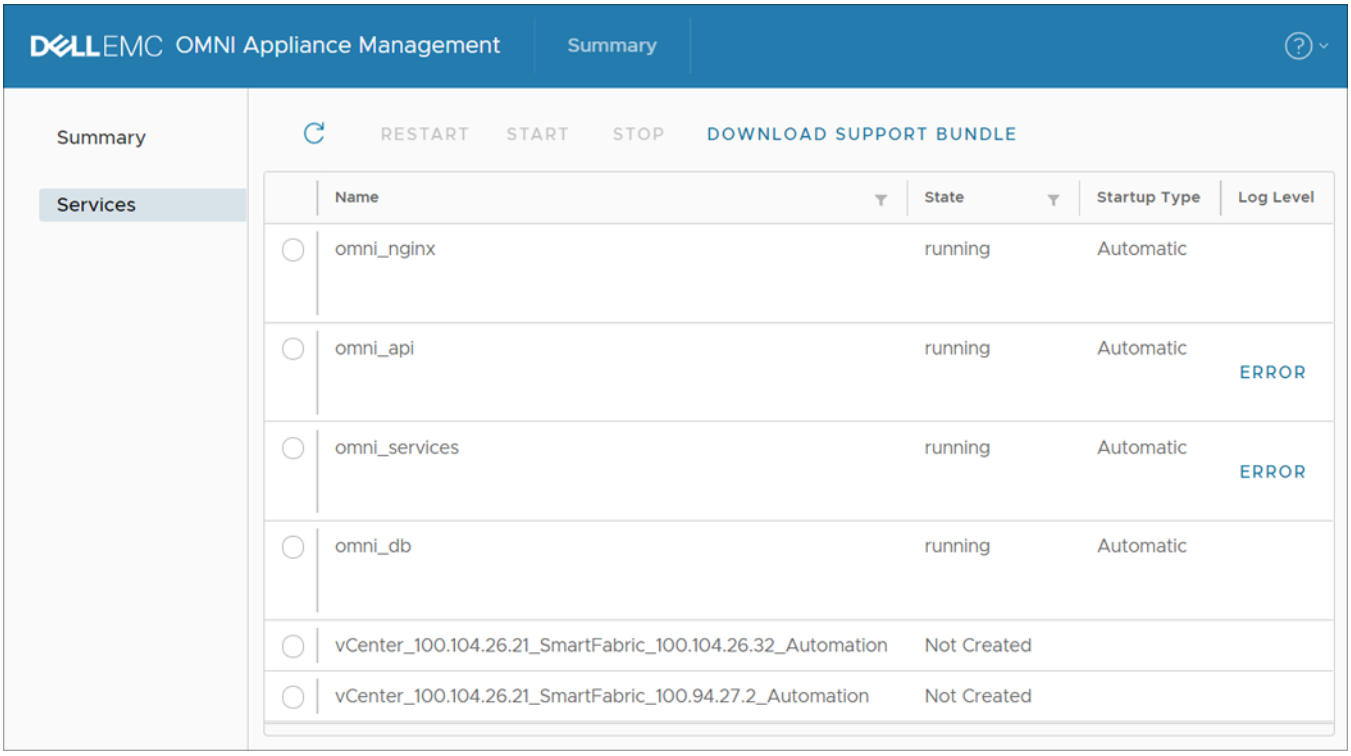
By default, the web and database essential services start automatically, and the services must be in running state. Once you complete the OMNI virtual appliance setup by adding the SmartFabric service instances and register the relevant vCenters, the system creates individual fabric automation services. The automation services are created based on the combination of the number of vCenters registered and the SmartFabric service instances that are managed by the OMNI appliance. For example, if OMNI appliance has two service instances and two registered vCenters, the system displays four automation services.

List of OMNI services:

Table 7. List of OMNI services

Service	Function	States
`omni_api`	Service serving REST APIs for OMNI Fabric Management interface	Can restart the services.
`omni_services`	Orchestration service that provides APIs to start, stop, and manage all OMNI services.	
`omni_db`	Database service that stores crucial information	Cannot restart, start, or stop the services.
`omni_nginx`	Web server service that manages all incoming and outgoing web requests.	
Automation services	Automation services running between vCenter and SFS	Can start, stop, or restart individual automation services anytime.

Services menu displays the list of OMNI management and automation services running on the OMNI appliance. Select the automation service of the relevant vCenter and SmartFabric combination and start the services manually. Also start, stop, and restart the automation services individually.

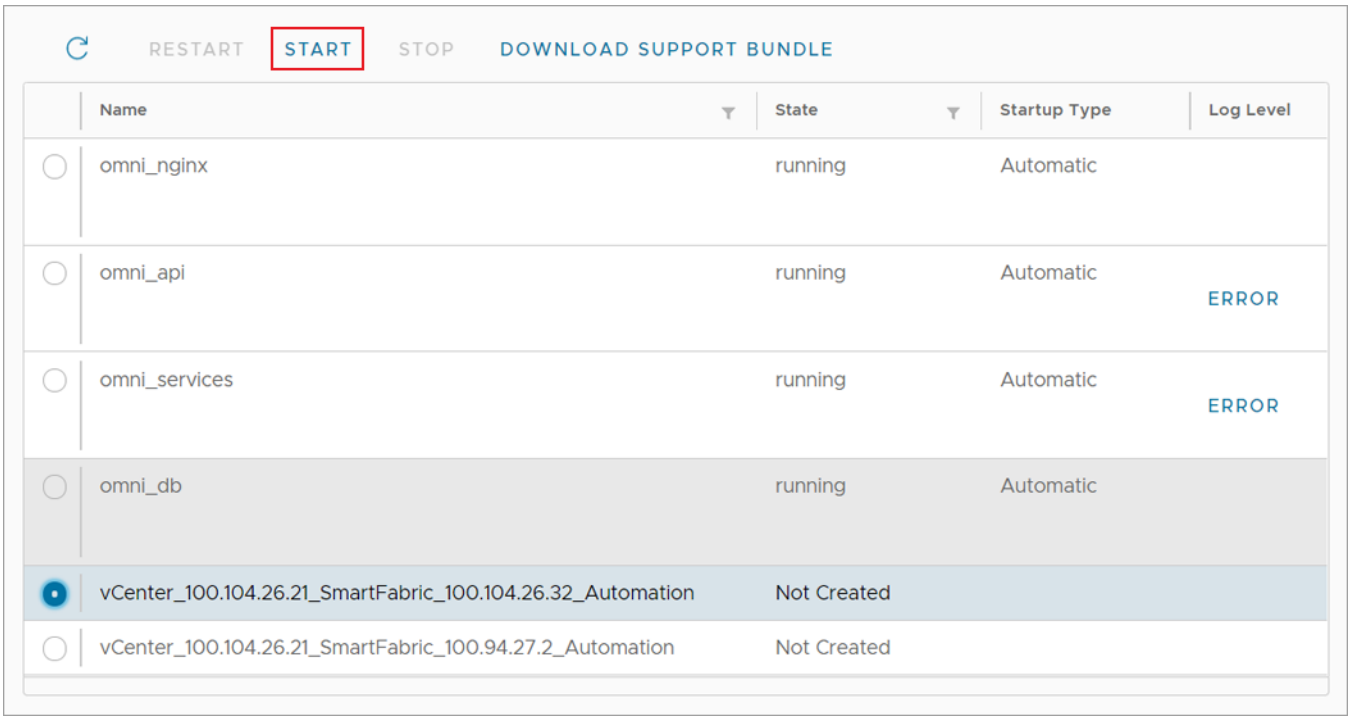


Click **Refresh** icon to update the data and display the updated contents.

Start fabric automation services

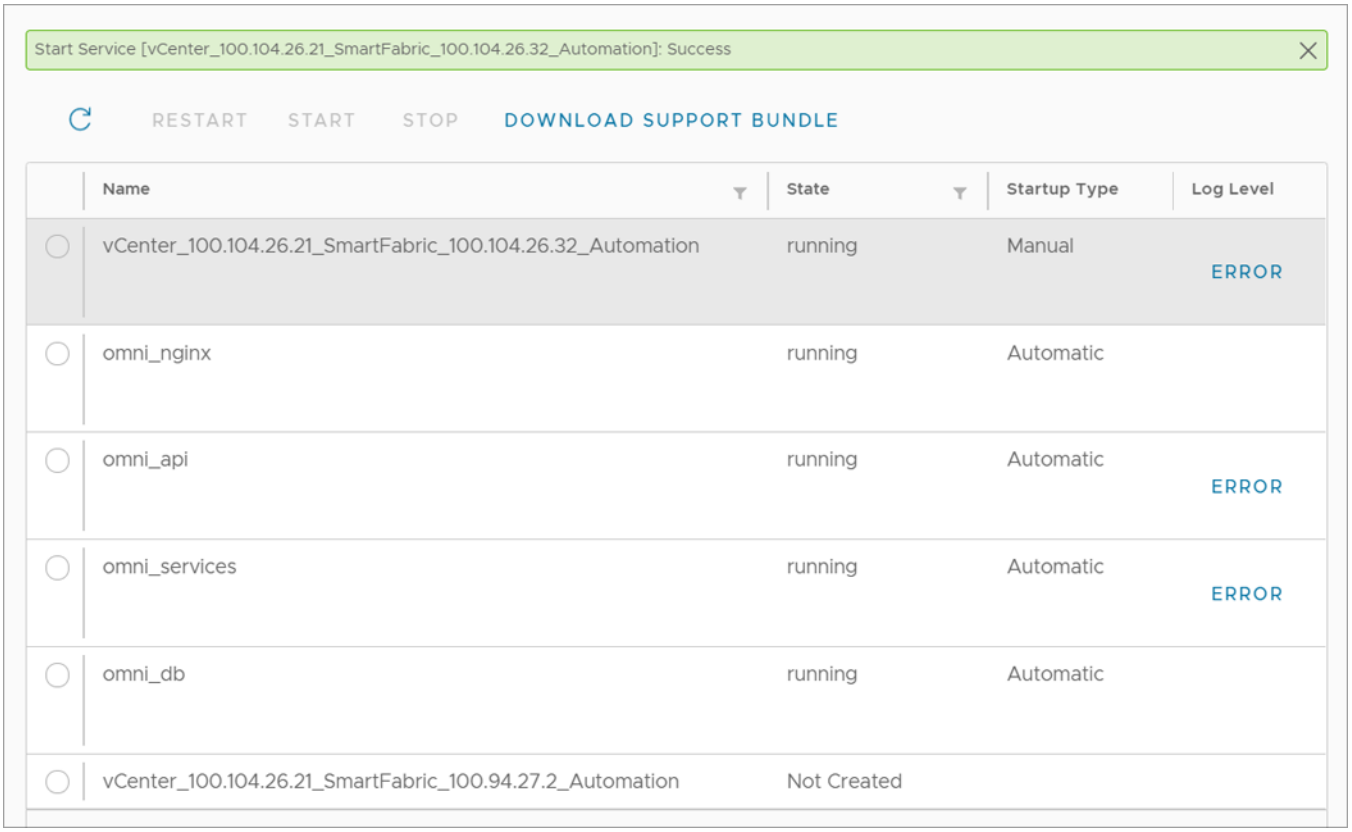
To start the fabric automation services:

1. From the **OMNI Appliance Management** UI, click **Services** tab menu.
2. Select the automation service that you want to start, and click **Start**.



After you start the service, OMNI starts monitoring the networking events for the registered service instance.

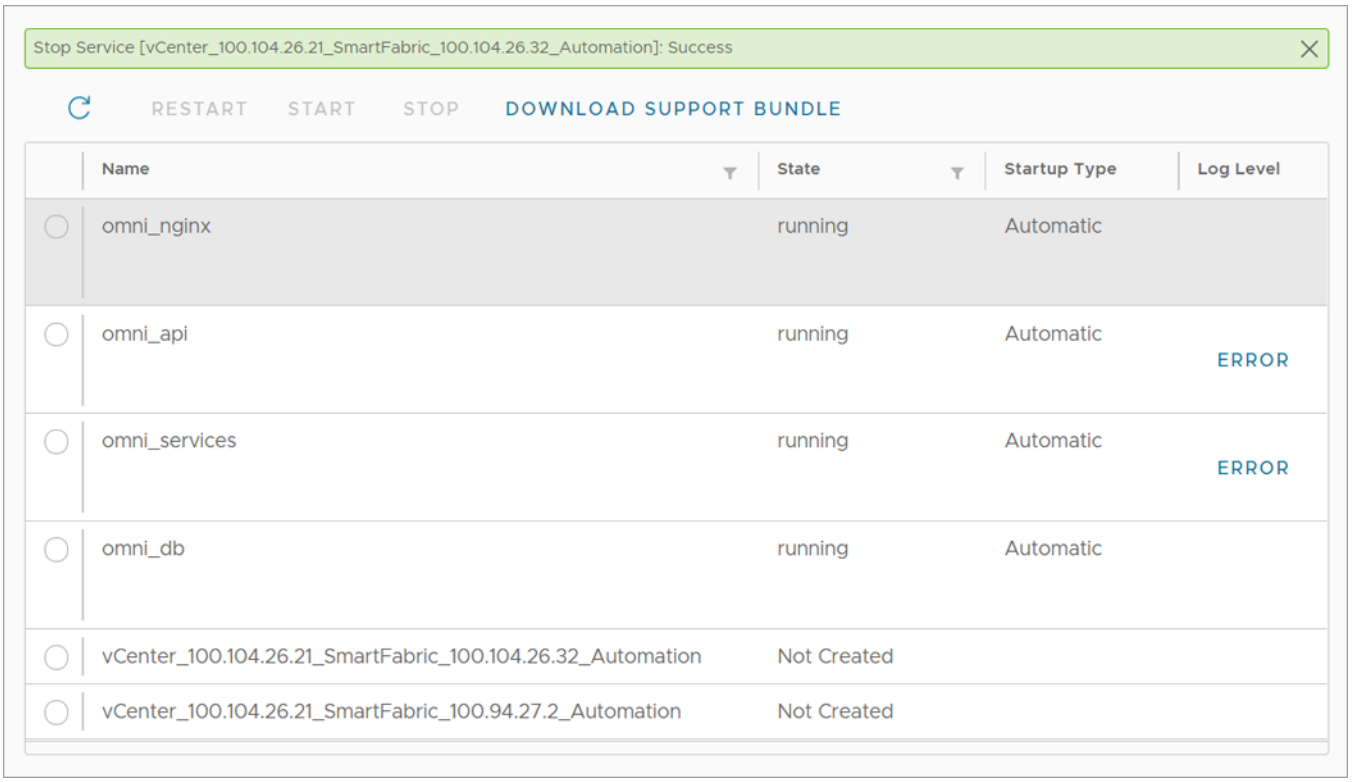
3. The system displays start service success message.



Stop fabric automation services

To stop the fabric automation services:

1. Select the relevant automation service that you want to stop, and click **Stop**.



2. The system displays stop service success message.

To restart the fabric automation service, select the relevant automation service, and click **Restart**.

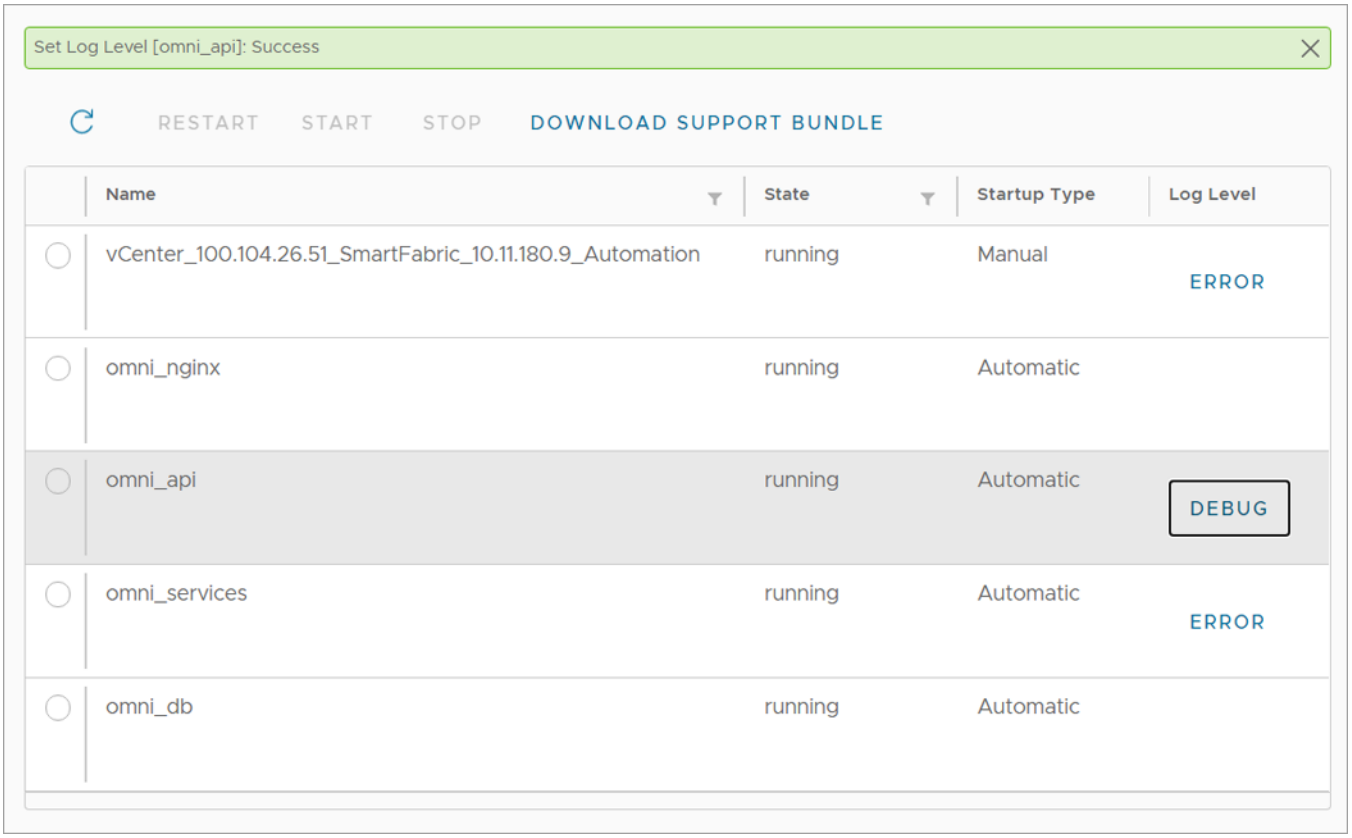
View the status of automation service in the OMNI VM **Home** page, see View vCenter Host Automation status.

Download Support Bundle

1. Support options are used for debugging. If there is an issue, download a support bundle containing all the logs that are found in OMNI. Also change the log-level of OMNI to collect logs of different types.

   When the log-level of OMNI is set to ERROR, the system records the error logs. When the log-level is set to DEBUG, error logs and logs with additional information is recorded. Use the DEBUG level when you want to diagnose an issue.

2. (Optional) Click **Error** under log-level of each service to modify the log-level to **Debug**.



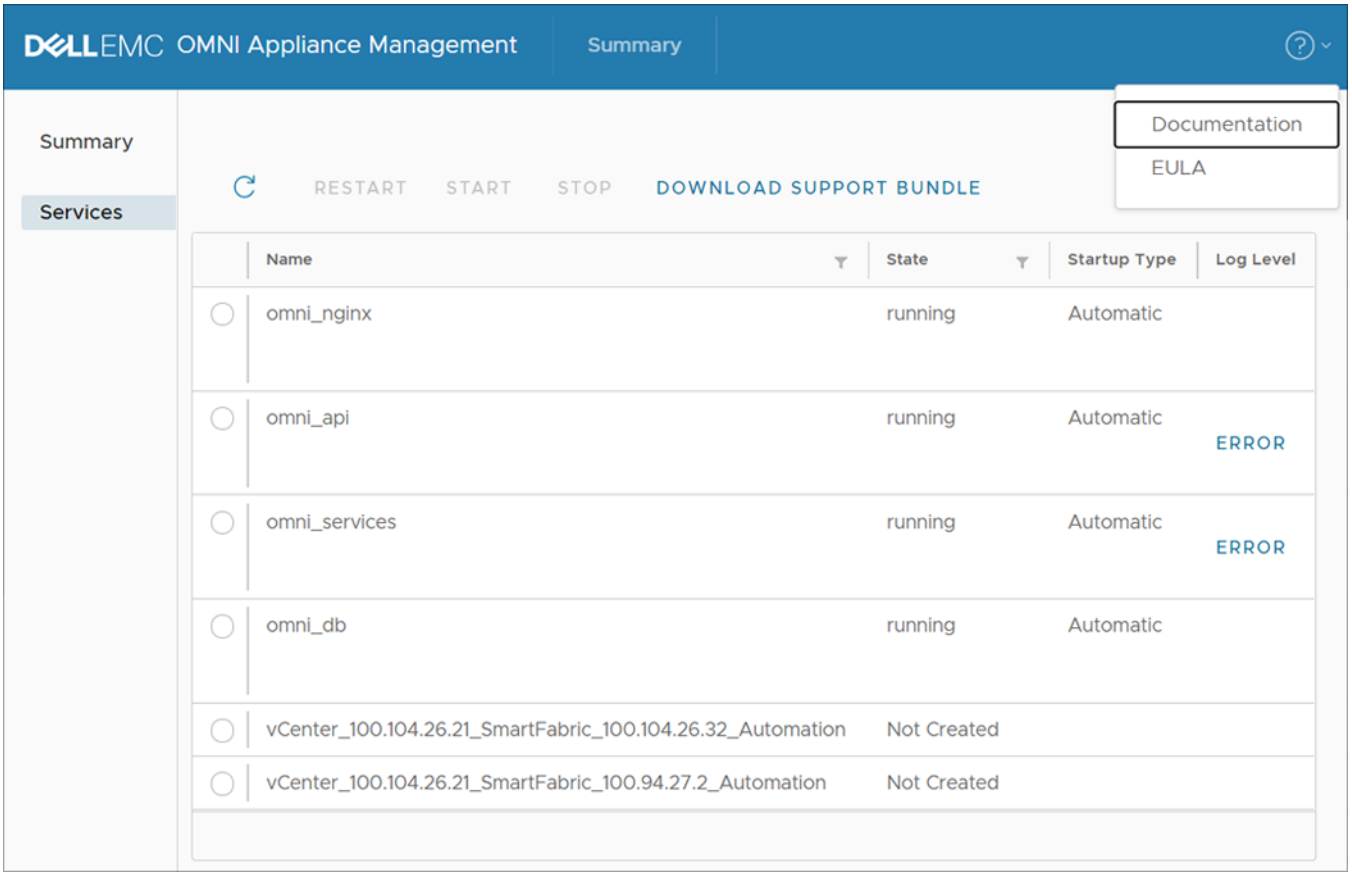
   The system displays set log level success message.

3. (Optional) Click **Debug** under log-level of each service to modify the log-level to **Error**.

   The system displays set log level success message.

Help links

Use the help icon to access the link to Dell EMC documentation support page. Also view the end-user license agreement (EULA) using the help icon.



Related Videos

OMNI Appliance Management UI

6

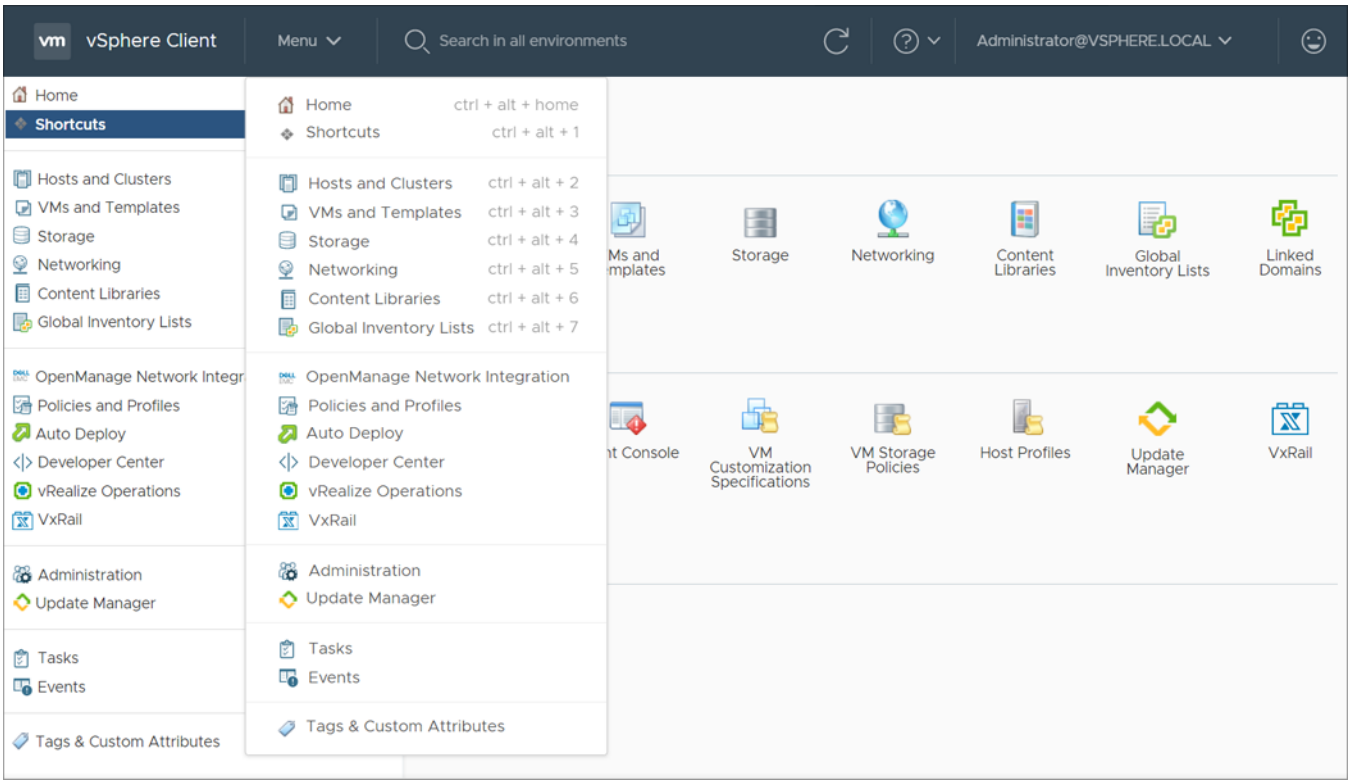
Access to OMNI Fabric Management Portal

This information describes how to access SmartFabric vCenter through the vSphere Client. A shortcut is available from the vSphere Client left-pane within the menu drop-down and shortcuts view.

Access OMNI portal using registered vCenter

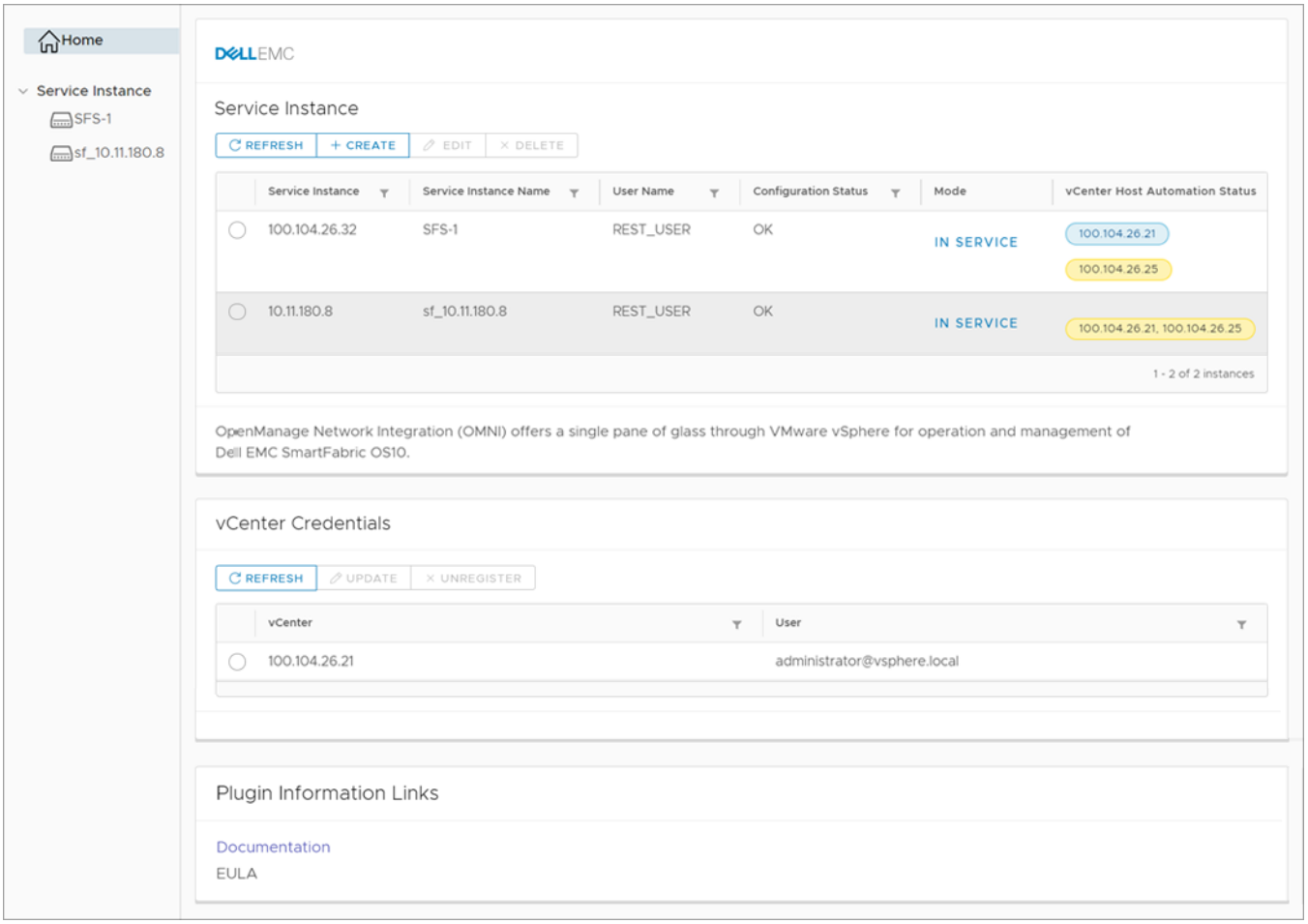
Before you use the plug-in, you must set up an OMNI appliance in vSphere. Once you register OMNI with vCenter, an OMNI plug-in is available in the vCenter.

NOTE: vCenter 7.0 supports plug-in autodiscovery feature. So, when you register or unregister OMNI 1.3 appliance with vCenter 7.0, refresh the browser to view the OMNI UI plug-in from the vCenter. For OMNI 1.3 with older versions of vCenter, log out and log in to access the plug-in from the vCenter.



When you select SmartFabric, the home page displays information about the SmartFabric domains being managed. This page also allows you to update extensions if available. Information includes:

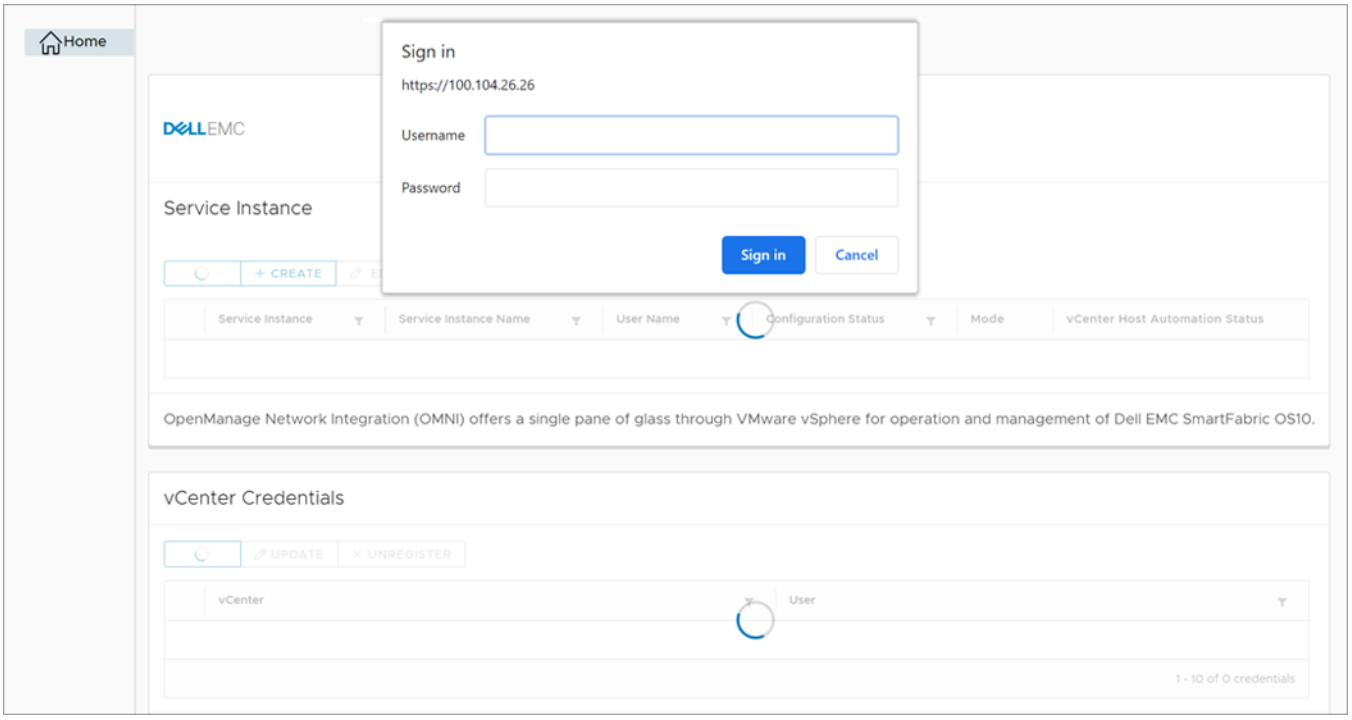
- Service instance
- vCenter credentials



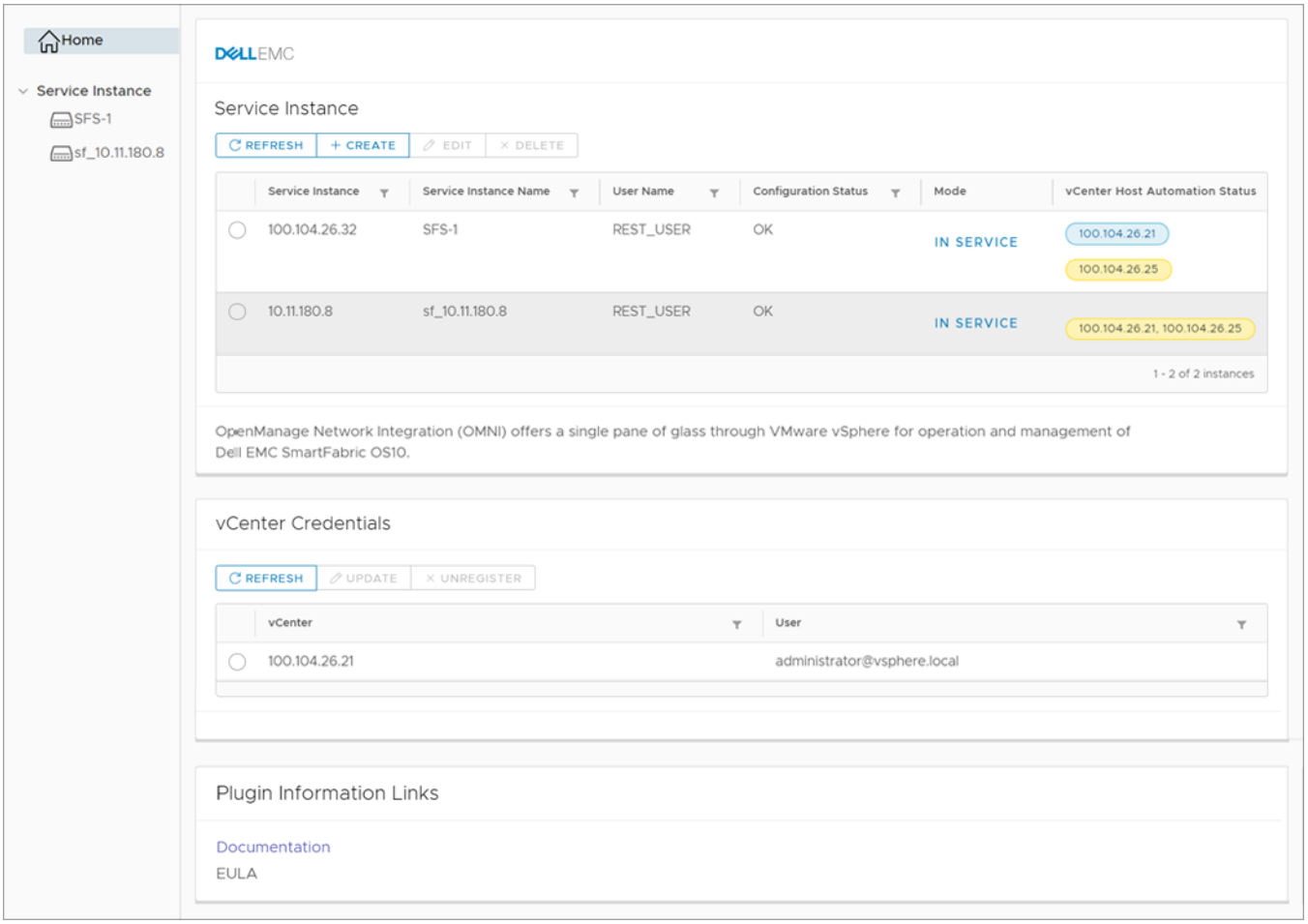
Access OMNI portal using the OMNI IP address

Once the vCenter registration steps are complete, you can log in to the OMNI UI using the OMNI stand-alone page. This information describes how to access the OMNI UI from a browser.

1. Open a browser session, go to **https://*OMNI_IP*/delawareos10** with the IP configured during setup.
2. Enter the **username** and **password** for the OMNI VM, then click **Sign In**.



Once the username and password are authenticated, the OMNI page displays.



OMNI Fabric Management Portal

Once you log in to the OMNI UI using the OMNI appliance IP, you can use the OMNI to manage the SmartFabric instances.

From the **Home** page, you can:

- Add a SmarFabric instance manually.
- Configure OMNI autodiscovered SmartFabric instance.
- Enable or disable OMNI Maintenance mode.
- View the vCenter host automation status.
- Manage vCenter with OMNI.
- View Plugin information links.

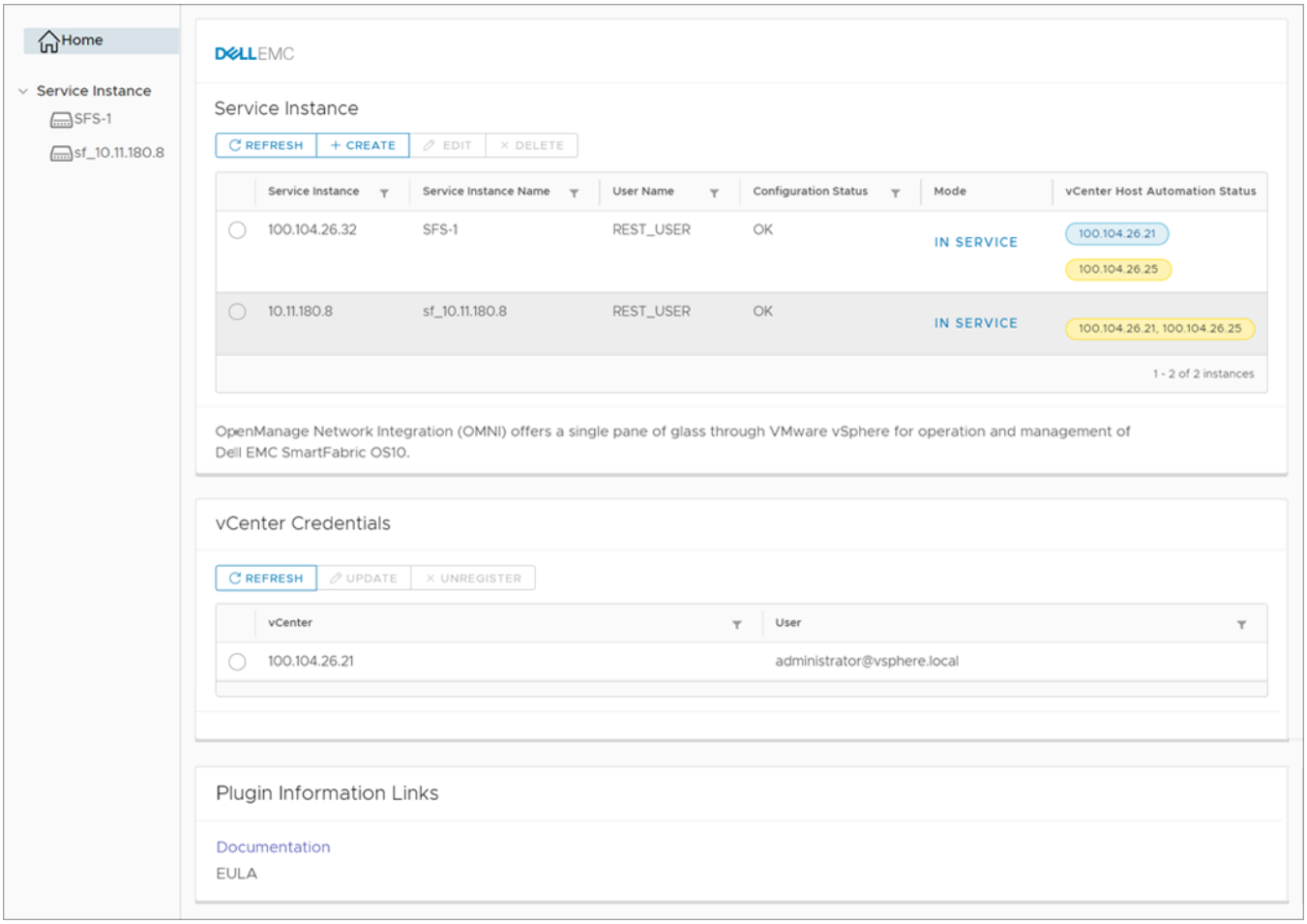
Add SmartFabric instance

This information describes how to add SmartFabric instances in OMNI.

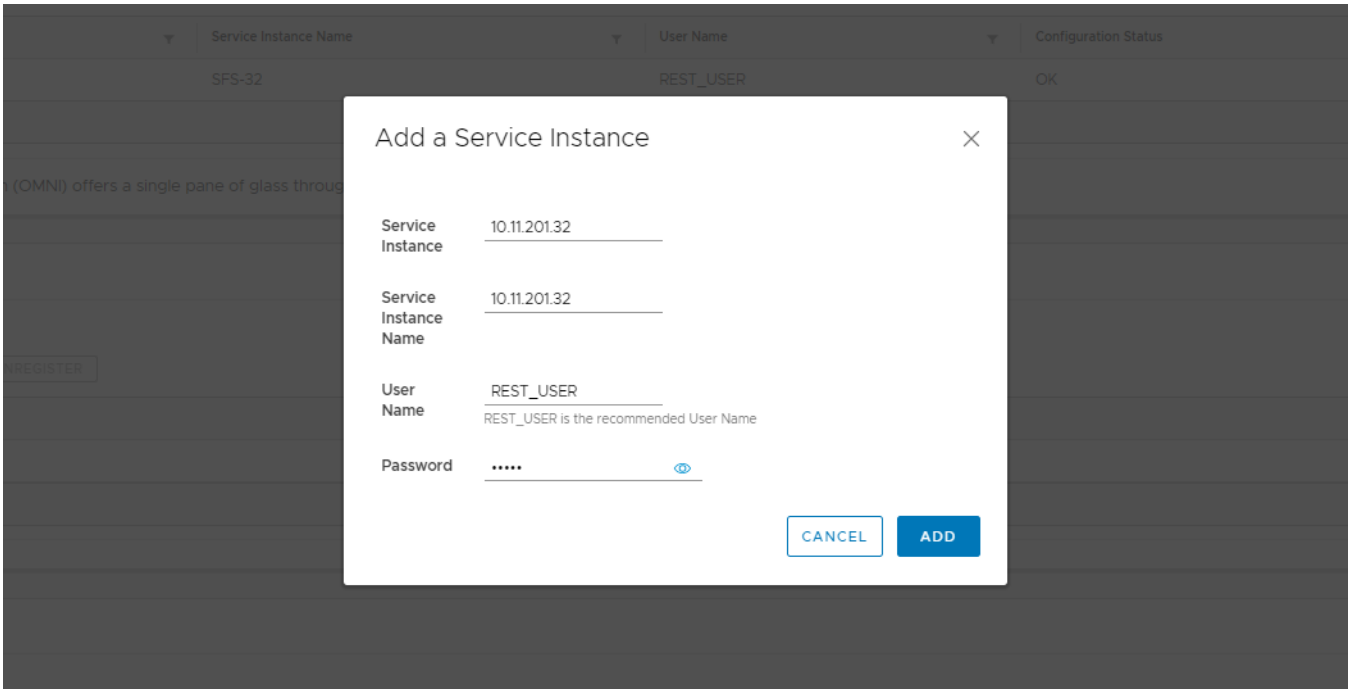
1. Identify the master IP address of the switch in a SmartFabric cluster. To identify the master, use the `show smartfabric cluster` command in the OS10 switch CLI.

```
OS10# show smartfabric cluster

-------------------------------------------------------------
CLUSTER DOMAIN ID : 100
VIP               : fde2:53ba:e9a0:cccc:0:5eff:fe00:1100
ROLE              : MASTER
SERVICE-TAG       : FX6HXC2
MASTER-IPV4       : 10.11.180.8
PREFERRED-MASTER  : true
-------------------------------------------------------------
```

2. Go to the OMNI portal.
3. From **Service instance** pane, click **Create** to manually add the master IP address of the SmartFabric Service instance.



4. Enter the service instance name, username, and password. Click **Add**.



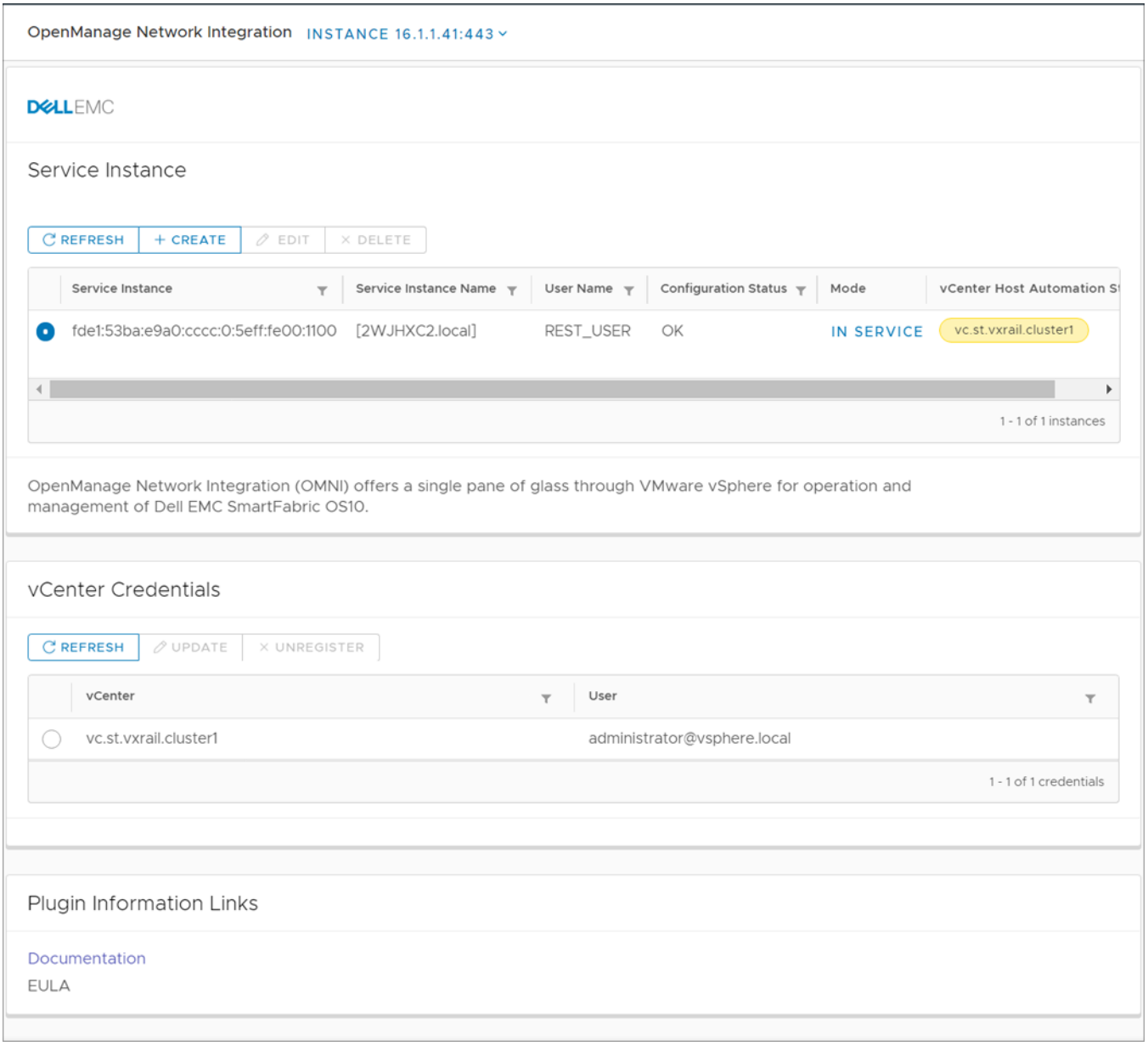
5. The system displays service instance creation success message.

Configure OMNI autodiscovered SmartFabric instance

This information describes how to configure OMNI autodiscovered SmartFabric instances. If the OMNI virtual appliance is connected to a link-local network on SmartFabric (such as VxRail Management Network-VLAN 3939), find the SmartFabric IPv6 VIP autodiscovered by OMNI. For complete information about discovery, see *mDNS service* in Fabric creation.

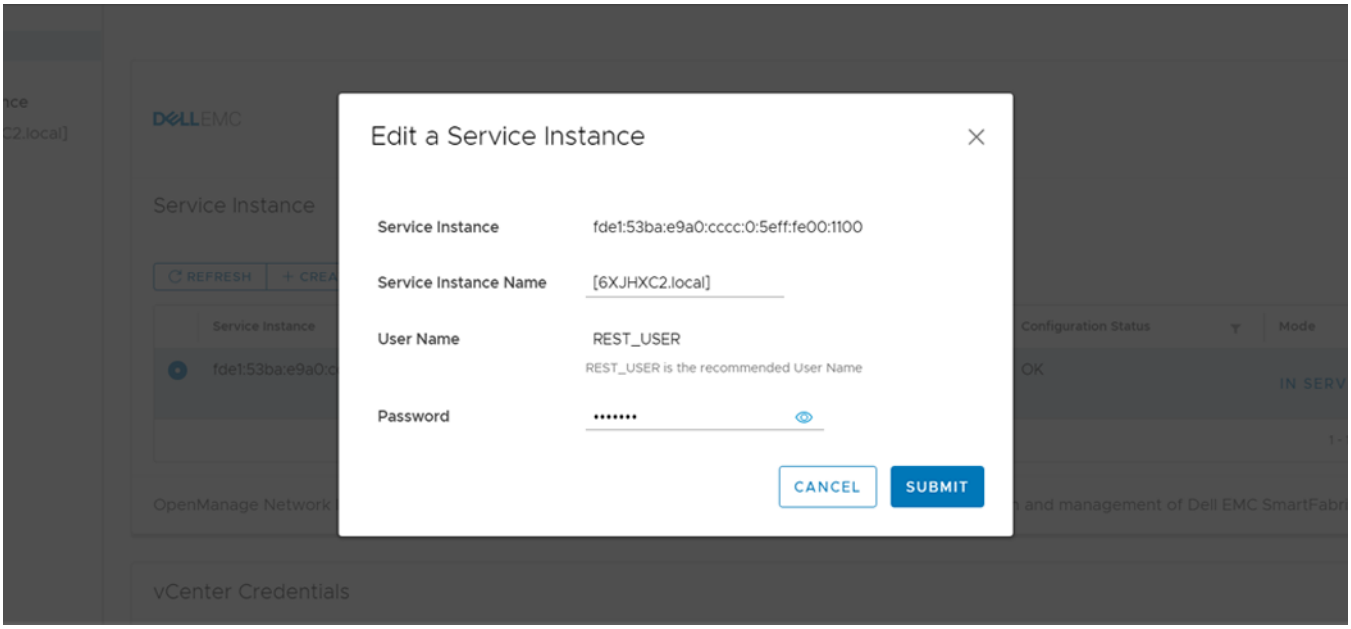
Edit the autodiscovered SmartFabric instance for the REST_USER password to complete the configuration.

1. Go to the OMNI portal.
2. Select **Auto Discovered VIP**, and click **Edit**.



NOTE: During VxRail initial deployment, the system forces you to change the password. If you forget the REST_USER password, contact Dell support to reset REST_USER password.

3. Enter the service instance information, then click **Submit**.



NOTE: After you configure the SmartFabric instance, start the fabric automation services from the OMNI appliance management User Interface (UI).

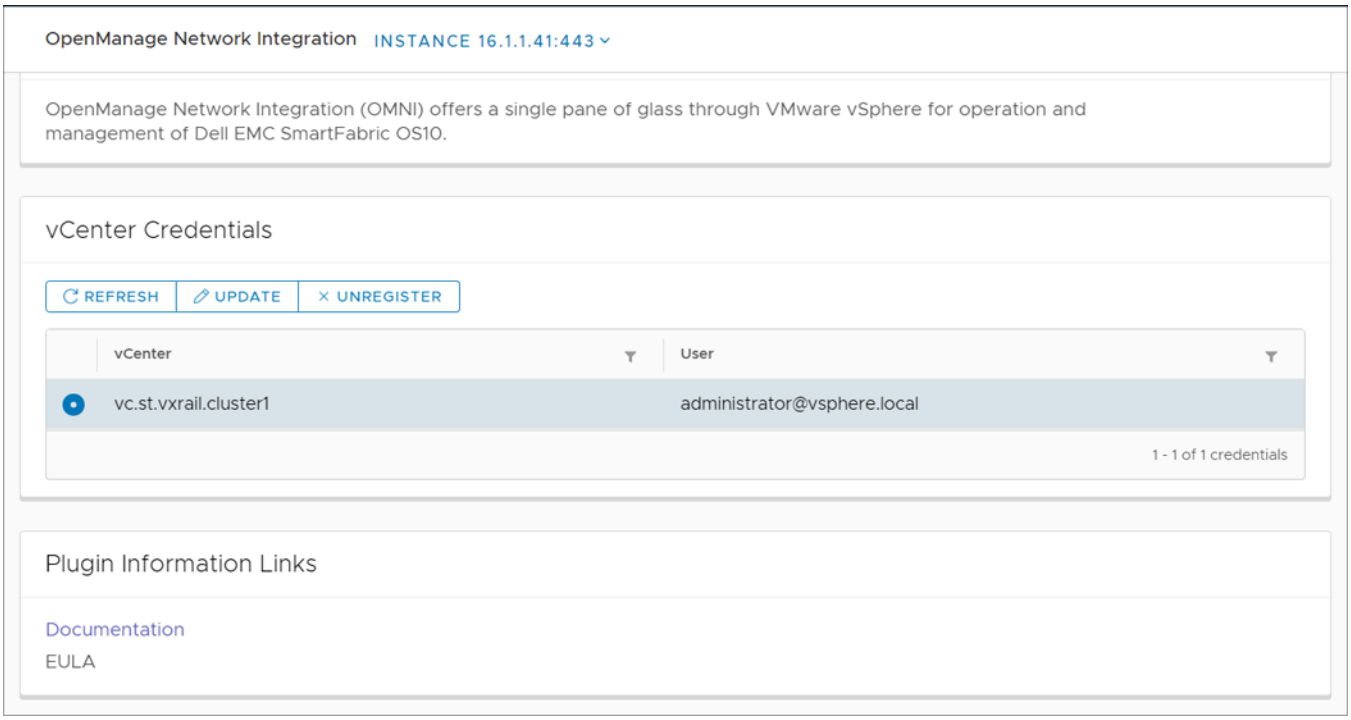
4. The system displays service instance configuration success message.

Manage vCenter with OMNI

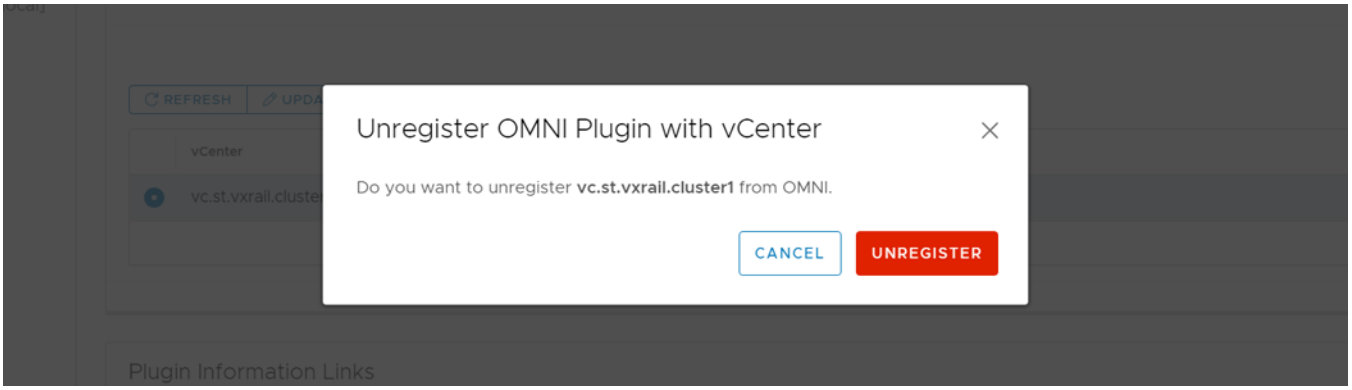
You can unregister vCenter and manage vCenter credentials with OMNI.

Unregister vCenter with OMNI

1. From the **Home** page, go to **vCenter Credentials** pane.



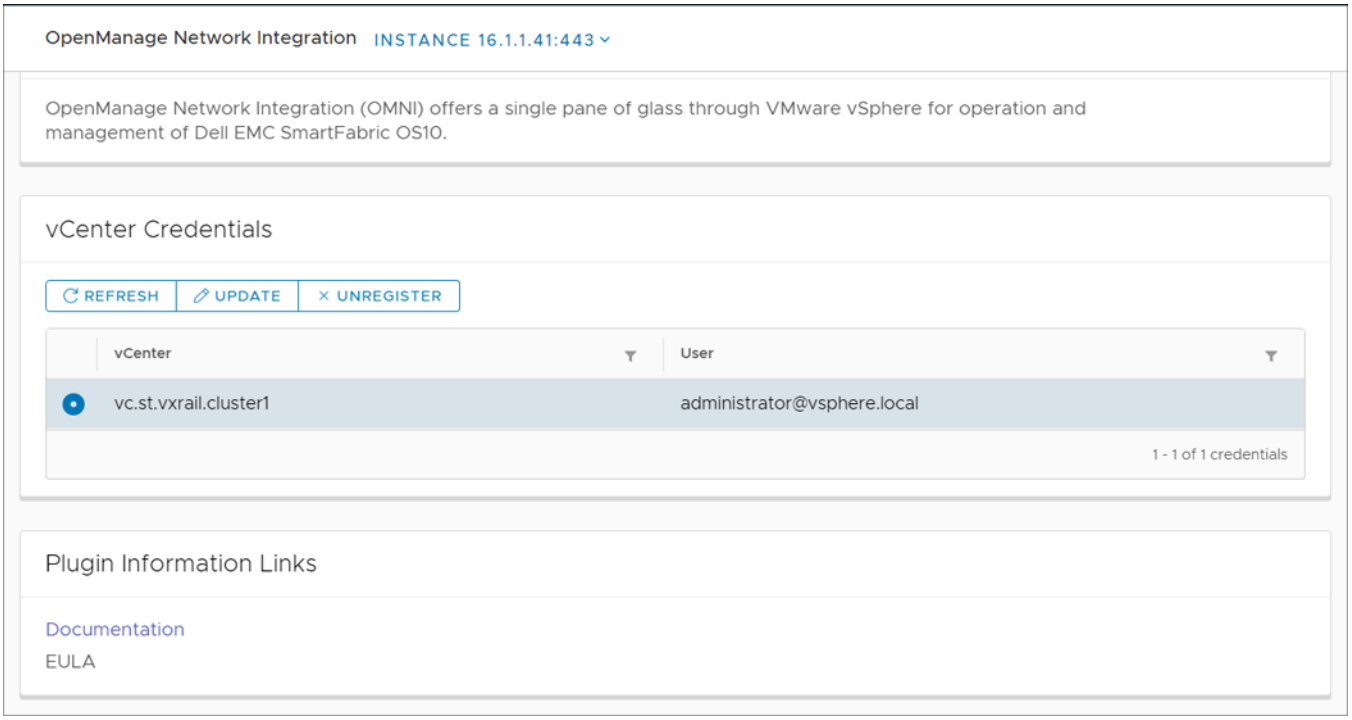
2. Select the vCenter from the list, and click **Unregister**.



3. Click **Unregister** to confirm.

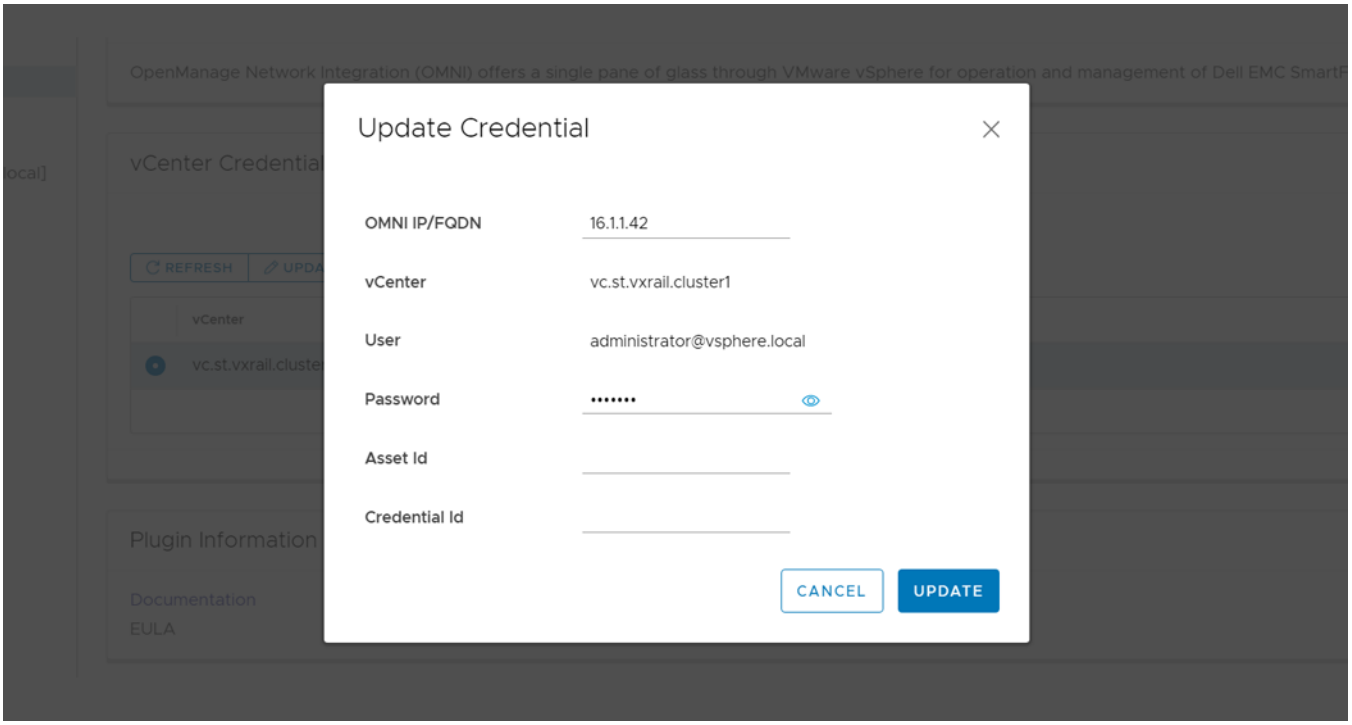
Update the credential of the registered vCenter

1. Select the existing vCenter from the list, and click **Update** to update the credentials.



Update Credential window appears.

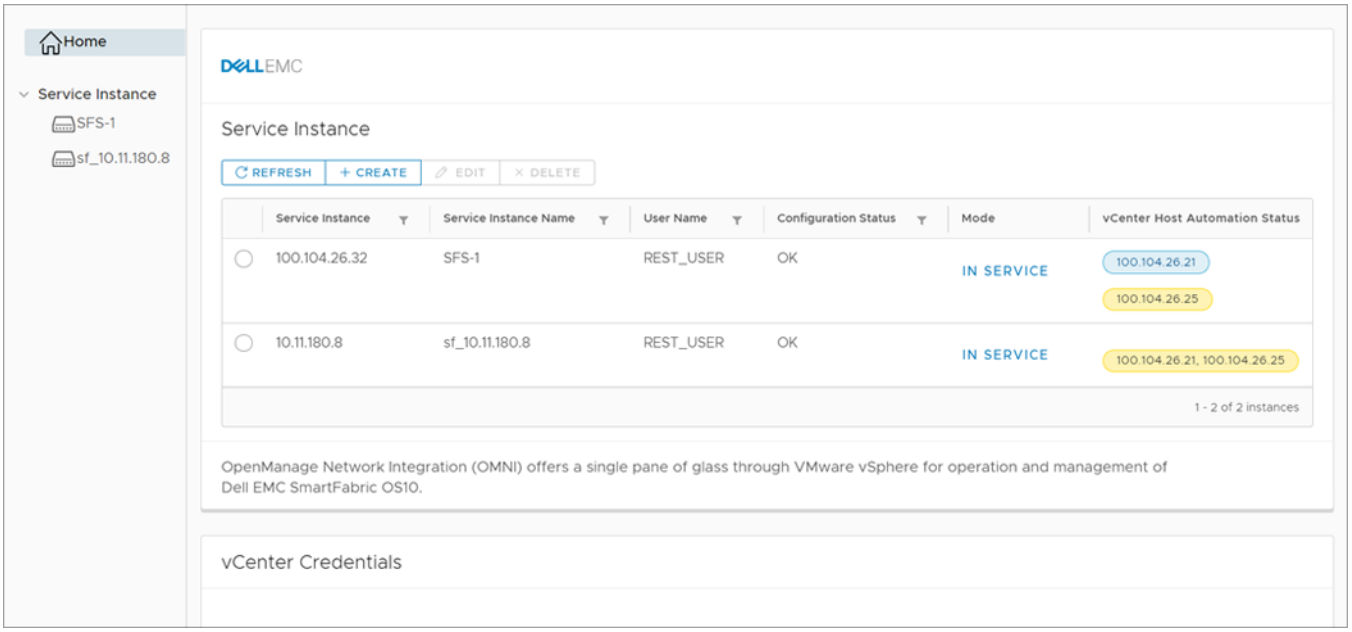
2. Enter the required information to edit (user and vCenter fields are automatically populated), then click **Update**.



3. The system displays an update success message.

Enable and disable OMNI Maintenance mode

The OMNI Fabric Management portal **Home** page displays the mode of each service instance in the OMNI VM.



Enabling Maintenance mode disables zero-touch automation for all SmartFabric instances. Enabling Maintenance mode prevents OMNI from configuring networks on SmartFabrics when there are changes in the vCenter port groups.

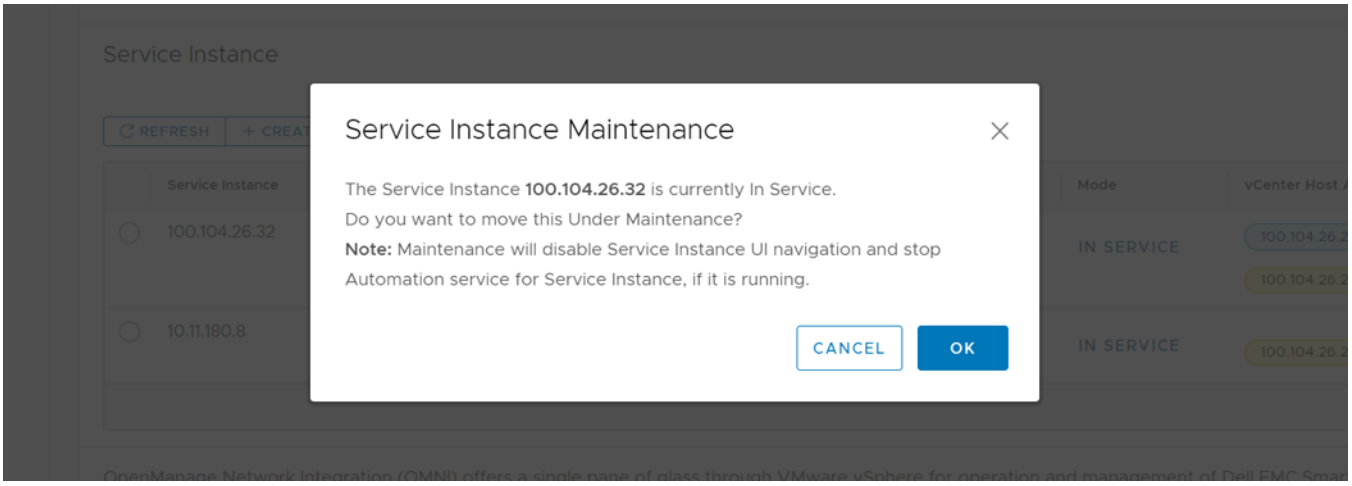
Enable Maintenance mode

To enable Maintenance mode for a service instance:

1. From the **Home** page, under **Service Instance**, click **In Service** for a specific service instance from the

   NOTE: Enabling Maintenance mode disables all the Service Instance UI navigation and stops the automation services that are running for the service instance.

2. Click **Ok** to confirm.



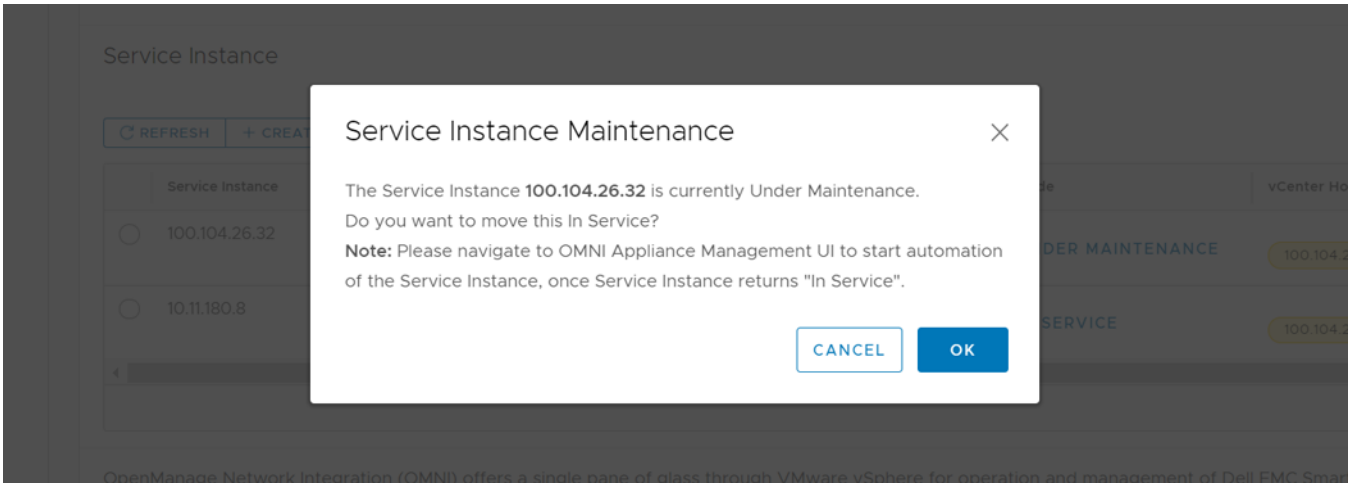
3. The system displays Maintenance mode change success message.

Disable Maintenance mode

To disable Maintenance Mode for a service instance:

1. From the **Home** page, under **Service Instance**, click **Under Maintenance** for a specific Service Instance from the list.

   Click **Ok** to confirm.



   NOTE: Once the status changes to **In Service**, go to the OMNI Appliance Management UI to start the relevant automation services.

2. Click to confirm.
3. The system displays Maintenance mode change success message.

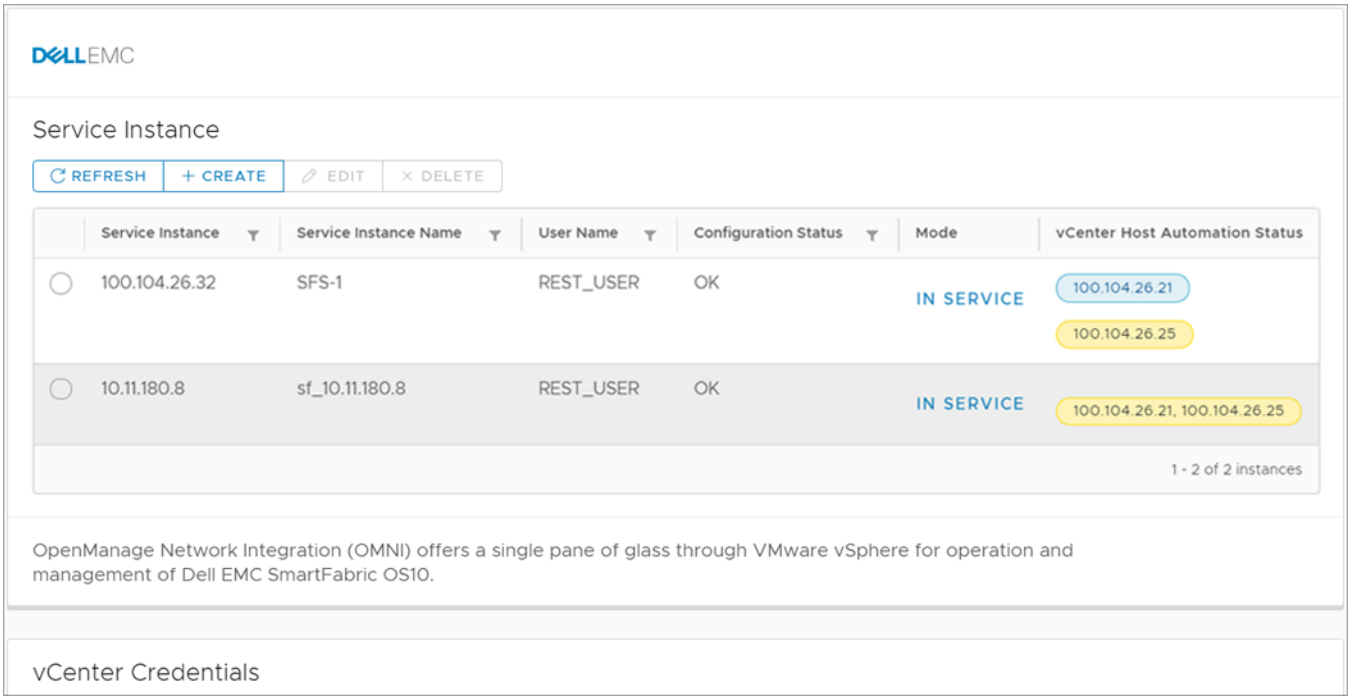
View vCenter host automation status

OMNI appliance **Home** page displays the vCenter host automation status. **vCenter Host Automation Status** displays the list of all automation services available for the service instance and the status of the automation services for the vCenter host.

OMNI VM represents the status of automation service for the vCenter host using color.

- Blue—Automation service is running.
- Yellow—Automation service is not started.

Also check the status of vCenter host services by placing the cursor on the list.

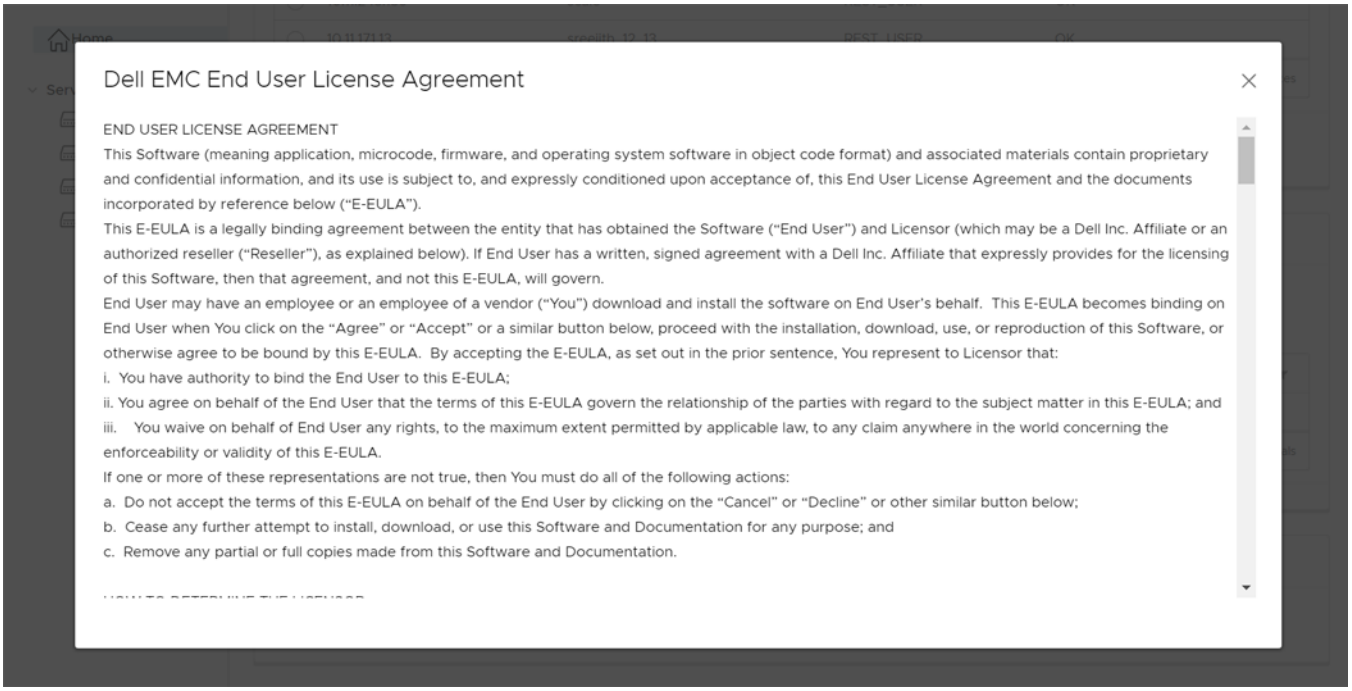


Plugin information links

You can view the links to documentation and end-user license agreement (EULA).

1. **Plugin Information Links** has links to:
   - Documentation
   - End User License agreement

2. Click **EULA** to view the Dell EMC End User License Agreement.



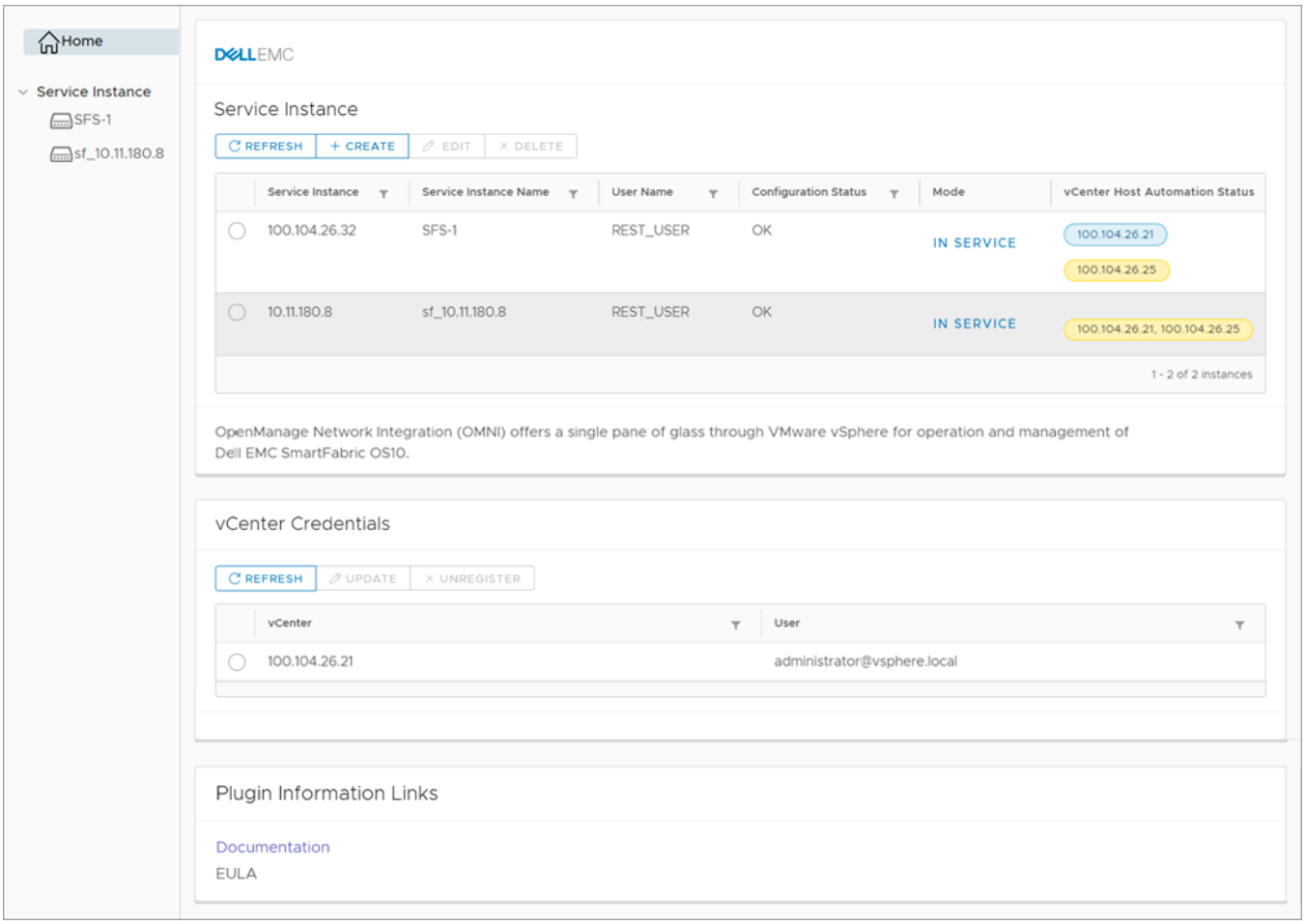
3. Click **Documentation** to view the User Guide and Release Notes uploaded at www.dell.com/support.

7

OMNI SmartFabric Management

This chapter explains how to manage SmartFabric components or entities using OMNI. The OMNI VM displays the list of manually created service instances, and the OMNI autodiscovered SmartFabric instances. For more information about the service instances, see OMNI Fabric Management Portal.

After you log in to the OMNI Fabric Management Portal, you can access and manage the SFS entities that are configured in a service instance.

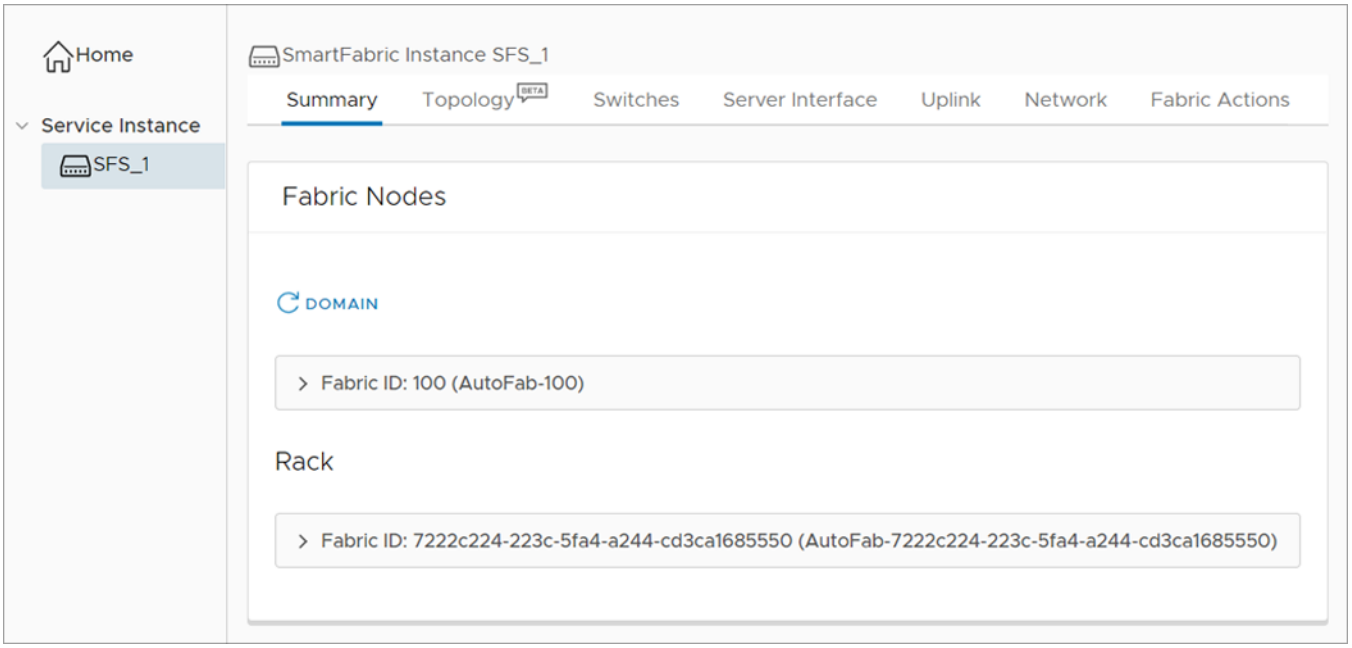


For each service instance, you can:

- View the summary of the fabric.
- View fabric topology design.
- Manage switches in a service instance.
- Manage server interface configuration.
- Manage uplinks.
- Manage network configuration.
- Manage network fabric entities.

View Service Instance summary

From **Home**, select the **Service Instance** > **Summary** to view details of each SmartFabric. The **Summary** page displays the fabric summary including fabric nodes and racks in a network fabric.



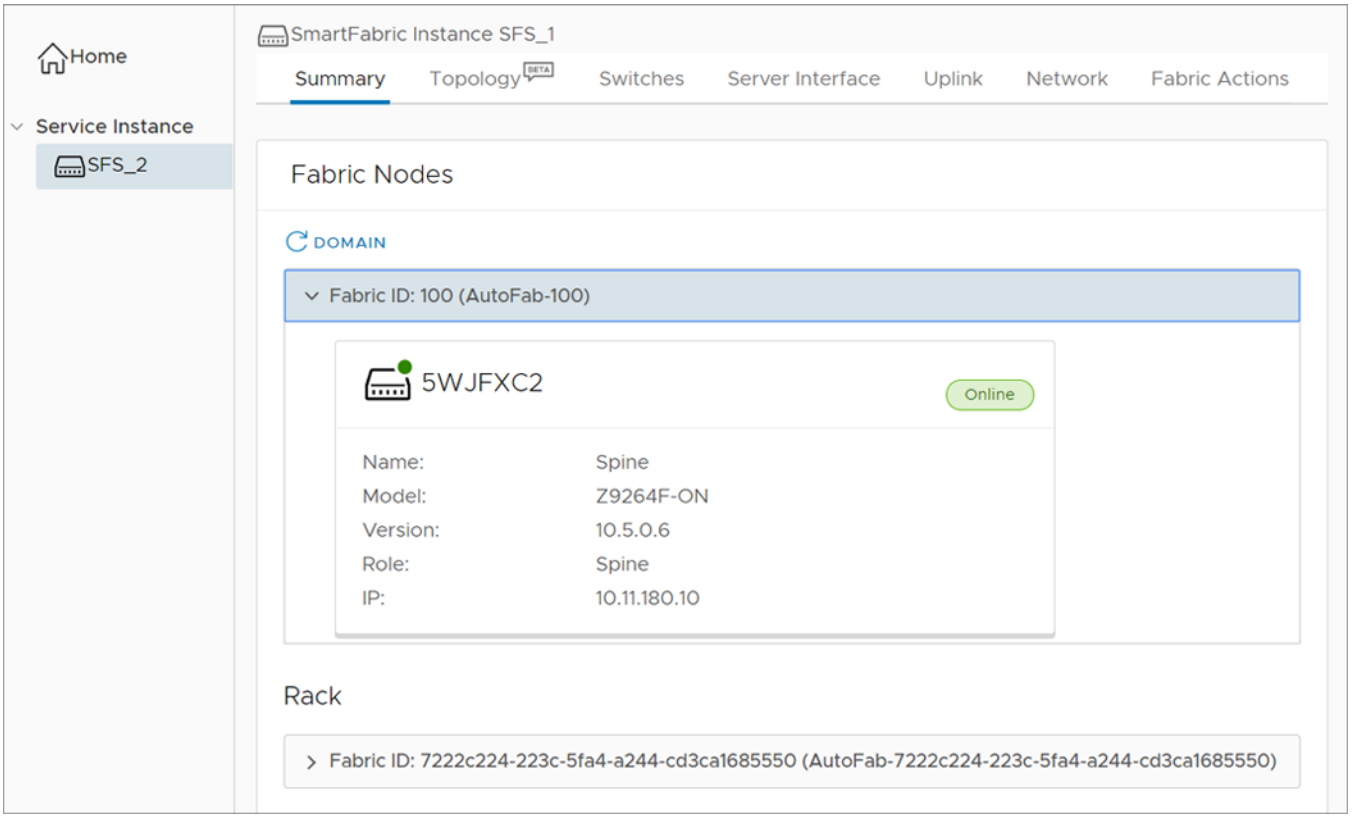
View node details

To view the details of the nodes or switches in the fabric, select the **Service Instance** > **Summary** > **Fabric Nodes**.

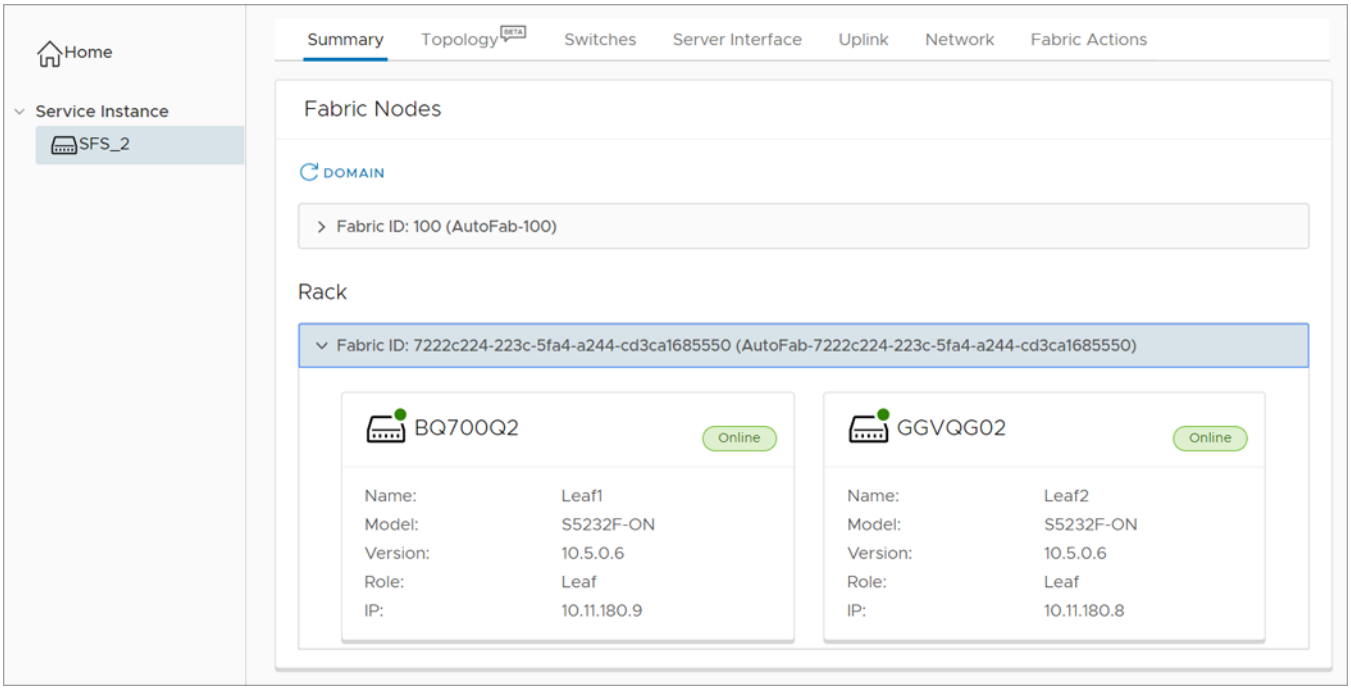
From **Fabric Nodes**, view the list of spine and leaf nodes that are deployed in the fabric. The page displays node information of the selected spine fabric structure which is arranged in racks. Select the **Fabric ID** to view the fabric details. Each spine fabric has corresponding switches. Each switch includes status (online or offline), name, model, version, role, and IP address.

Click **Domain** at any time to update the fabric details.

Fabric ID—Displays the list of spine switches connected in the fabric.



Rack—Displays the summary of the racks, which contains logical groupings of switches.

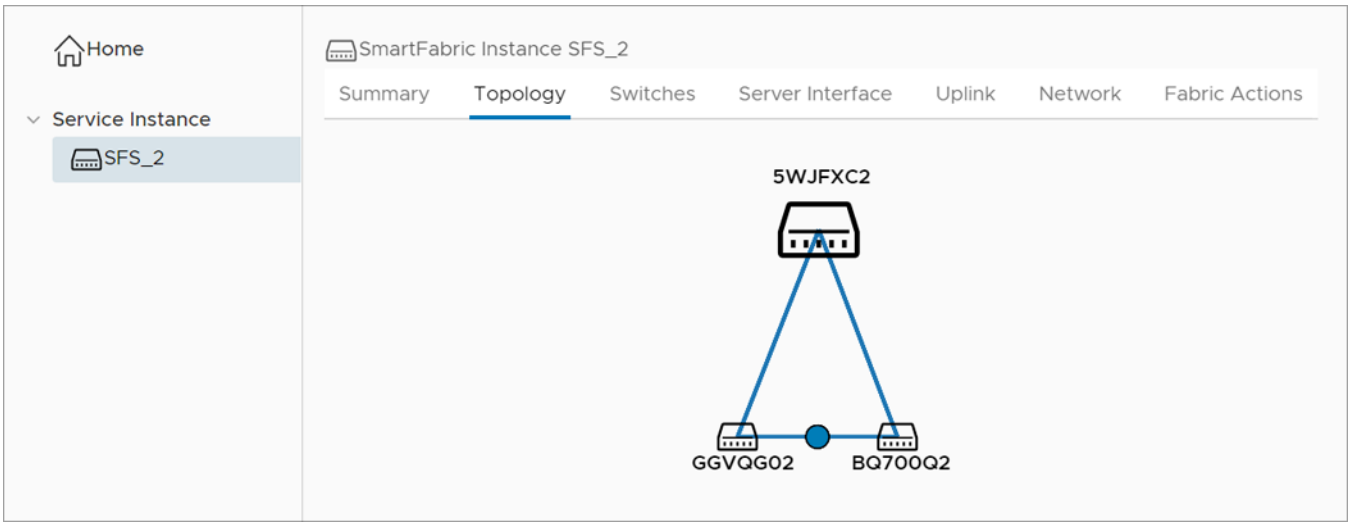


View fabric topology

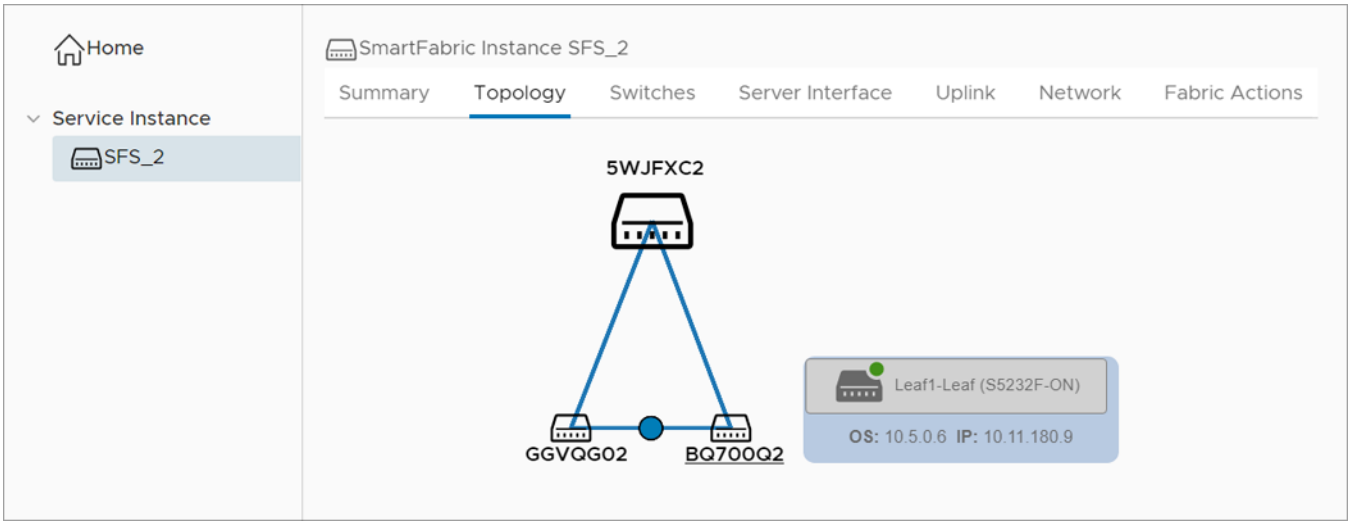
The **Topology** tab displays the graphical topology of the network fabric for the selected service instance. You can also view the details of the switch in the fabric.

Select the **Service Instance** > **Topology**.

NOTE: In this release, this feature is marked as beta.



The topology view displays the graphical icons of all the nodes and the link connectivity between the nodes. Each graphical node is represented with their service tag. Hover over an icon to view the detailed information about the node, and the link connectivity in the nodes. The detailed information of the node includes switch ID, switch platform, type of switch (leaf or spine), OS10 version running on the switch, and IP address. You can also view the details of source and destination interfaces of the link, when you hover over the links between the nodes.



Manage switches in a fabric

You can manage the list of spine and leaf switches available in a fabric.

From **Switches** page:

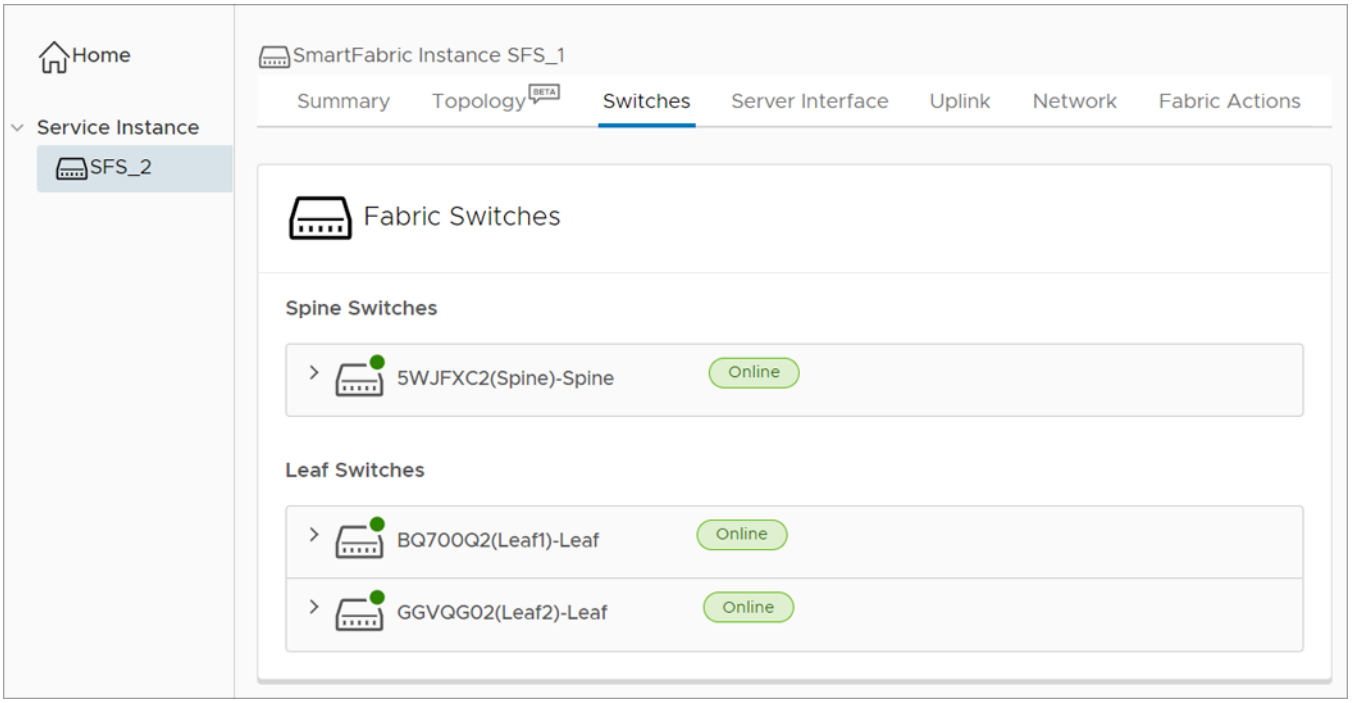
- View the details of the switches and the ports in a fabric.
- Edit the interface details.
- Set the MTU value for the port.
- Manage the unused ports in the switches.
- Configure breakout ports in leaf switches.
- Configure jump port.

View switch and port details

View the details of the leaf and spine switches, and the list of all ports and unused ports available in each switch. All ports category contains the list of interface and port channel in the switch.

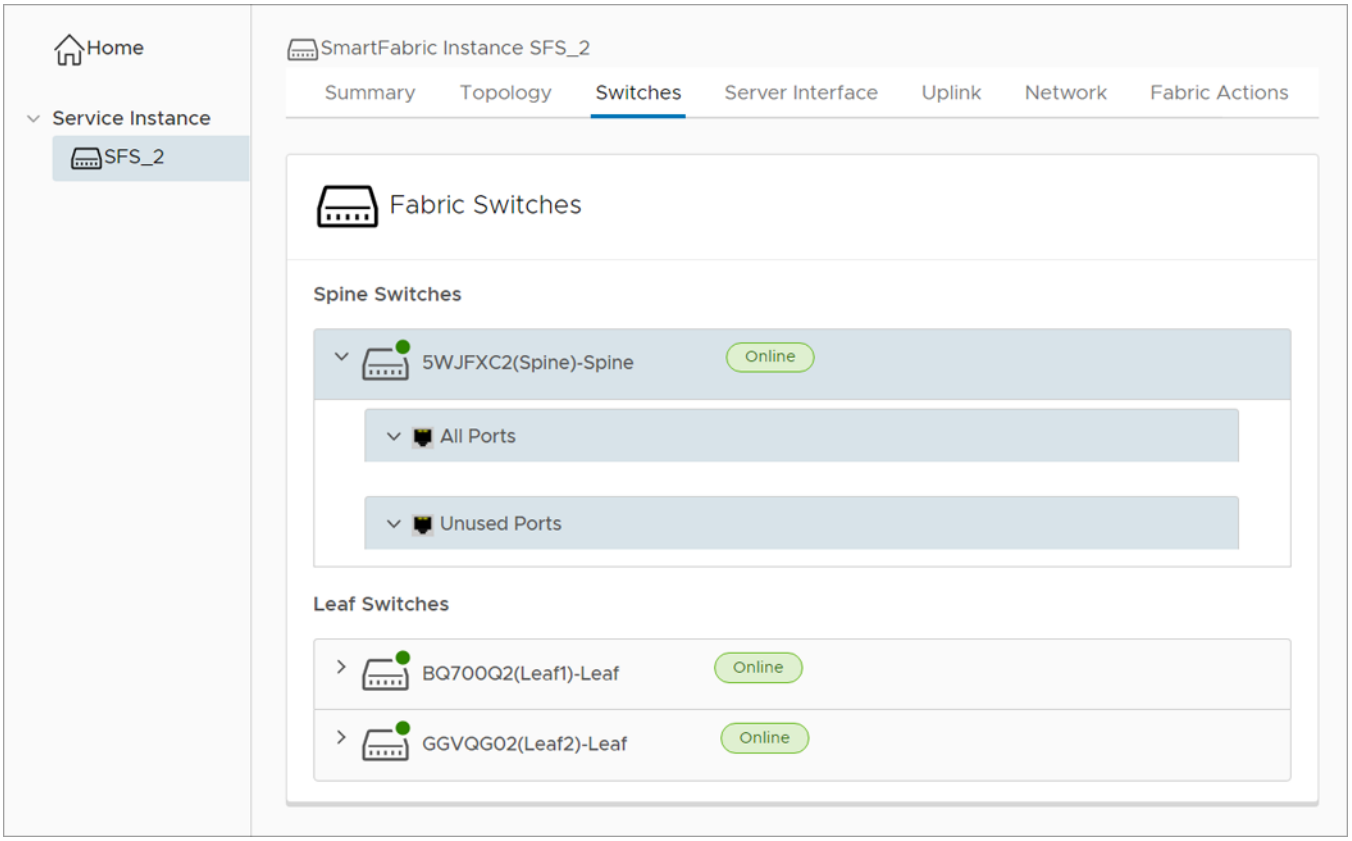
1. Select the **Service Instance** > **Switches**.

   Fabric Switches—Displays the list of spine and leaf switches available in the selected service instance.

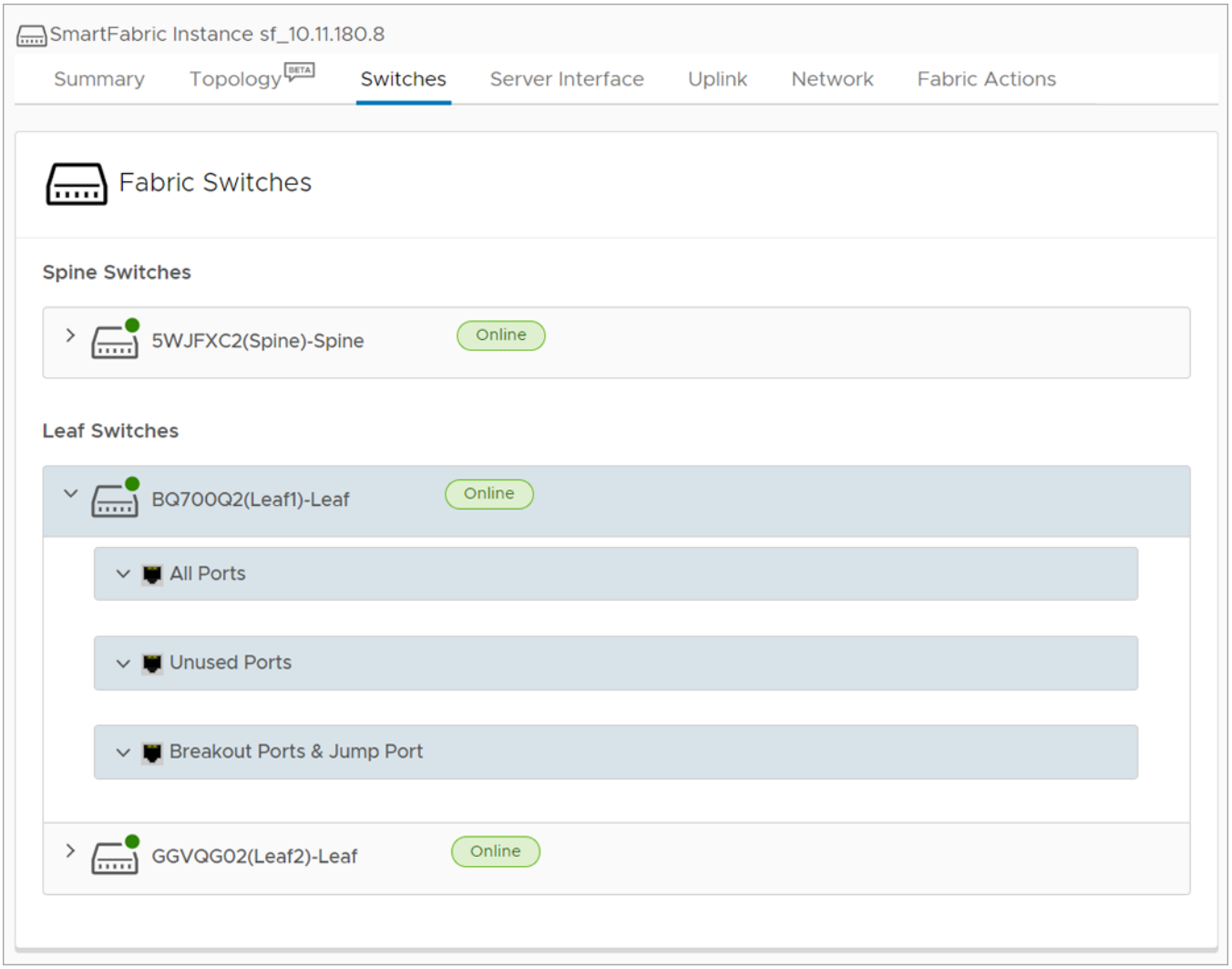


2. Select the arrow of the respective leaf or spine switch to view more information.

Spine Switches—Displays the list of all spine switches with ports information in categories. Click the arrow of the respective switch and category to view more about port information.



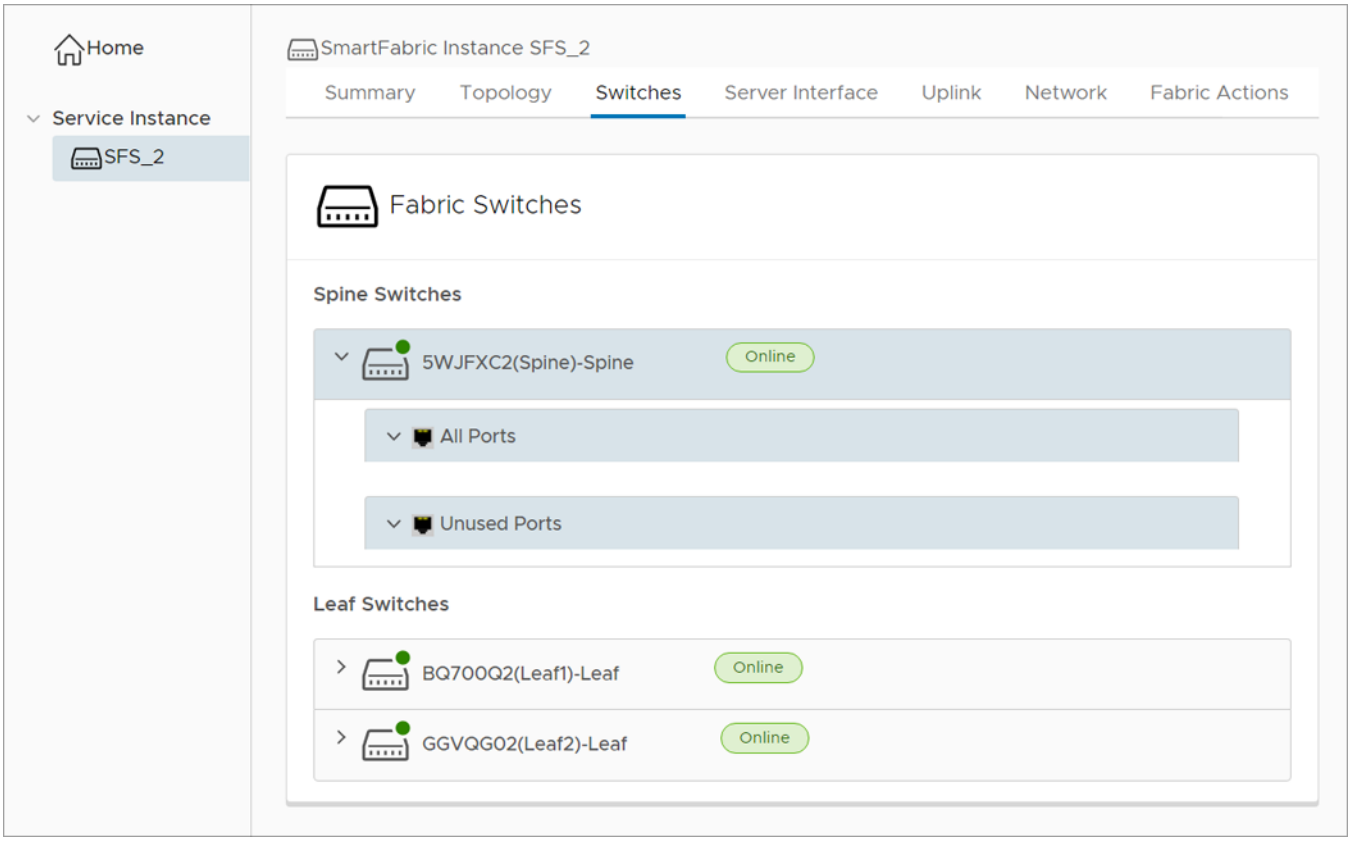
Leaf Switches—Displays the list of all leafs in the fabric with ports, unused ports, breakout ports, and jump port information in categories. Click the arrow of the respective leaf switch category to view more information about the ports.



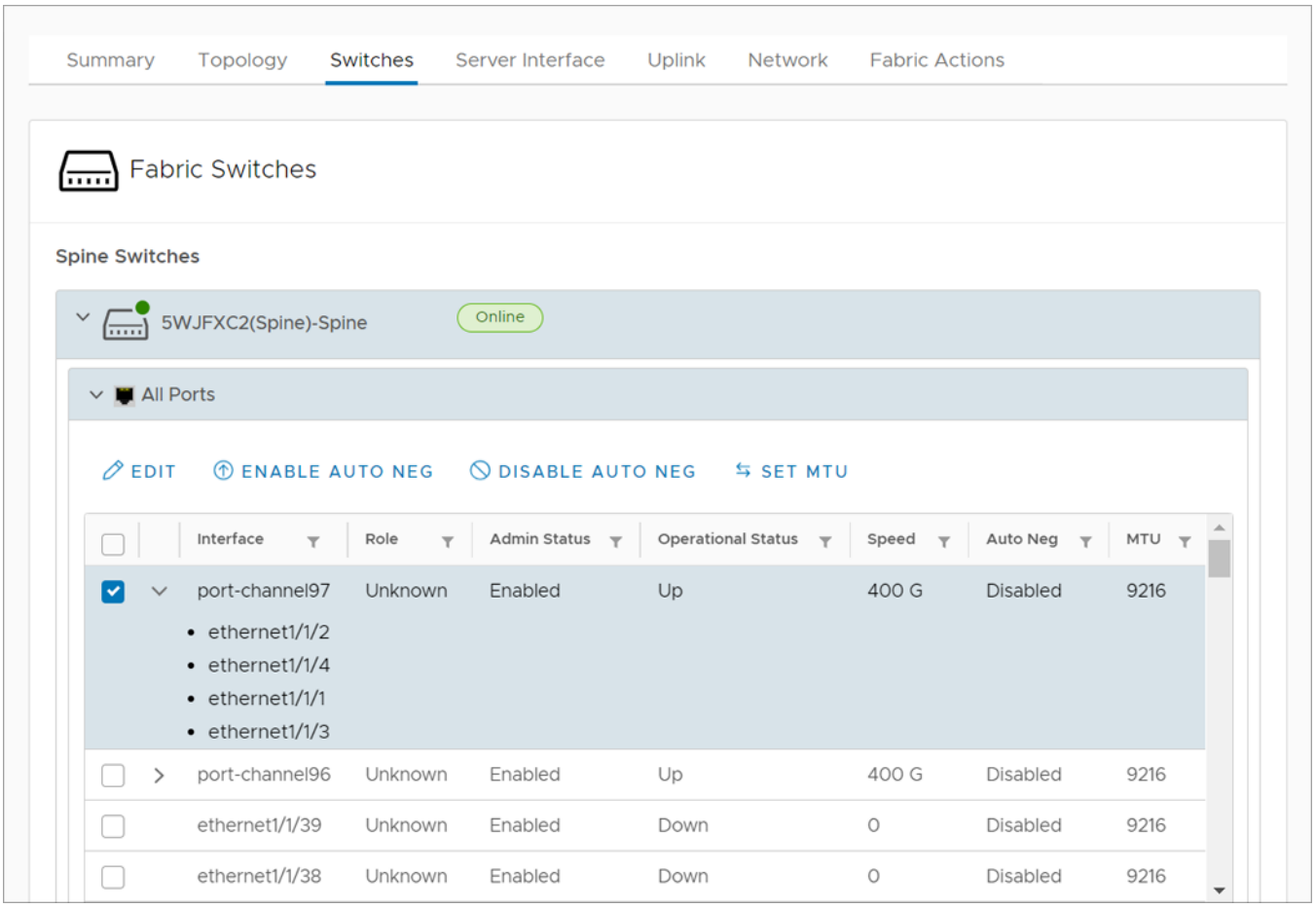
Edit port configuration on a switch

Edit the configuration of port on a leaf or spine switch.

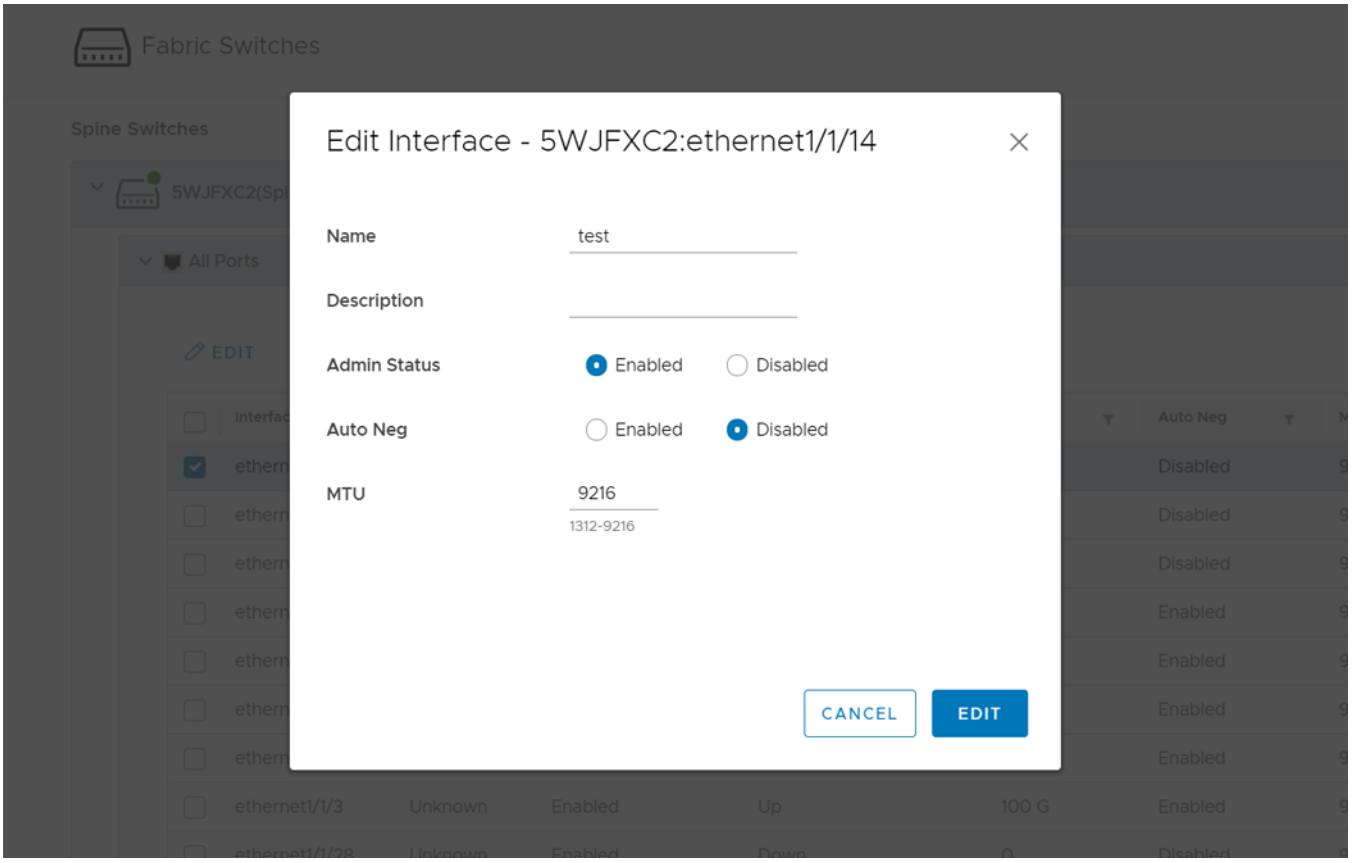
1. Select the **Service Instance** > **Switches**.
2. Select the spine or leaf switch by clicking the arrow to view more information.



3. Select a port from **All Ports** category, and click **Edit**.



4. Edit the name, description, admin status, auto negotiation, and MTU, and click **Edit**.

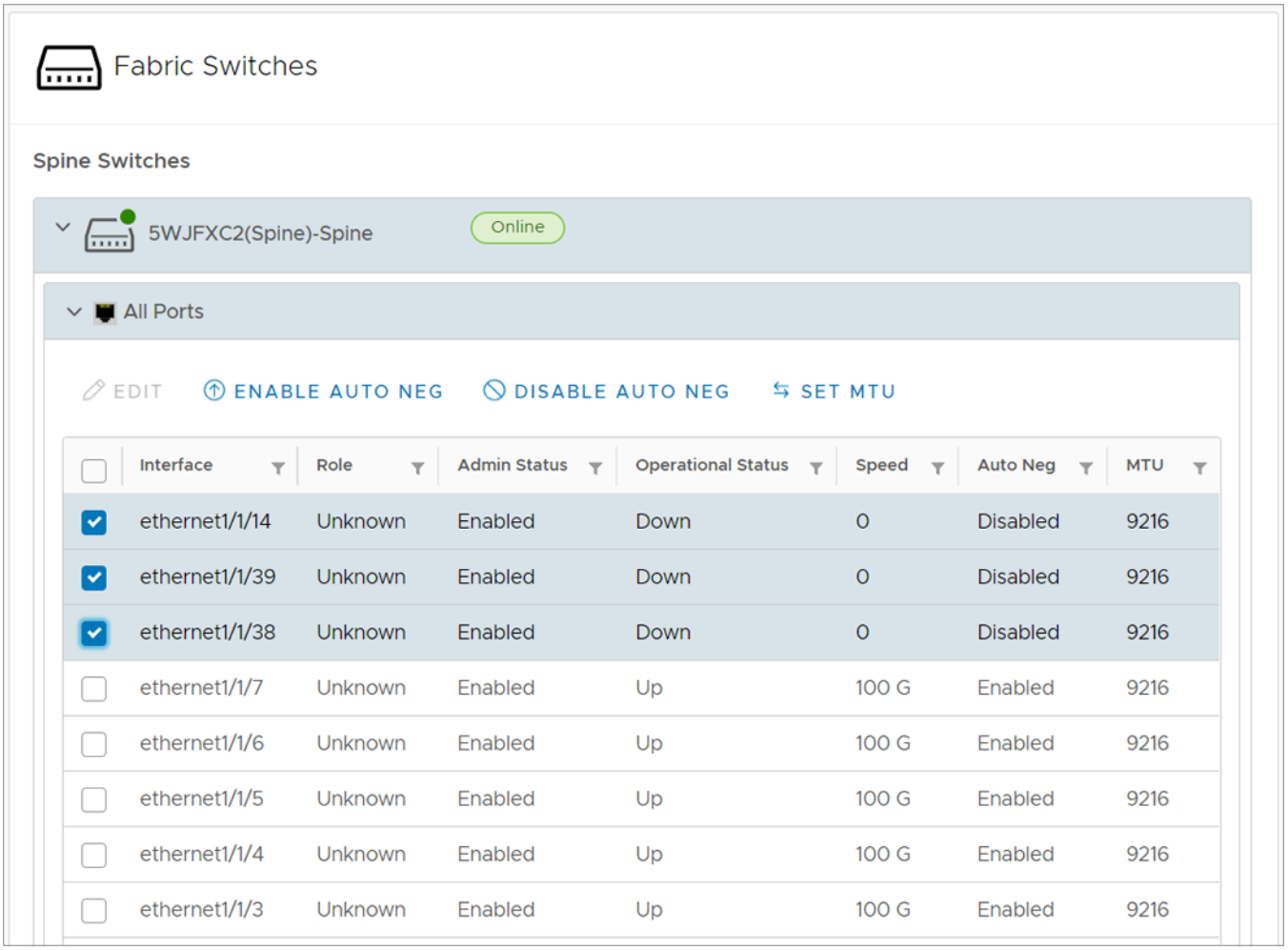


Configure auto negotiation status

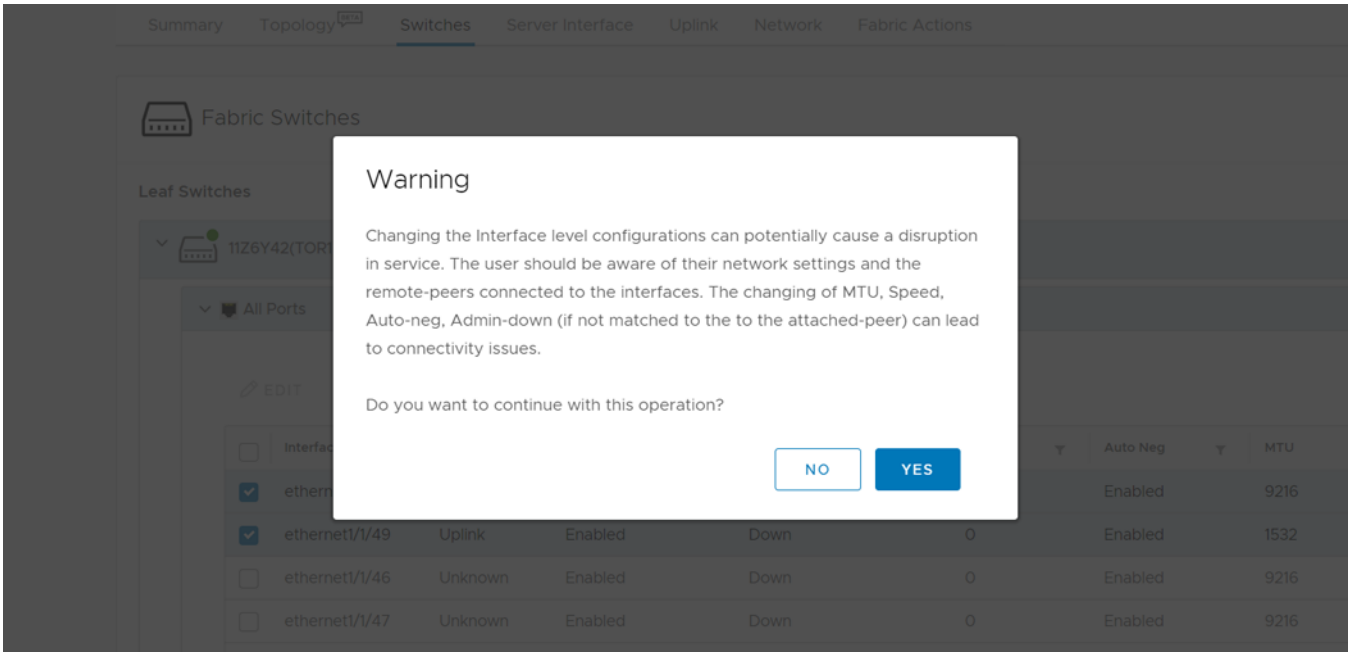
You can enable or disable the auto negotiation on a single port or multiple ports.

To enable auto negotiation:

1. From **All Ports**, select a port or multiple ports and click **Enable Auto Neg**.



2. The system displays a warning message. Click **Yes** to confirm.



3. The system displays the stage-wise progress of the interface status.

To disable auto negotiation:

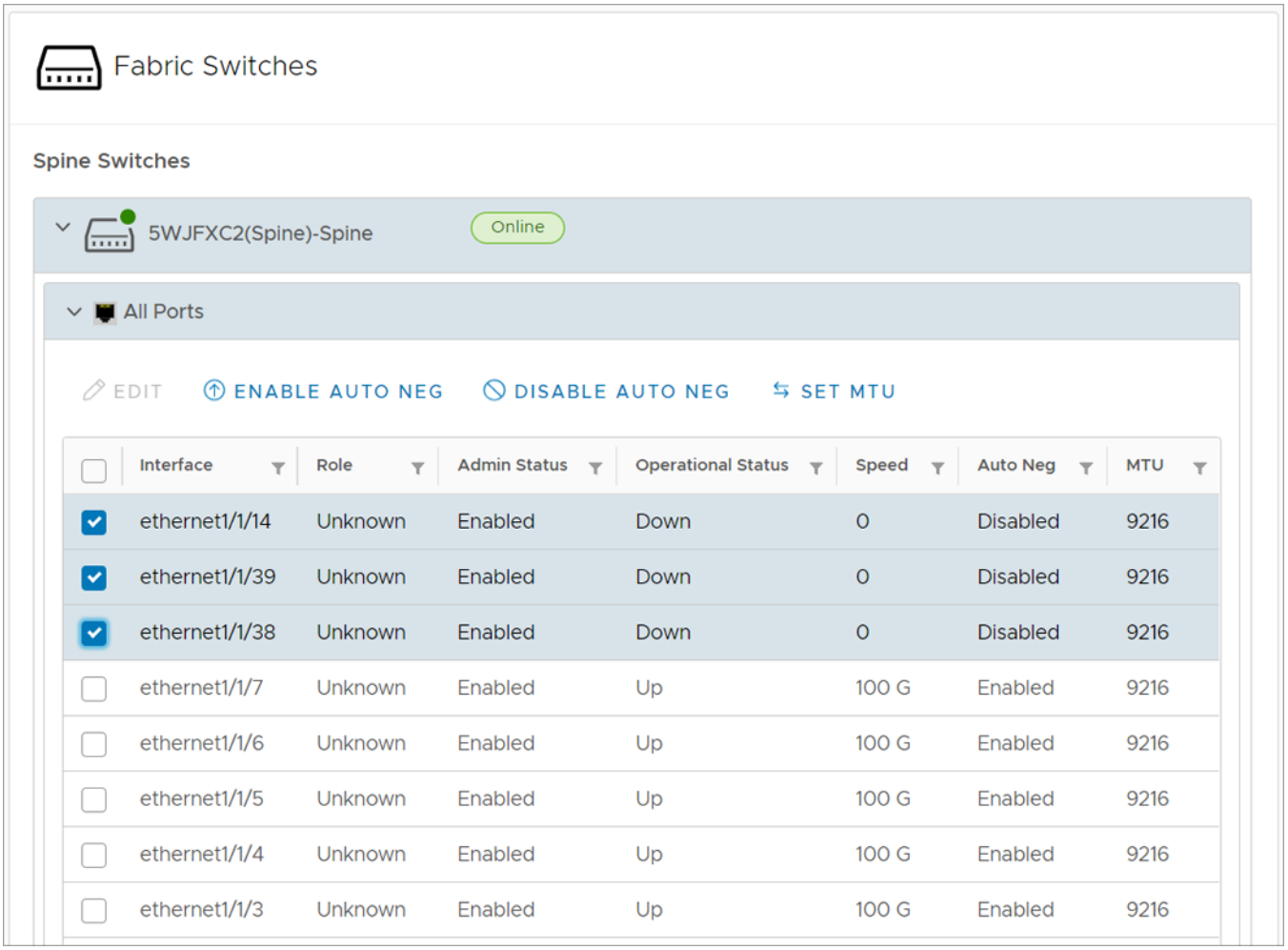
1. From **All Ports**, select a port or multiple ports and click **Disable Auto Neg**.

2. The system displays the stage-wise progress of the interface status.

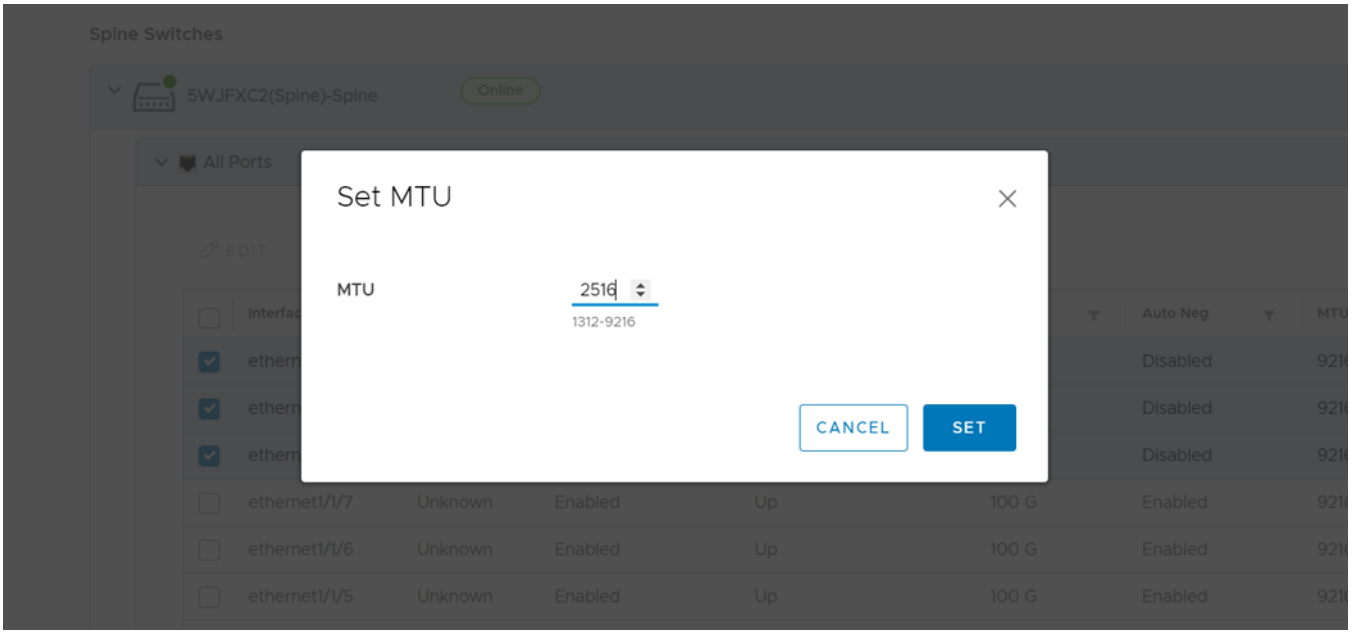
Set MTU value

Set maximum transmitting unit (MTU) for the port.

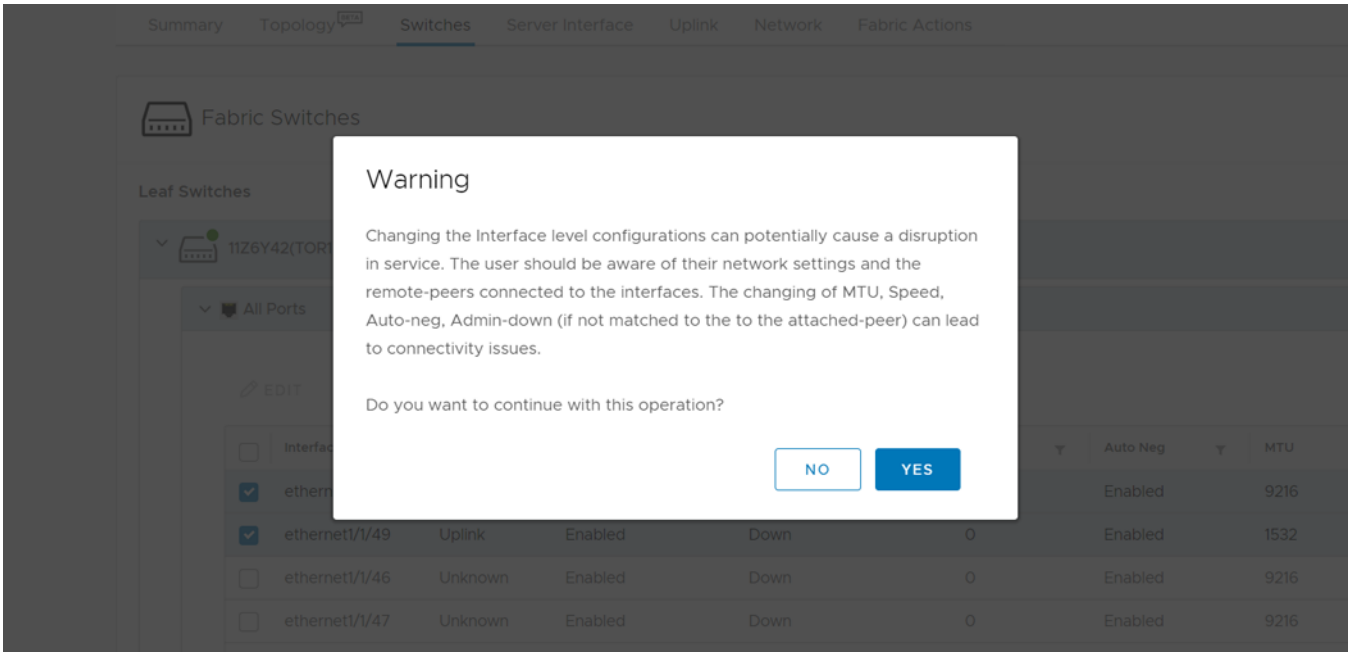
1. Select a port or multiple ports and click **Set MTU**.



2. Enter the MTU value and click **Set**.



3. The system displays a warning message. Click **Yes** to confirm.



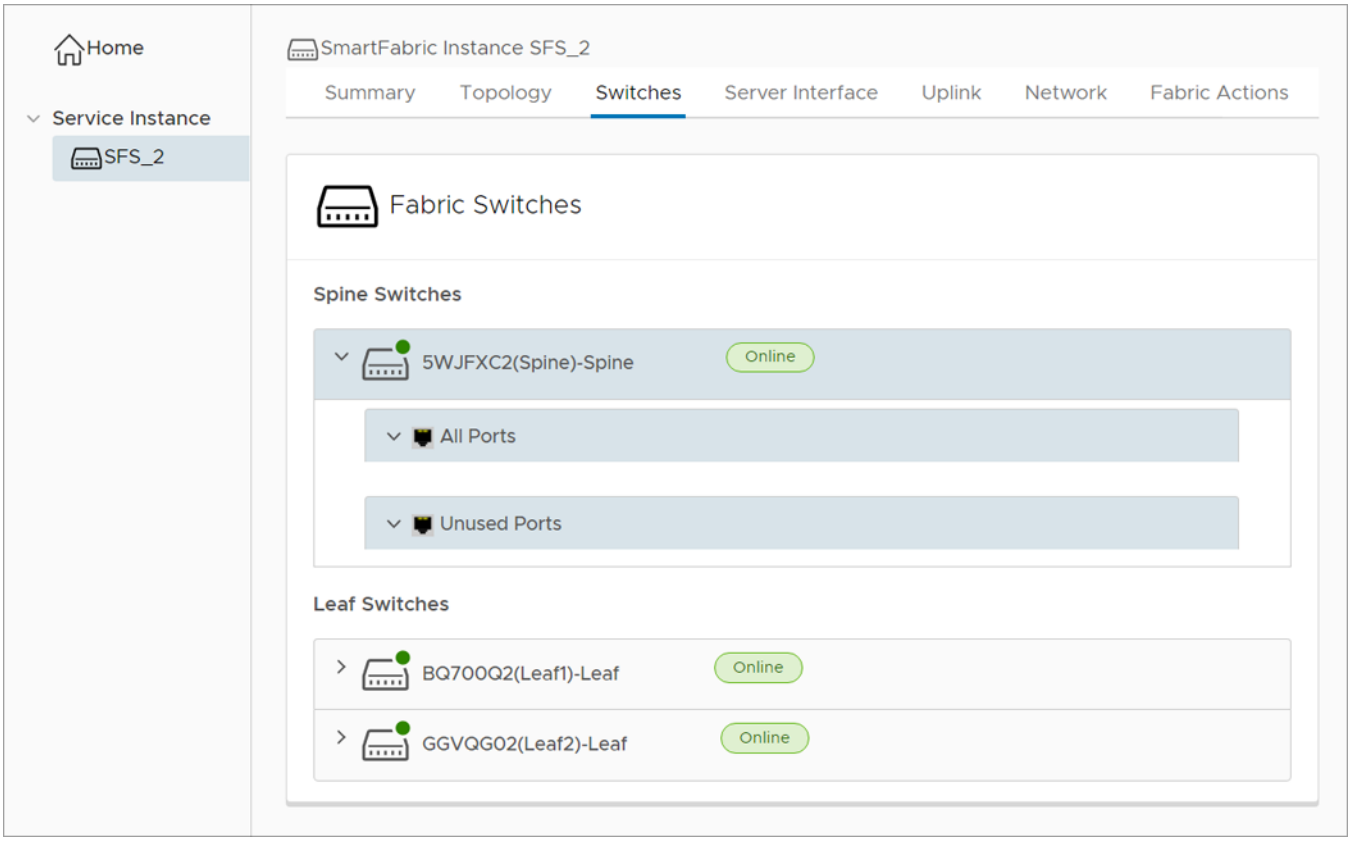
4. The system displays the action success or failure message.

Manage unused switch ports

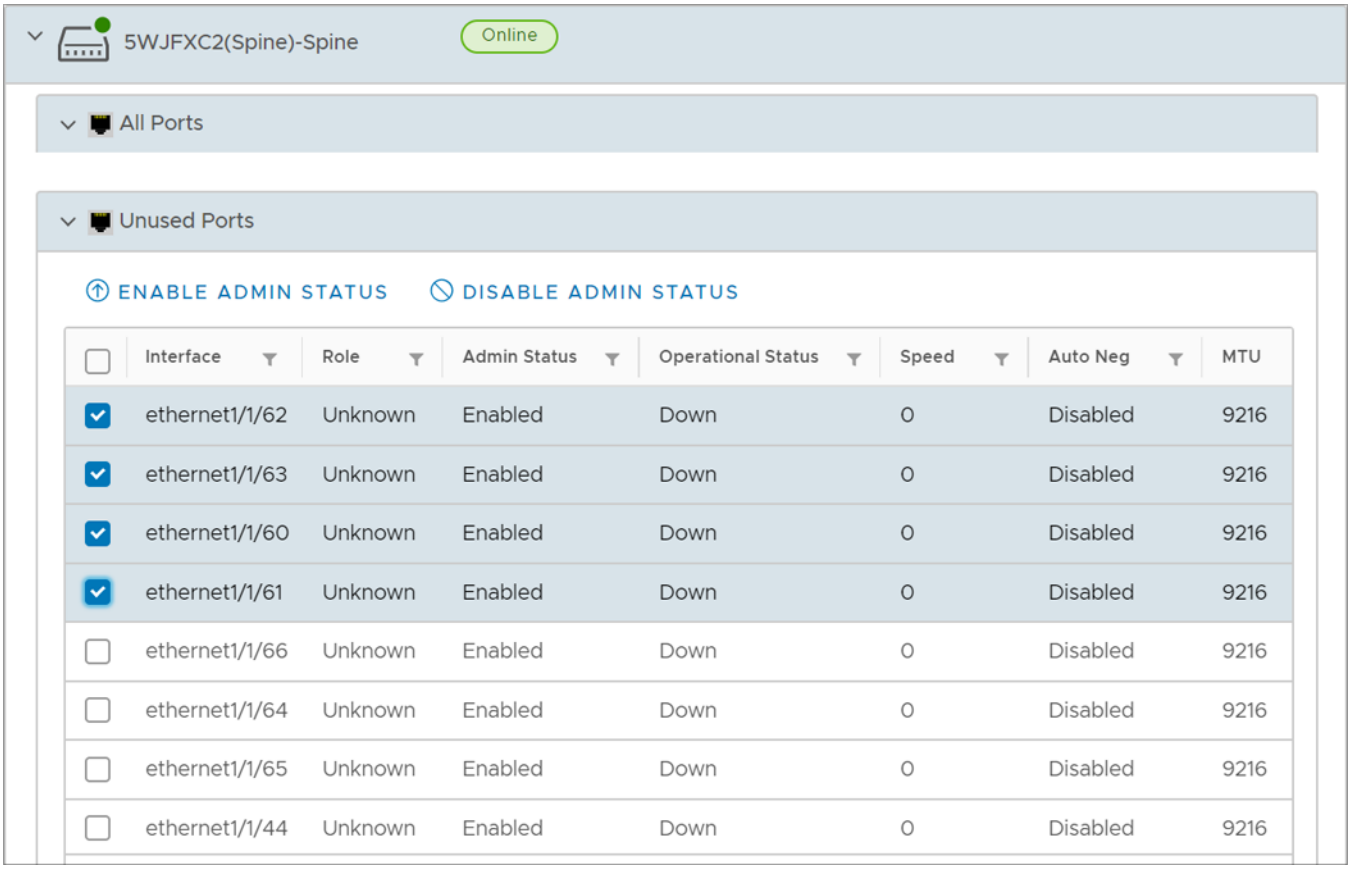
You can view and manage the unused ports in the switches.

To enable or disable unused ports:

1. Select the **Service Instance** > **Switches**.
2. Select any spine or leaf switch by clicking the arrow to view the list of ports.



3. Click **Unused Ports** category to view the list of unused ports available in the switch.
4. Select a port or multiple ports, and click **Enable Admin Status**.



Interface	Role	Admin Status	Operational Status	Speed	Auto Neg	MTU
ethernet1/1/62	Unknown	Enabled	Down	0	Disabled	9216
ethernet1/1/63	Unknown	Enabled	Down	0	Disabled	9216
ethernet1/1/60	Unknown	Enabled	Down	0	Disabled	9216
ethernet1/1/61	Unknown	Enabled	Down	0	Disabled	9216
ethernet1/1/66	Unknown	Enabled	Down	0	Disabled	9216
ethernet1/1/64	Unknown	Enabled	Down	0	Disabled	9216
ethernet1/1/65	Unknown	Enabled	Down	0	Disabled	9216
ethernet1/1/44	Unknown	Enabled	Down	0	Disabled	9216

To disable the ports, select a port or multiple ports, and click **Disable Admin Status**.

The system displays the change status and update success message on completion.

Dell Technologies recommends to:

- Enable the port status to operationally up before adding any devices to the port, if the port is disabled using the OMNI UI.
  NOTE: Devices that are connected to the disabled port are not discovered.
- Ensure that the ports are UP before adding any switches, when you expand the leaf and spine fabric deployments.
- Ensure that the switch port is in UP, when onboarding a server to a leaf switch.

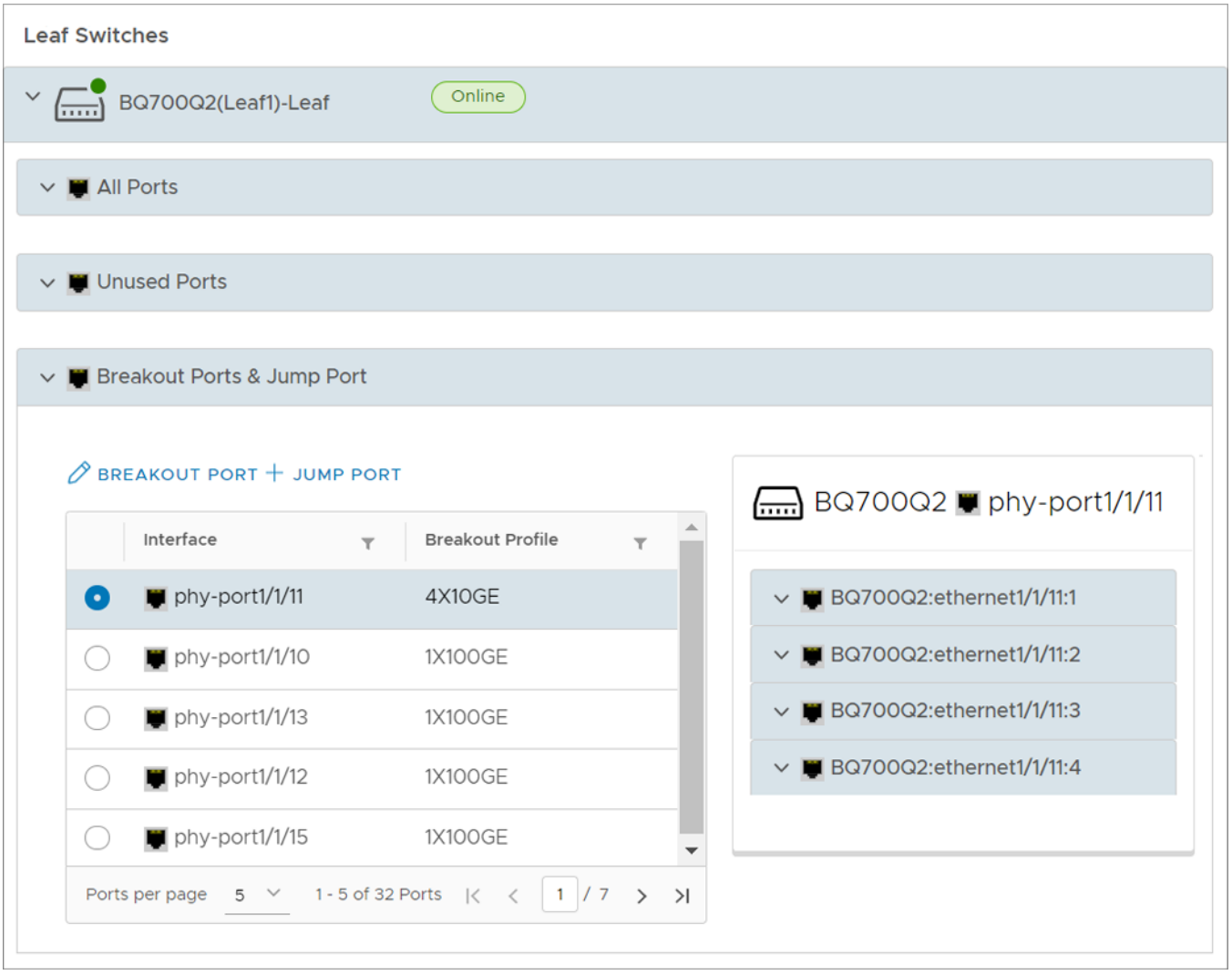
Configure breakout ports

Configure breakout ports on an interface of the leaf switch.

NOTE: By default, the auto breakout feature is enabled in spine switches. OMNI UI does not provide an option to break out ports in spine switches.

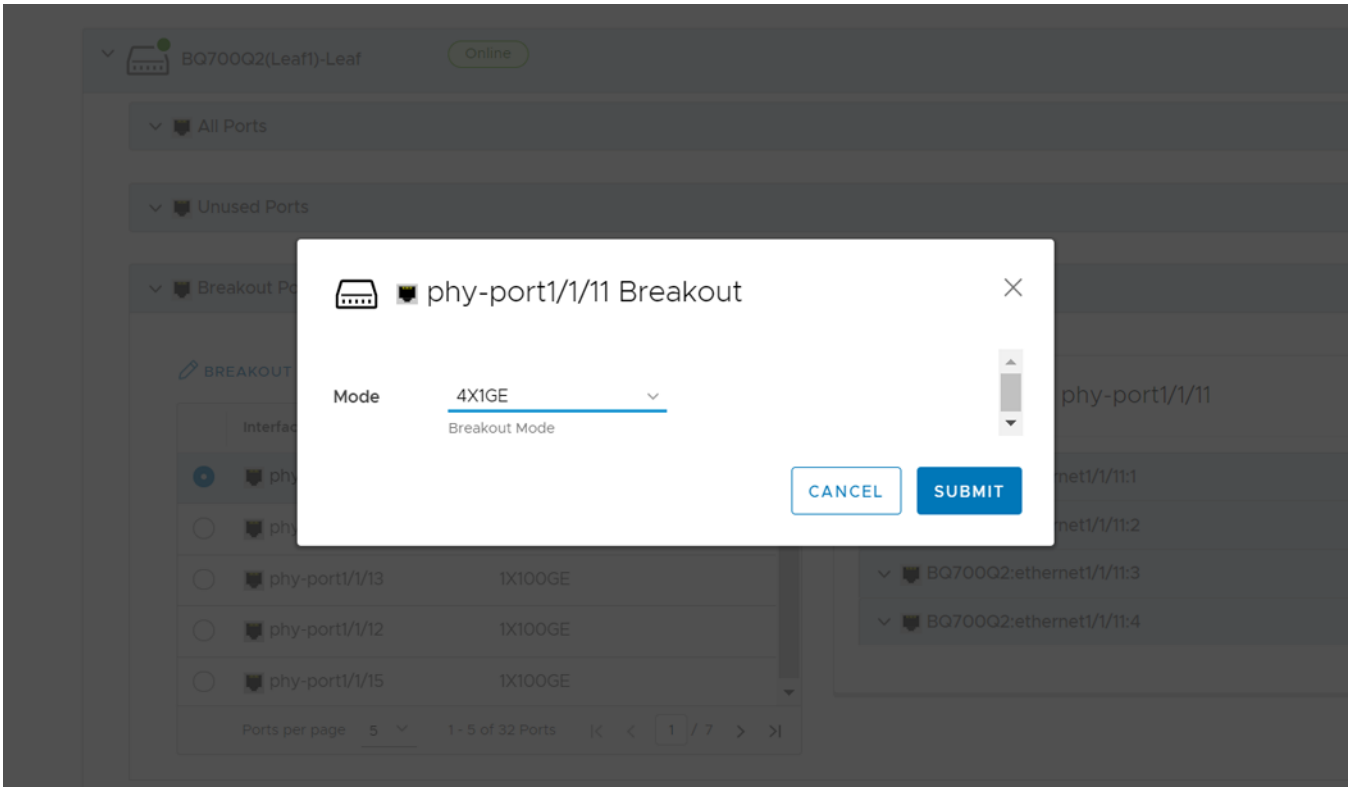
To configure the breakout ports in a leaf switch:

1. Select the **Service Instance** > **Switches** > **Leaf Switches**.
2. Select a leaf switch from the list.
3. From **Breakout Port and Jump Port** category, select a port that you want to breakout, and click **Breakout port**.



NOTE: While configuring a breakout port, the existing configuration of the port is reset to default.

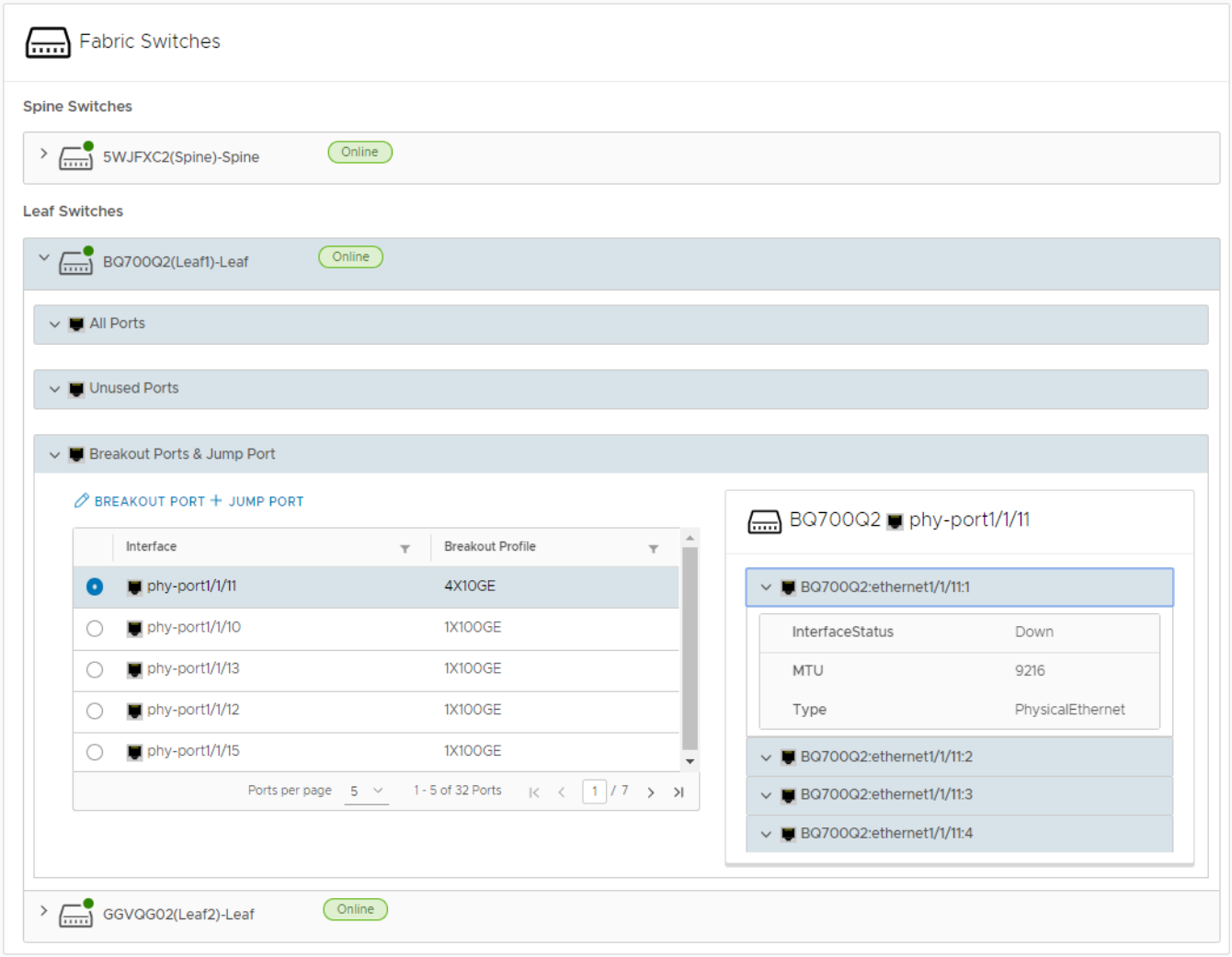
4. Select the **Breakout Mode** for the port from the list, and click **Submit**.



5. The system displays breakout port configured successful or failure message.

View port-group properties

Select a port to view properties on the right.

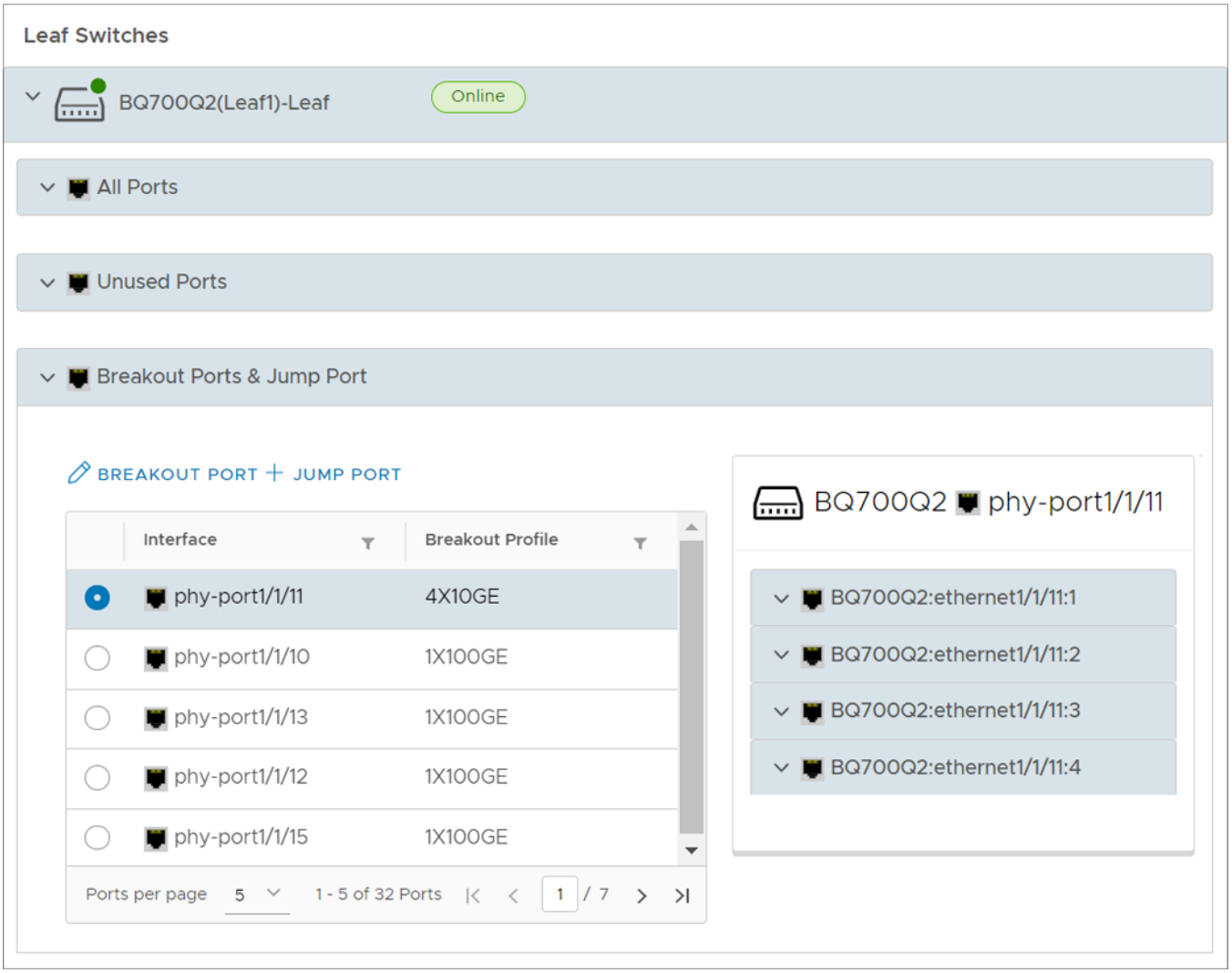


Add jump port

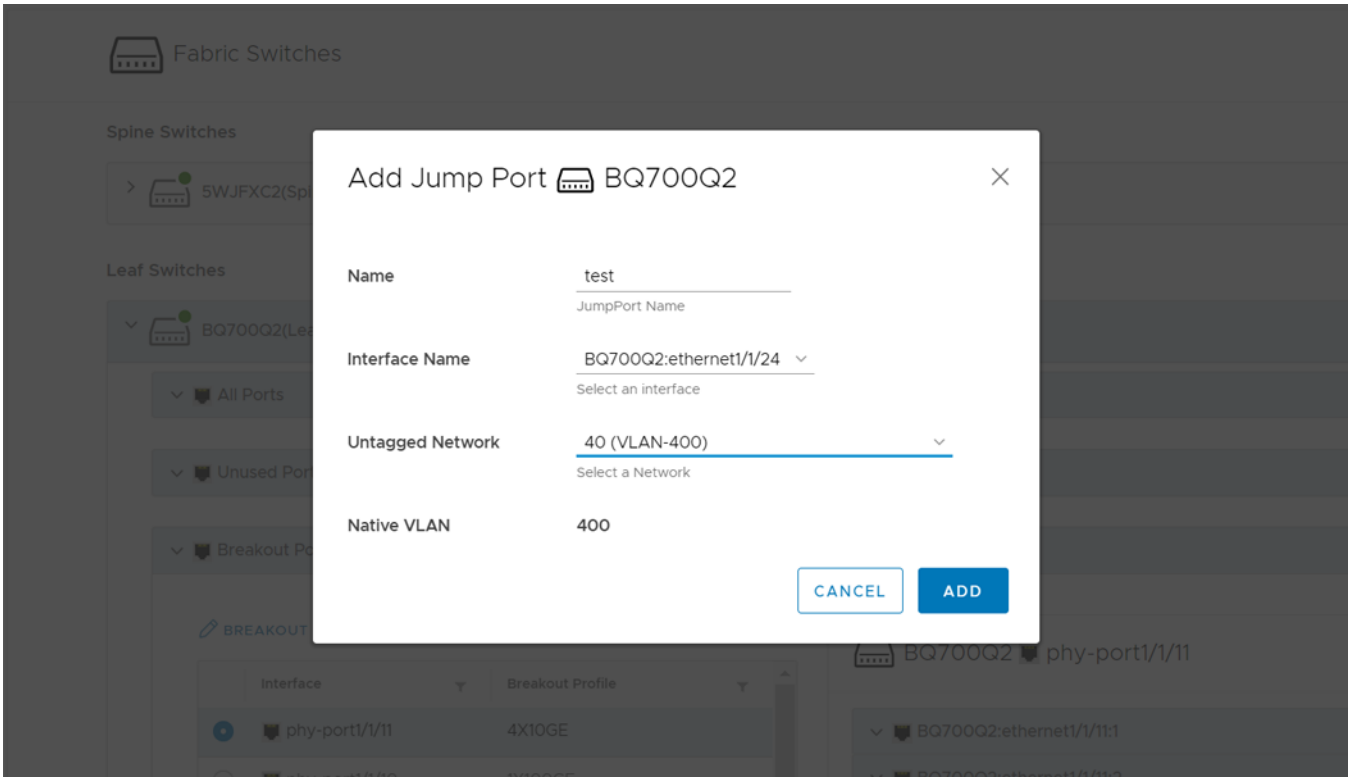
You can configure only one port in a leaf switch as a jump port. You can select any available port that is not part of an uplink and ICL, and port connected to a server in SmartFabric deployment.

To configure jump port:

1. Select the leaf switch from the list, and select the **Breakout Ports & Jump Port** category.
2. Select the switch to view the properties, and click **Jump Port**.



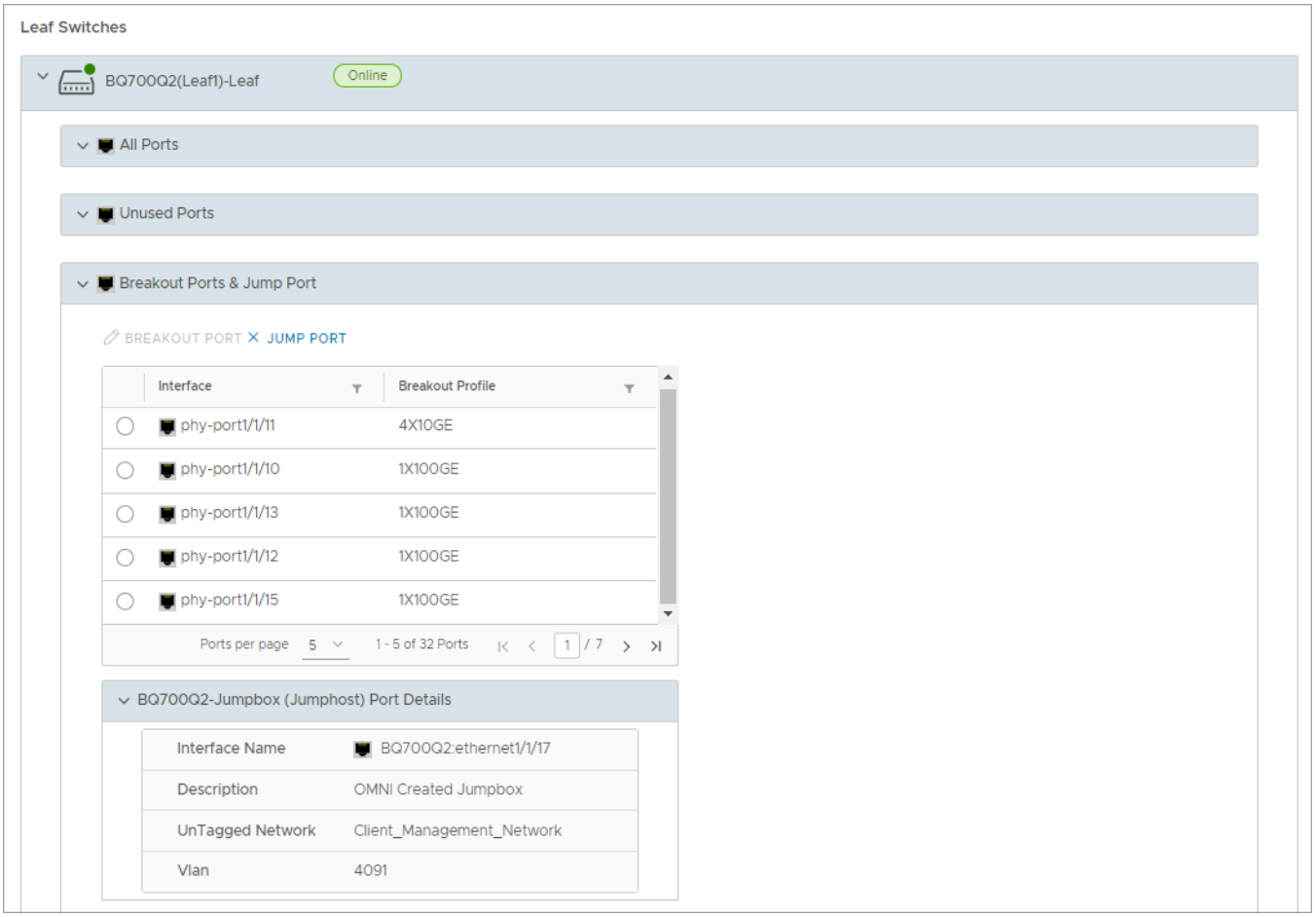
3. Enter the **Name** of the new jump port, select the **Interface Name**, select the **Untagged Network**, then click **Add**.



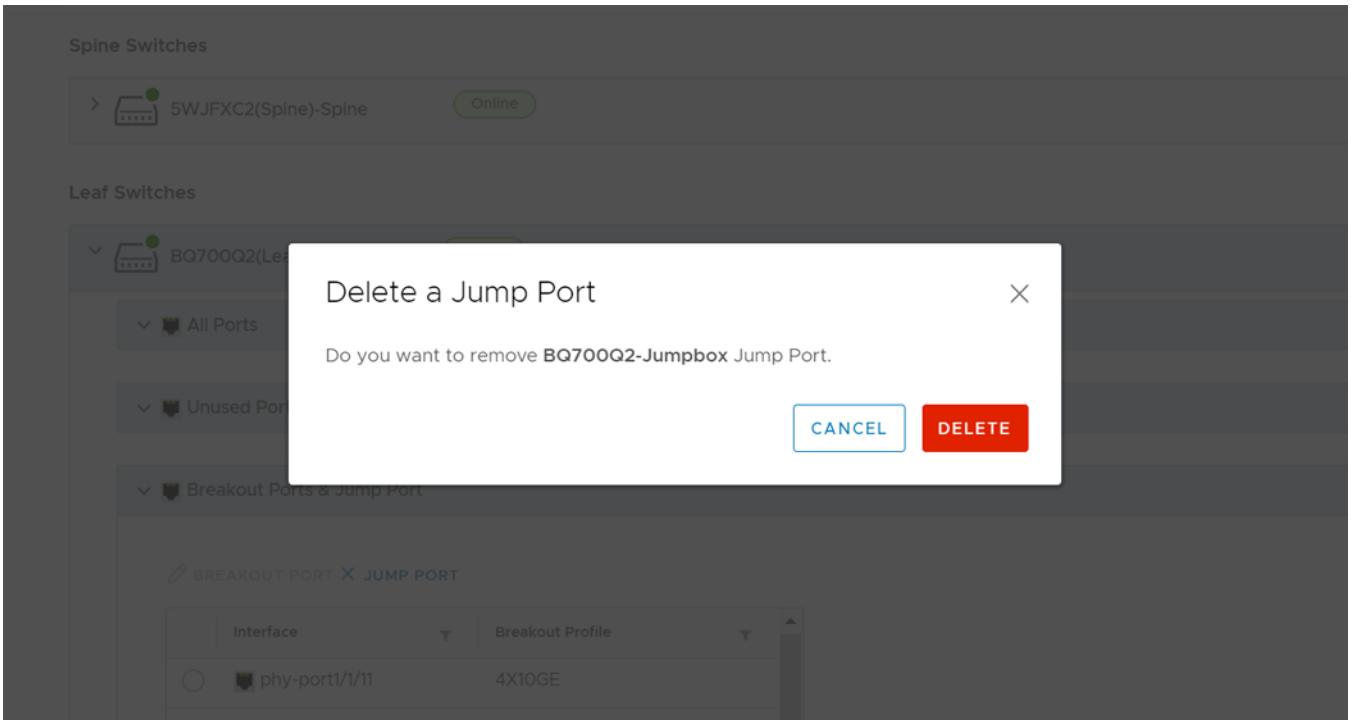
4. The system displays jump port addition success message.

Delete jump port

1. Select the leaf switch for which you want to delete the configured jump port.



2. Select the Jump port, and click **Delete**.



3. The system displays jump port deletion success message.

Configure server interface profile

Server Interfaces Profile page displays a list of Server Profile IDs and their respective onboard status. Select a profile to view details pertaining to that specific profile. You can view information including interface ID, fabric ID, native VLAN, and network name and VLAN ID (if applicable).

From **Server Interface**, you can:

- Create a server interface profile.
- Edit a network in a server interface profile.
- Edit the ports in a server interface profile.
- Delete a server interface profile.
- Automate server onboarding.

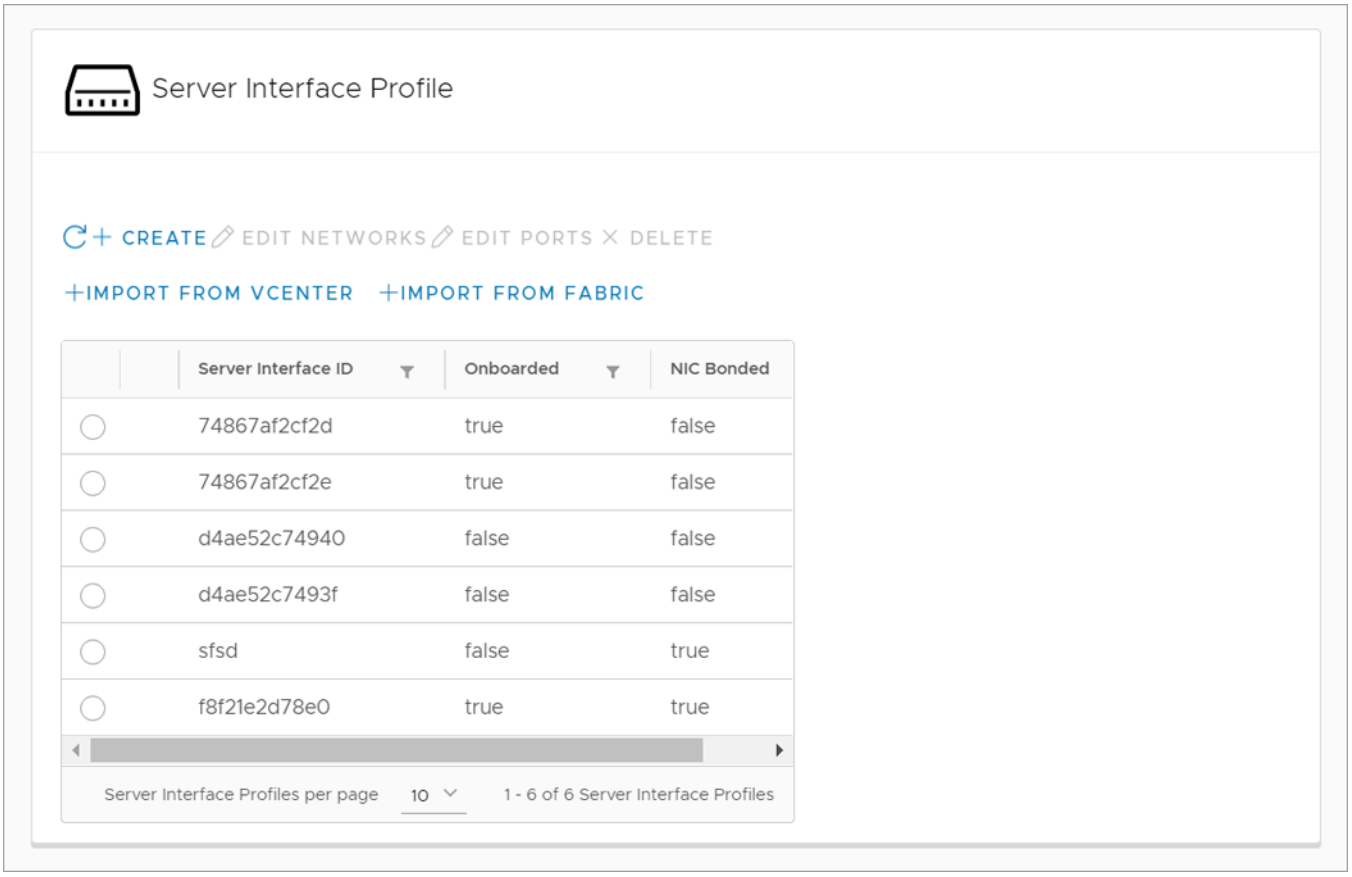
Create server interface profile

Create a server profile by providing the server profile type, name, and bonding technology.

Create server interface with an existing server profile

To create a server interface with an existing server profile:

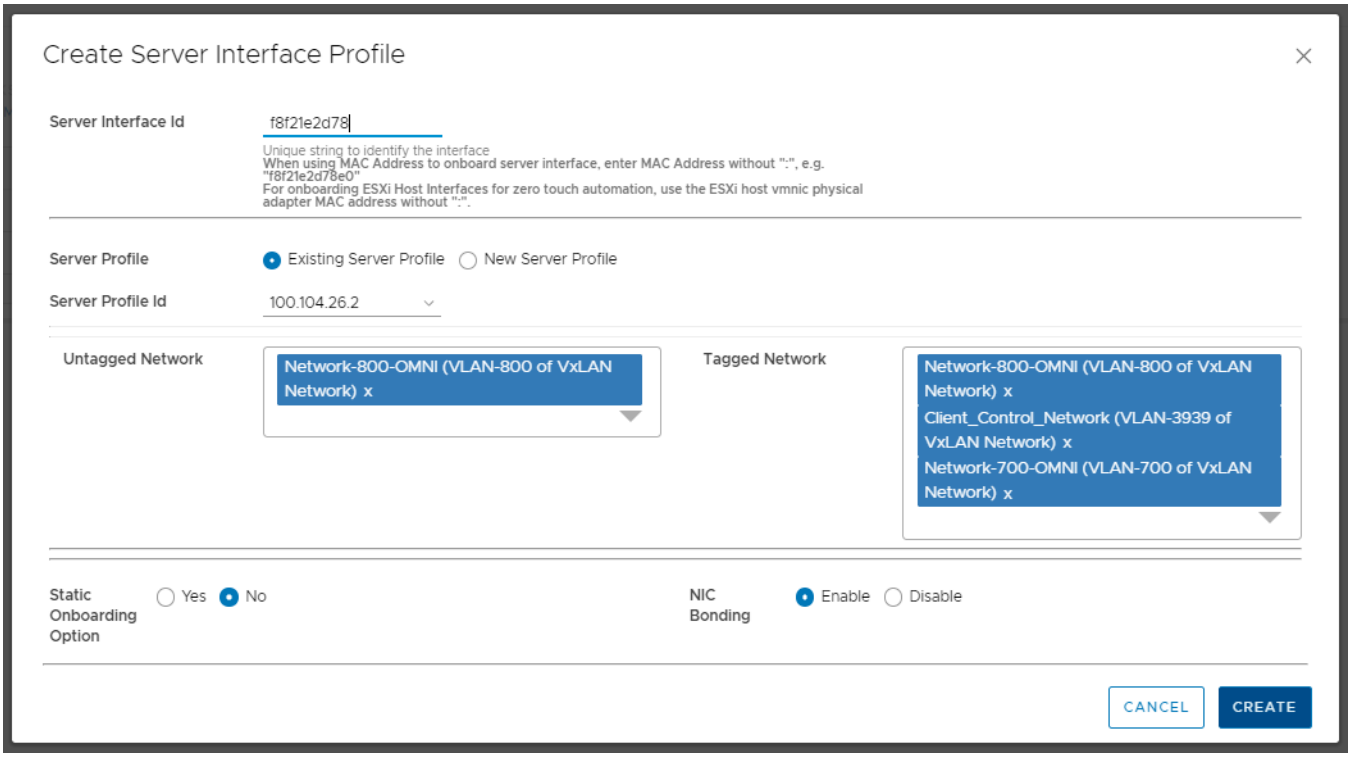
1. Select the **Service Instance** > **Server Interface**.



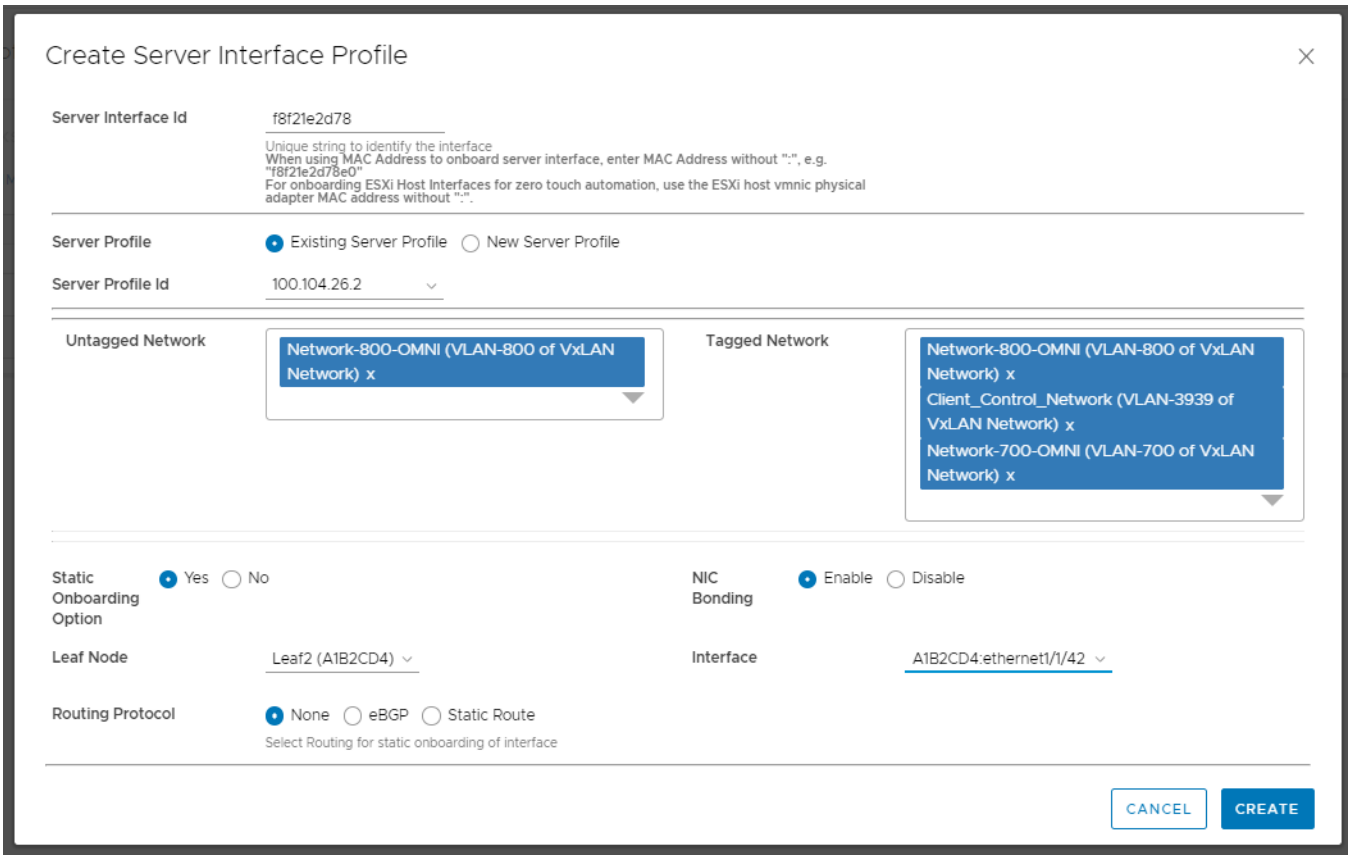
2. Click **Create** to create a server interface profile and provide server interface ID, then select **Existing Server Profile**.

   NOTE: You are allowed to configure duplicate server interface ID. When using MAC address to onboard server interface, enter MAC Address without ":", for example, f8f21e2d78e0. For onboarding ESXi host Interfaces for zero touch automation, use the ESXi host VM NIC physical adapter MAC address without ":".

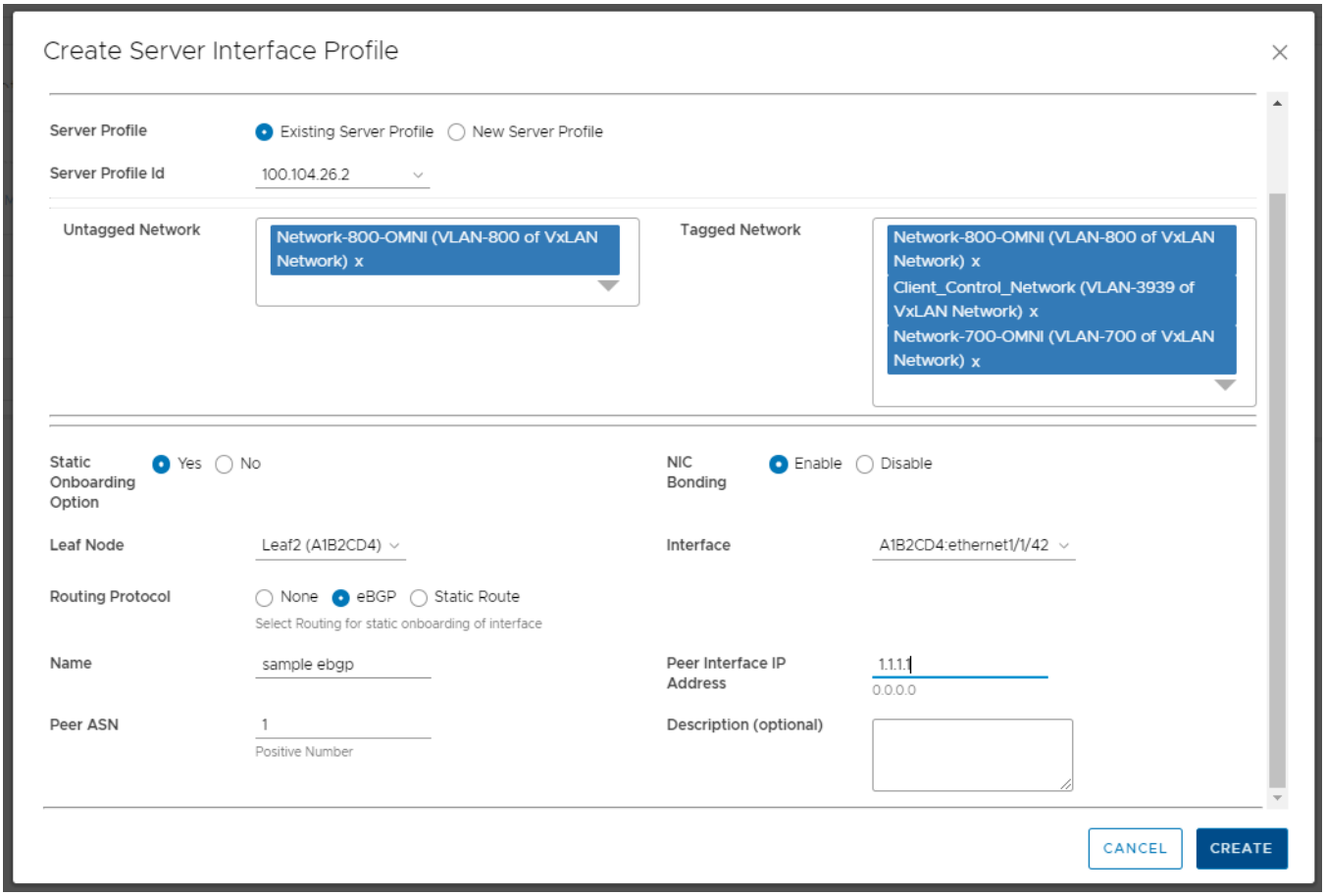
3. Select the **Server Profile Id** from the list, select one or multiple networks for the **Untagged Network**, enable or disable **NIC Bonding**, select **Static Onboarding Option** as **No**, and click **Create**.



4. (Optional) Select **Yes** for the **Static Onboarding Option**, add **Leaf Node** and **Interface** (where the server interface is connected), select the routing protocol as **None**, and click **Create**.

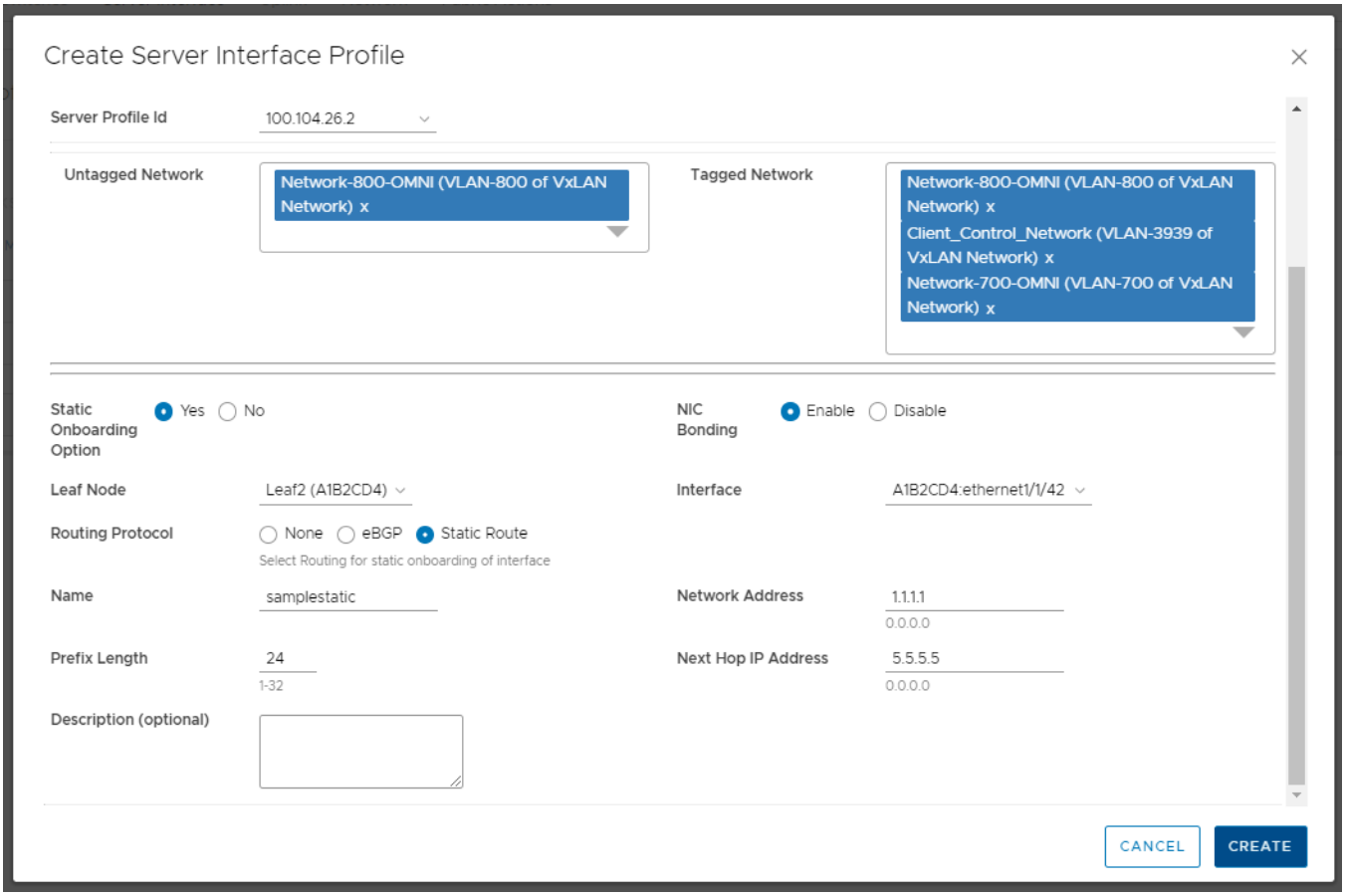


5. (Optional) Select **Yes** for the **Static Onboarding Option**, select **Leaf Node** and **Interface** (where the server interface is connected), select **eBGP**. Enter the eBGP routing template by entering the name, peer **ASN**, description, and peer interface **IP address**, and click **Create**.



NOTE: In static onboarding, the eBGP or static route routing protocol option is used for NSX-T deployment.

6. (Optional) Select **Yes** for the **Static Onboarding Option**, select **Leaf Node** and **Interface** (where the server interface is connected), select **Static Route**, enter the **Network Address** and **Next-Hop Address**, then click **Create**.



NOTE: You cannot delete any created server profile.

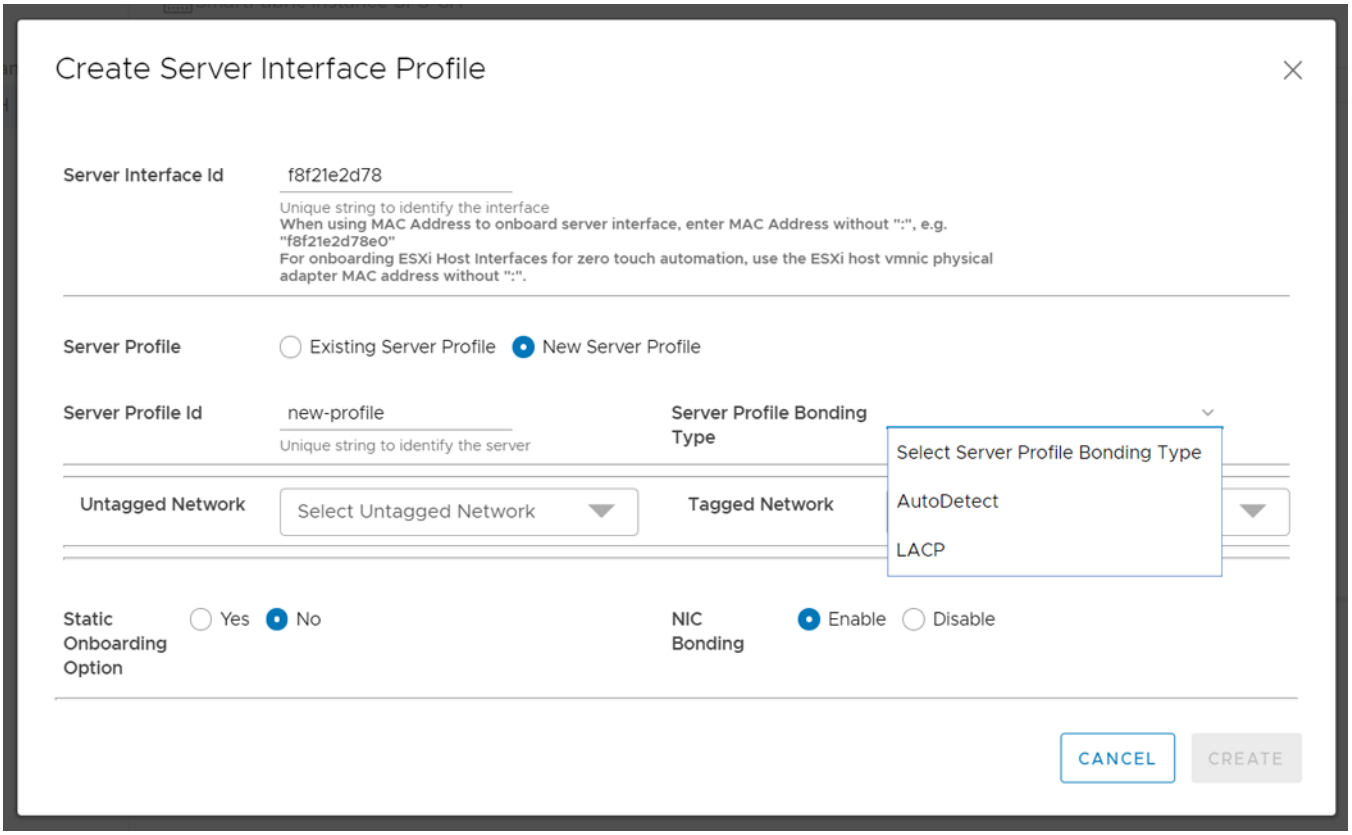
7. The system displays server profile and server interface creation successful messages.

Create server interface with new server profile

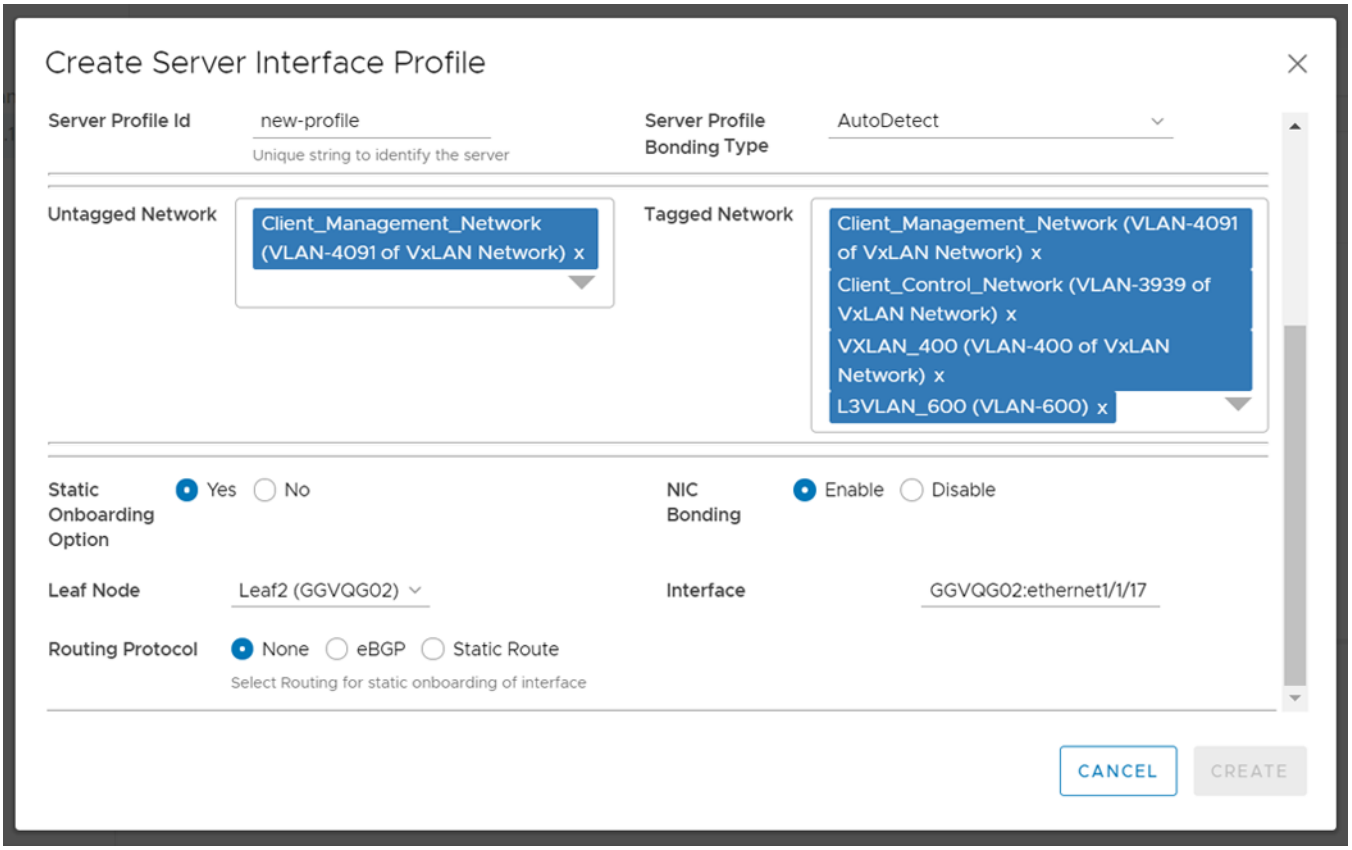
To create a server interface with new server profile:

1. Select the **Service Instance** > **Server Interface**.
2. Click **Create** to create a server interface profile and provide server interface ID, then select **New Server Profile**.

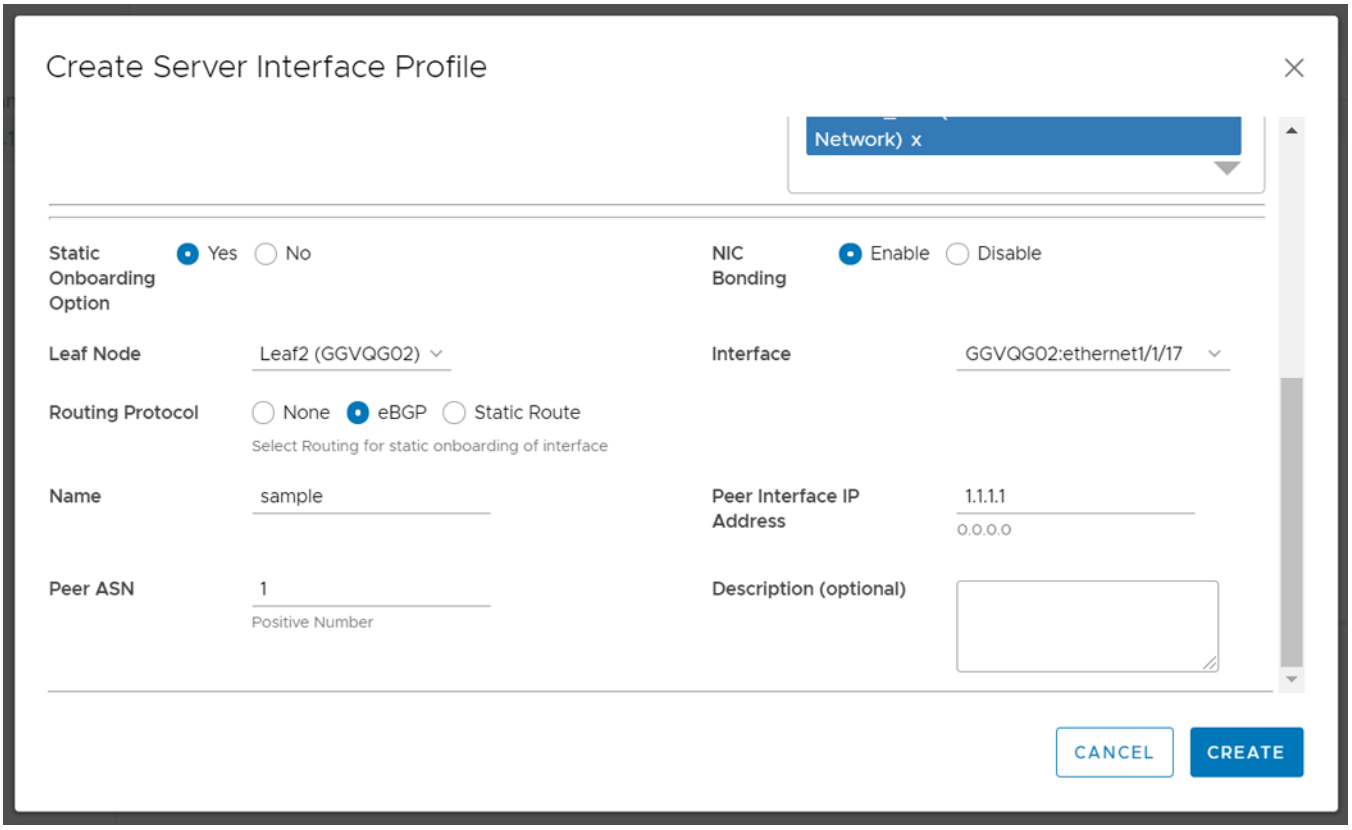
   NOTE: You can configure duplicate server interface ID. When using MAC address to onboard server interface, enter MAC Address without ":", for example, f8f21e2d78e0. For onboarding ESXi host Interfaces for zero touch automation, use the ESXi host VM NIC physical adapter MAC address without ":".
3. Select the **Server Profile Id** and **Server Profile Bonding Type** from the list, select the **Untagged Network** and **Tagged network**, enable or disable **NIC Bonding**, select **Static Onboarding Option** as **No**, and click **Create**.



4. (Optional) Select **Yes** for the **Static Onboarding Option**, add **Leaf Node** and **Interface** (where the server interface is connected), select the routing protocol as **None**, and click **Create**.

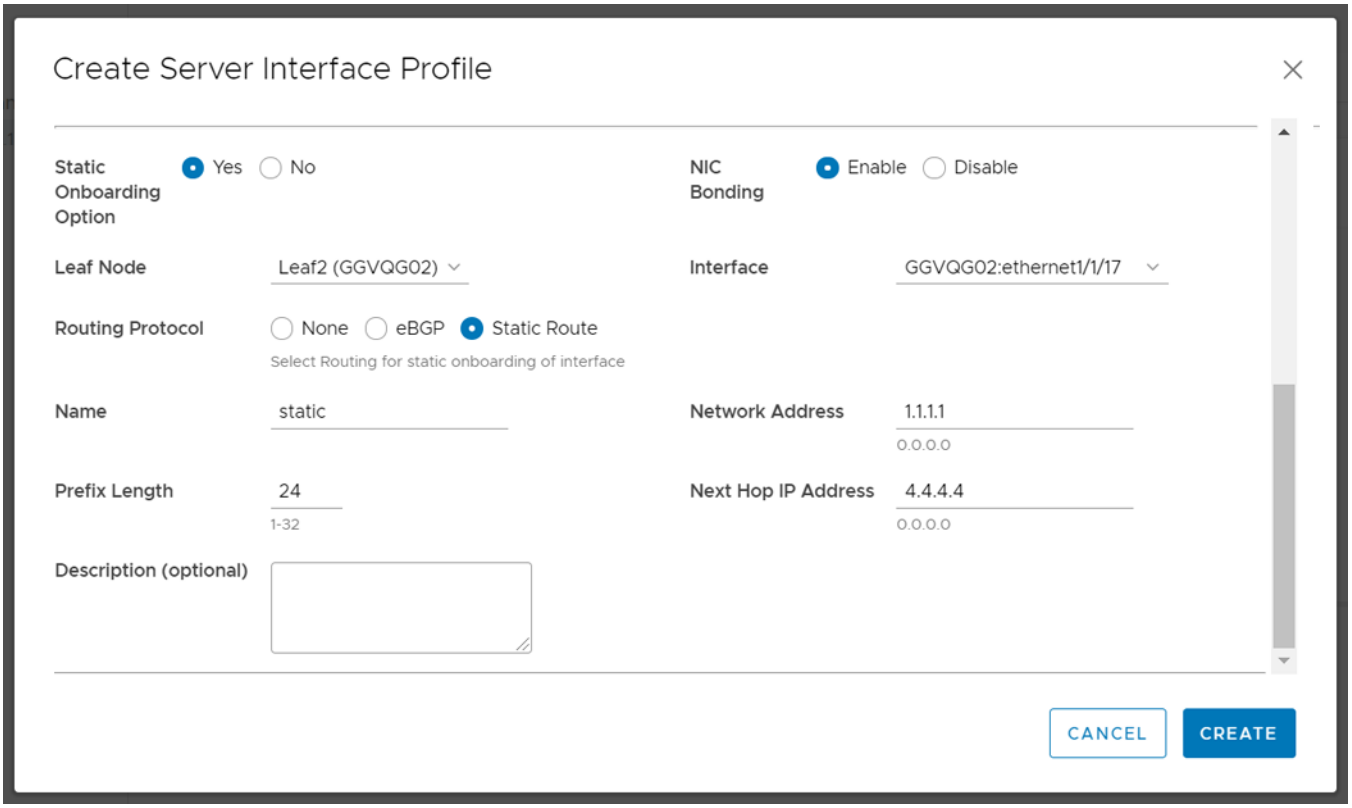


5. (Optional) Select **Yes** for the **Static Onboarding Option**, select **Leaf Node** and **Interface** (where the server interface is connected), select **eBGP**. Enter the eBGP routing template by entering the name, peer **ASN**, description, and peer interface **IP address**, and click **Create**.



NOTE: In static onboarding, the eBGP or static route routing protocol option is used for NSX-T deployment.

6. (Optional) Select **Yes** for the **Static Onboarding Option**, select **Leaf Node** and **Interface** (where the server interface is connected), select **Static Route**, enter the **Network Address** and **Next-Hop Address**, then click **Create**.



NOTE: You cannot delete any created server profile.

7. The system displays server profile and service interface creation successful messages.

NOTE: OMNI does not synchronize a statically onboarded interface when it is first added. For the synchronization to happen, a port-group change event on the vCenter must happen or a restart of the automation service for the specific vCenter and SmartFabric instance must occur.

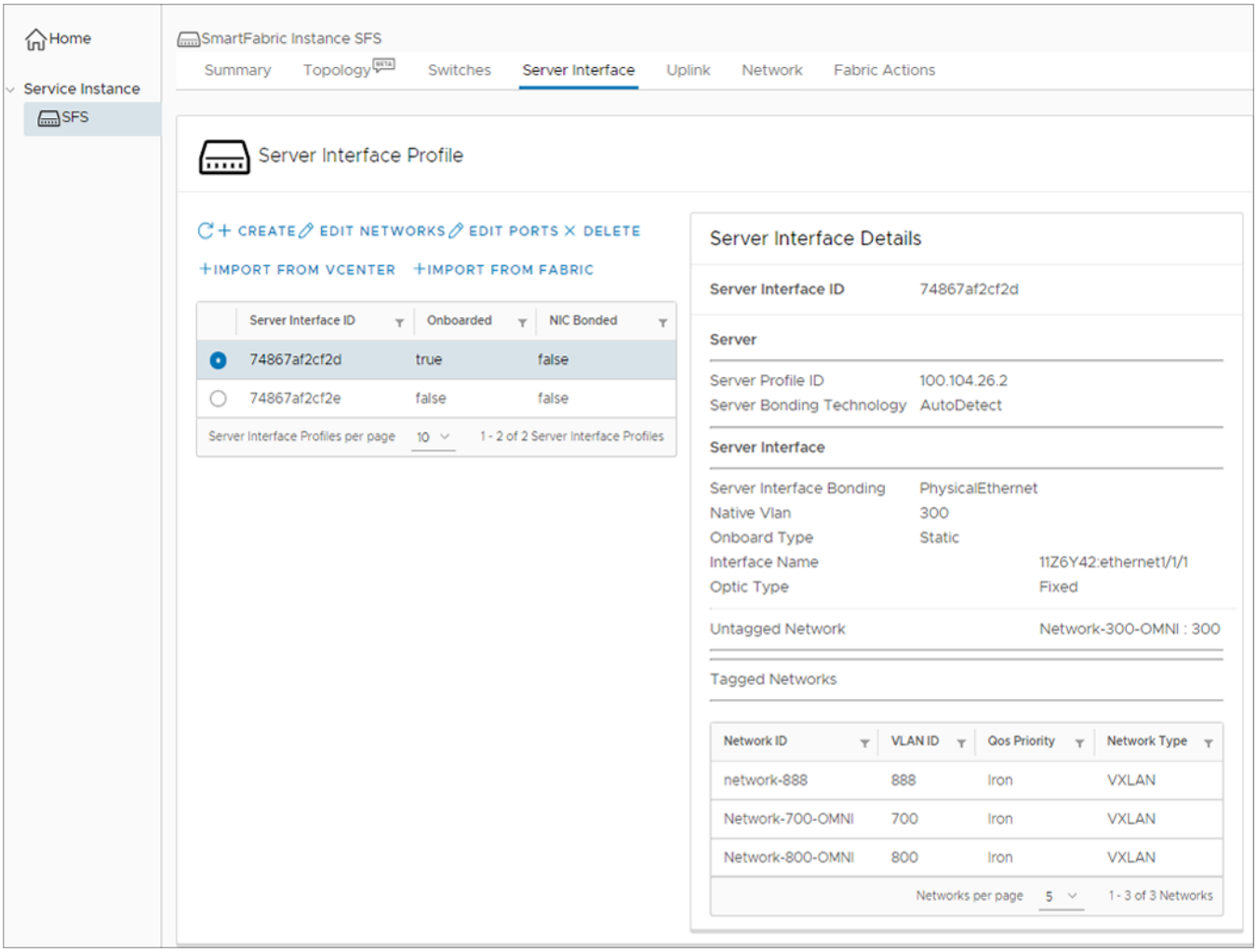
Edit networks and ports in a server interface profile

You can edit the network and port configuration in a server interface profile. You can also view the detailed information of a server interface profile.

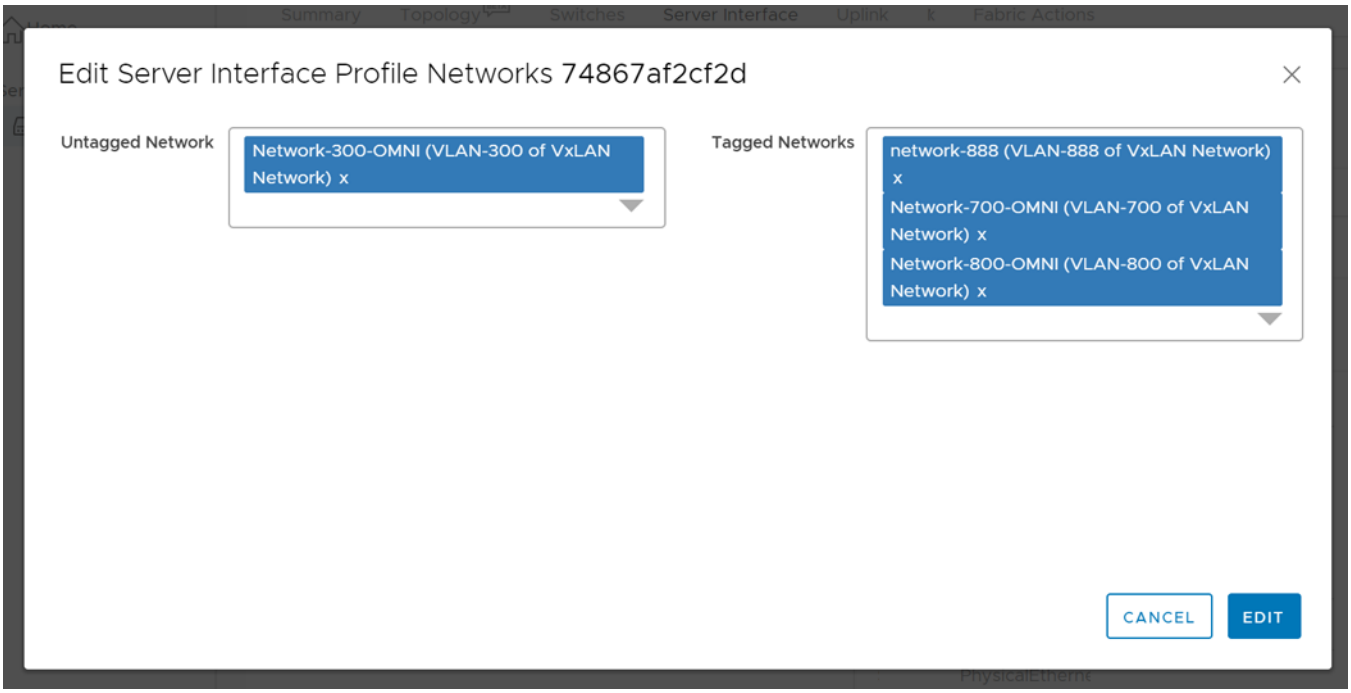
Select a server interface ID to view the properties of the profile on the right.

Edit networks on a server interface profile

1. Select the **Service Instance** > **Server Interface**.
2. Select the server interface ID from the list to view the detailed information.



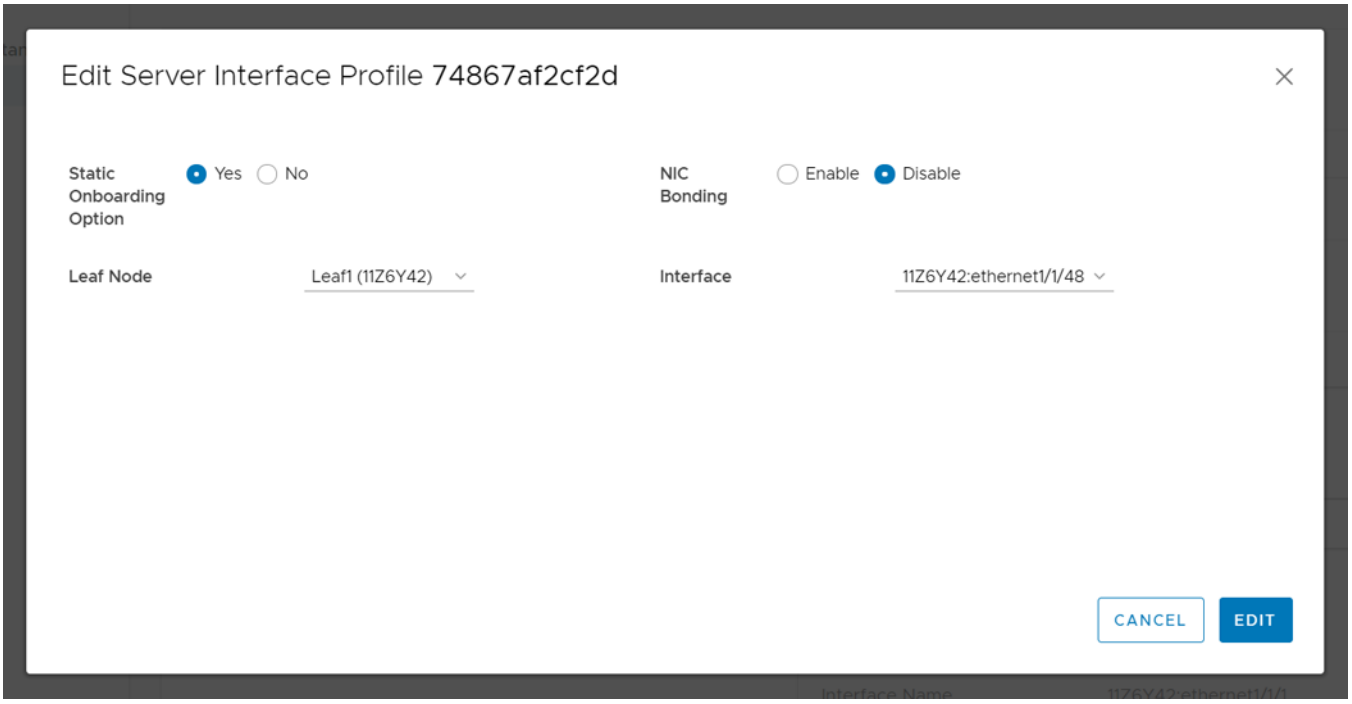
3. Select the server interface ID from the list, and click **Edit Networks**.
4. Edit the **Untagged Network** and the **Network** configuration for the profile, and click **Edit**.



5. The system displays the server interface profile update success message.

Edit ports on a server interface profile

1. Select the server interface ID from the list, and click **Edit Ports**.
2. Edit the **Static Onboarding Option** and the **NIC Bonding** configuration for the profile, and click **Edit**.

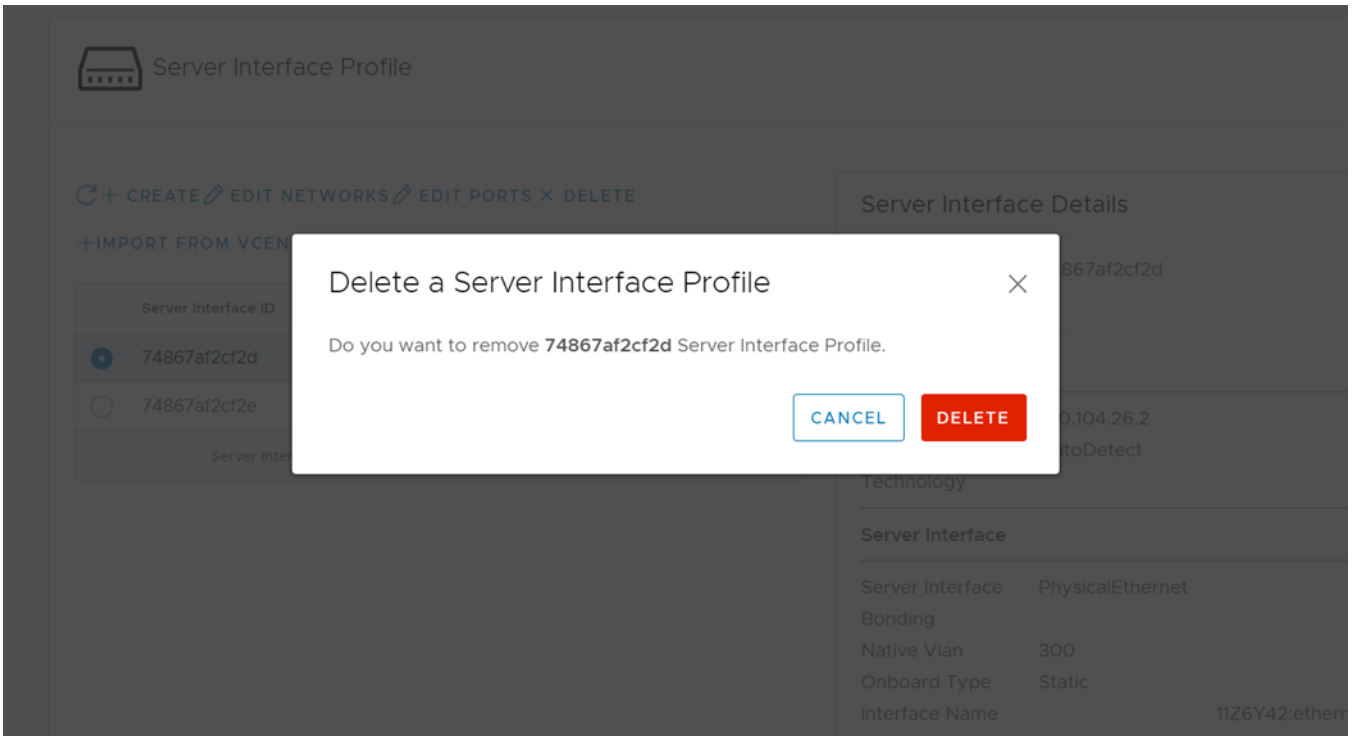


3. The system displays the server interface profile update success message.

Delete a server interface profile

You can delete a service interface profile from the service instance. To delete:

1. Select the server interface profile from the displayed list, and click **Delete**.



2. Click **Delete** to confirm.

Import ESXi host profiles from vCenter

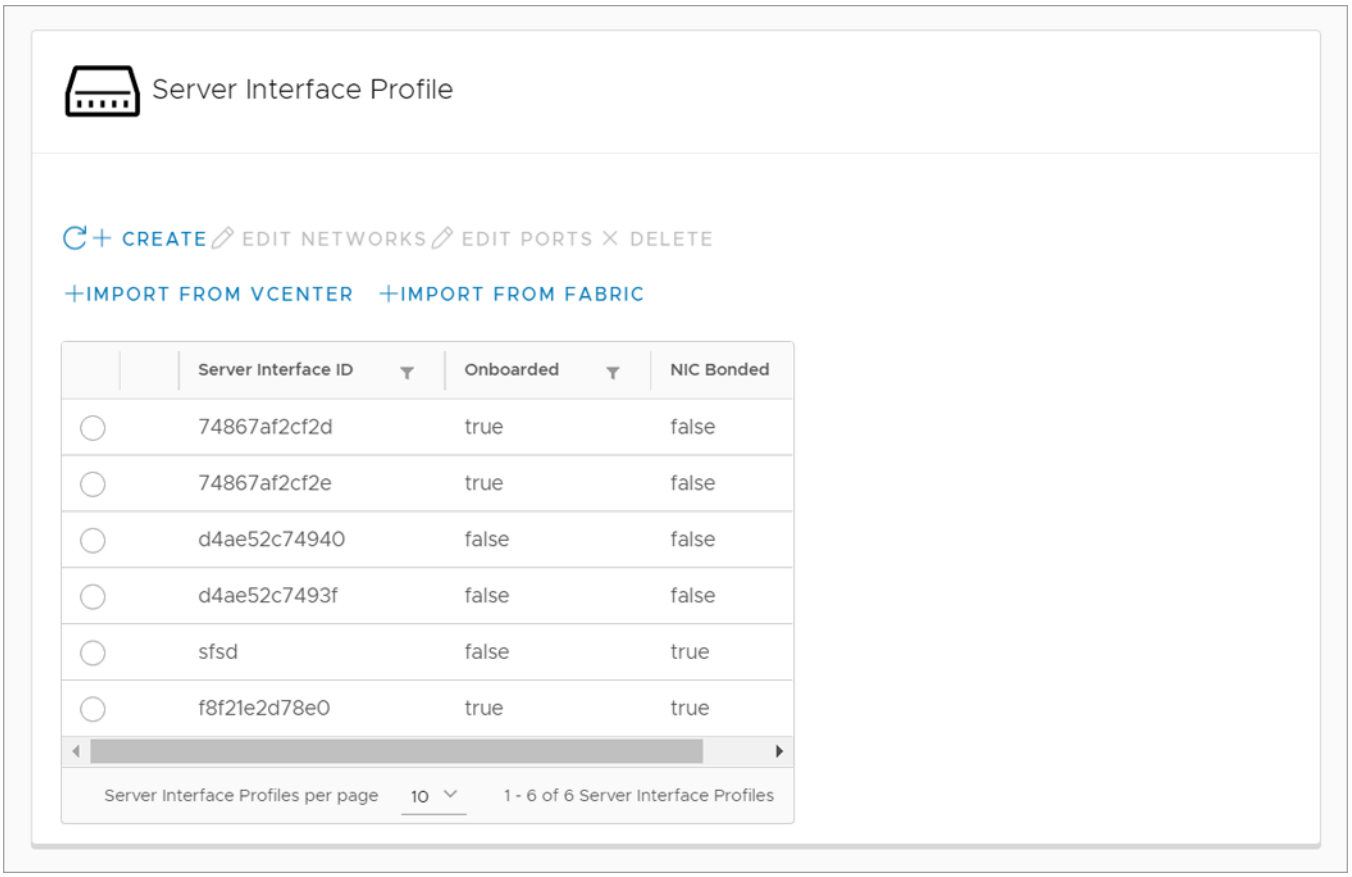
Automate onboarding of server interface profile by importing:

ESXi host profiles from the registered vCenter—Use this feature to migrate the existing ESXi hosts that are already connected to the vCenter and ready to be onboarded on to the fabric. The feature imports all the required servers to onboard on to the SFS instead of manually configuring the server interface one at a time.

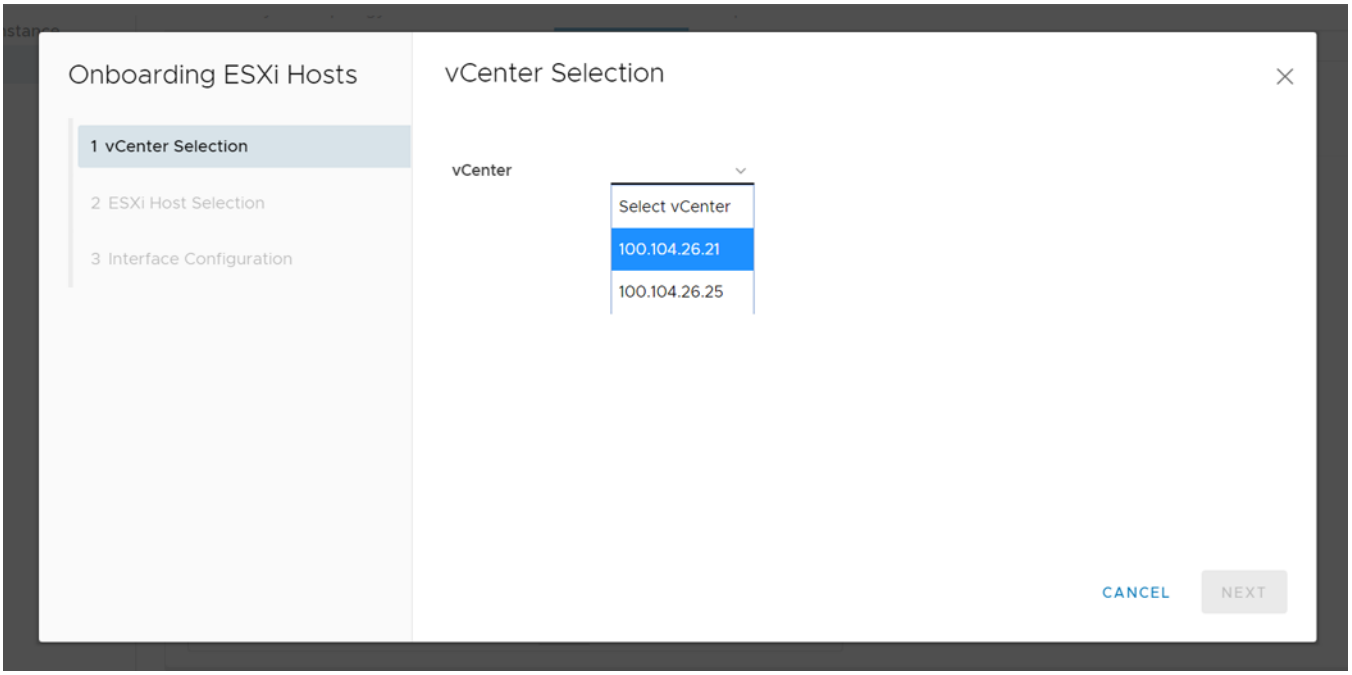
OMNI retrieves data center, clusters, hosts, VM NICs, and networks for the registered vCenter. Create server interface profiles for the set of available VM NICs in ESXi hosts from vCenter.

NOTE: In vCenter, enable LLDP on Distributed Virtual Switch of ESXi host to discover the interfaces automatically.

1. Select the **Service Instance** > **Server Interface**.
2. Click **Import from vCenter** to launch the **Onboarding ESXi Hosts** wizard.

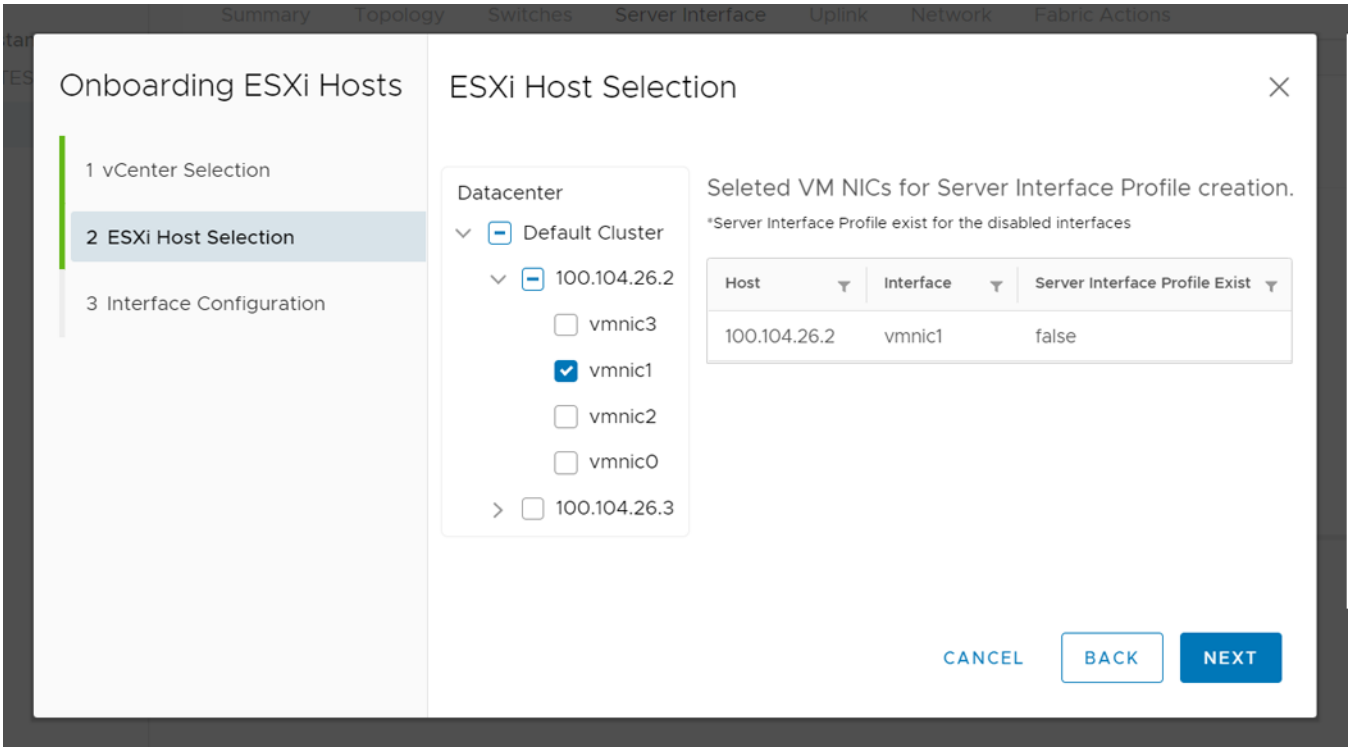


3. Select the **vCenter** from the list, and click **Next**.

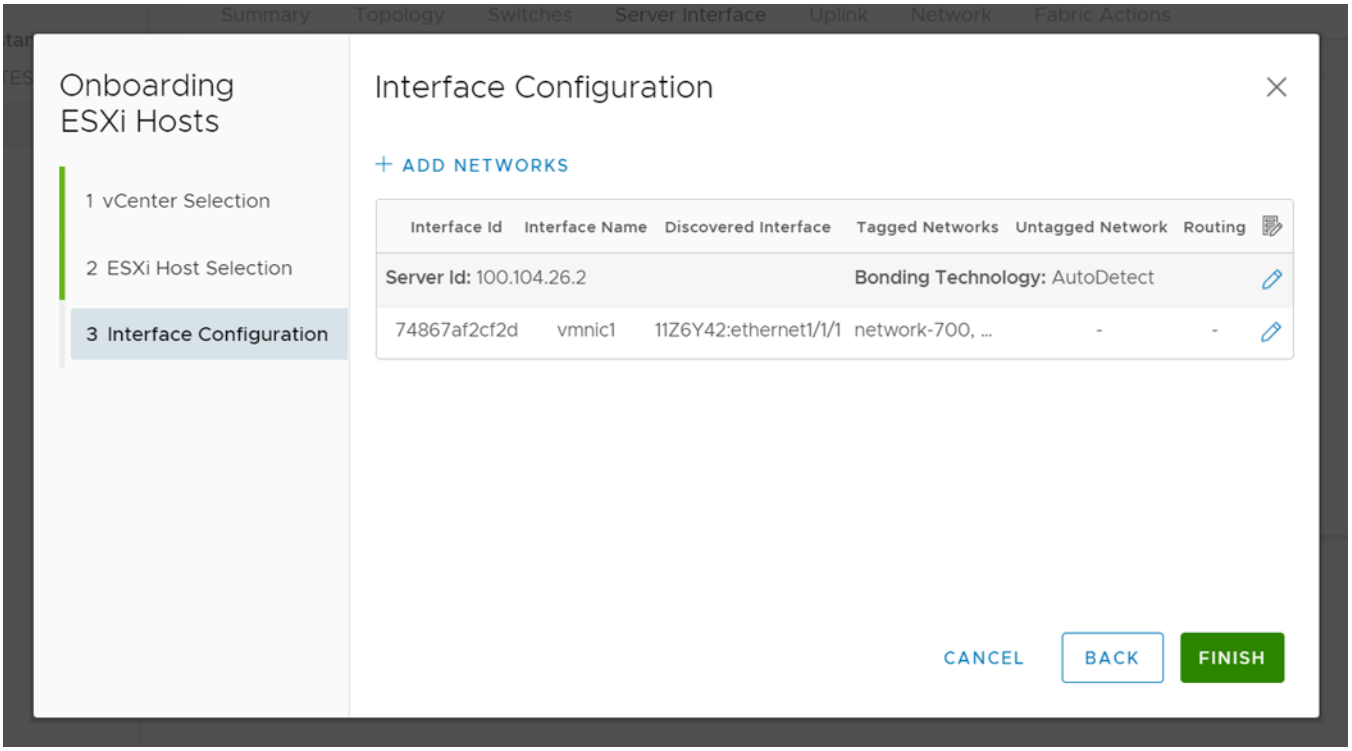


4. Select the relevant cluster, the ESXi host, or the VM NICs available on the ESXi host. **ESXi Host Selection** window displays the server profile status of the interfaces on the right.

   NOTE: You cannot select the VM NICs that are already part of a server interface profile in SmartFabric.

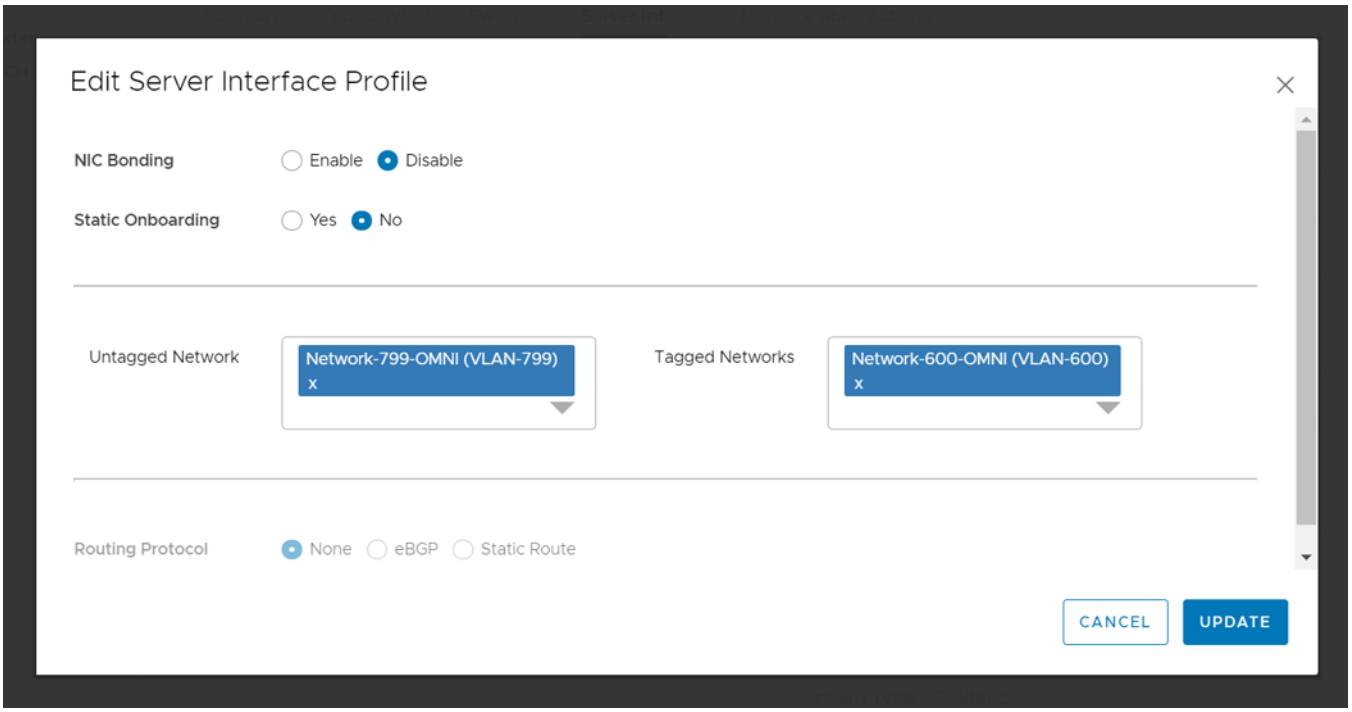


5. Click **Next** to complete the selection of the VM NICs.
6. The **Interface Configuration** screen displays the list of selected VM NICs.



7. (Optional) Click **Edit** icon available for each interface to edit the server profile information.

   Edit the NIC bonding configuration and **Static Onboarding**. If the static onboarding is **No**, select an **Untagged Network** and one or more **Tagged Networks** and click **Update**.



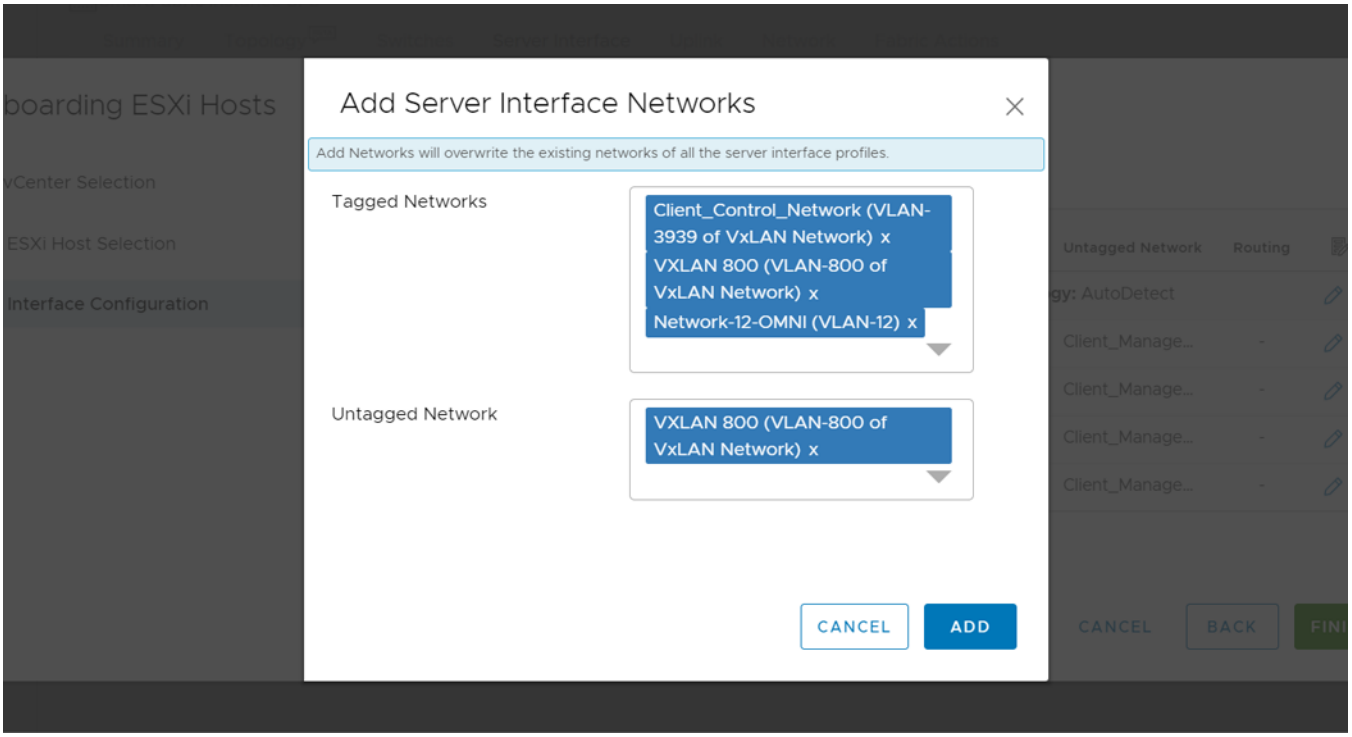
NOTE: You cannot select same network for both untagged and tagged networks.

(Optional) If the static onboarding is **Yes**, select **Leaf Node** and **Interface** (where the server interface is connected), select the **Routing Protocol**.

- (Optional) Select the **Routing Protocol** as **None**, and click **Update**.
- (Optional) Select the **Routing Protocol** as **eBGP**, enter the **ASN** and **IP address**, and click **Update**.
- (Optional) Select the **Routing Protocol** as **Static Route**, enter the **Network Address** and **Next-Hop Address**, and click **Update**.

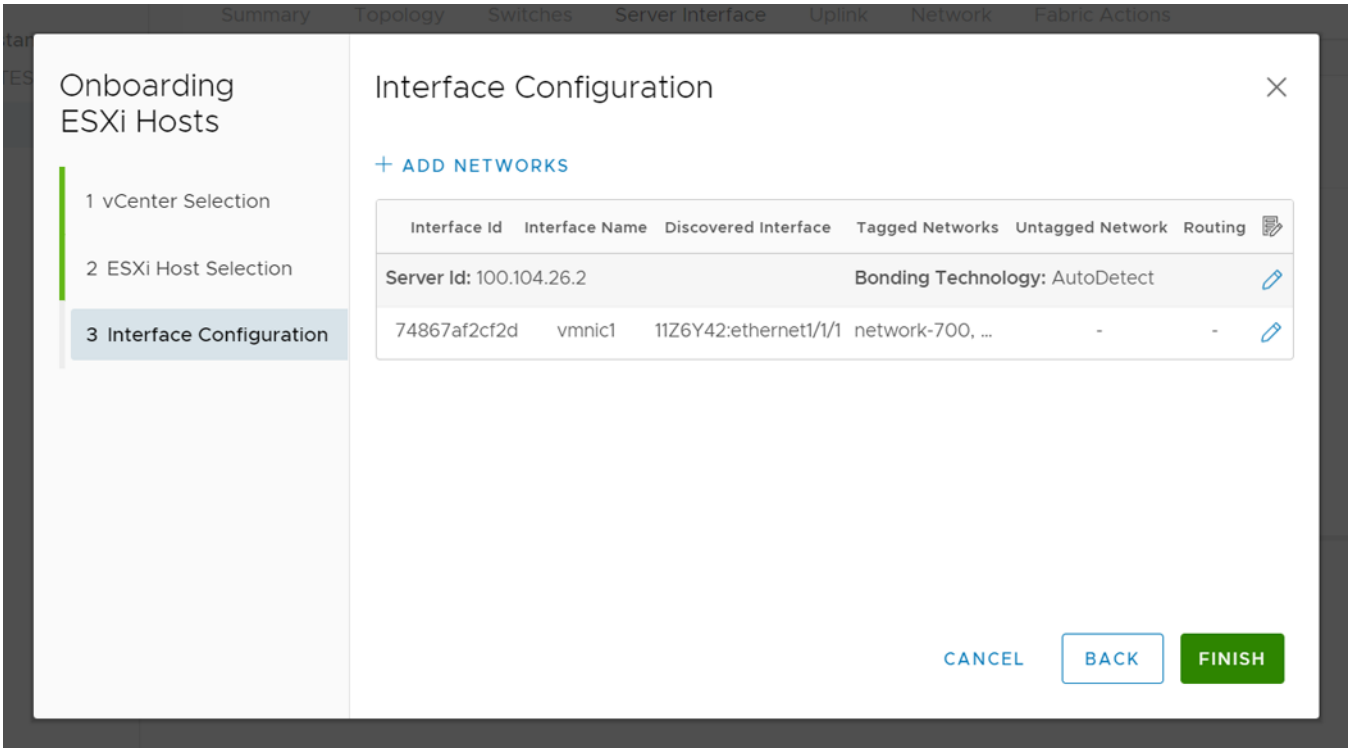
NOTE: You cannot edit the server profile that is already configured in the system.

8. Click **Add Networks** to associate the networks that are part of the fabric for all the server interface profile. Select the networks for **Tagged Networks** and **Untagged Network** from the list, and click **Add**.



NOTE: Add networks overwrite the existing networks of all the server interface profiles.

9. Click **Finish** after all the configurations are complete.



10. The system displays the server interface profile update success message.

Import SmartFabric discovered server interfaces

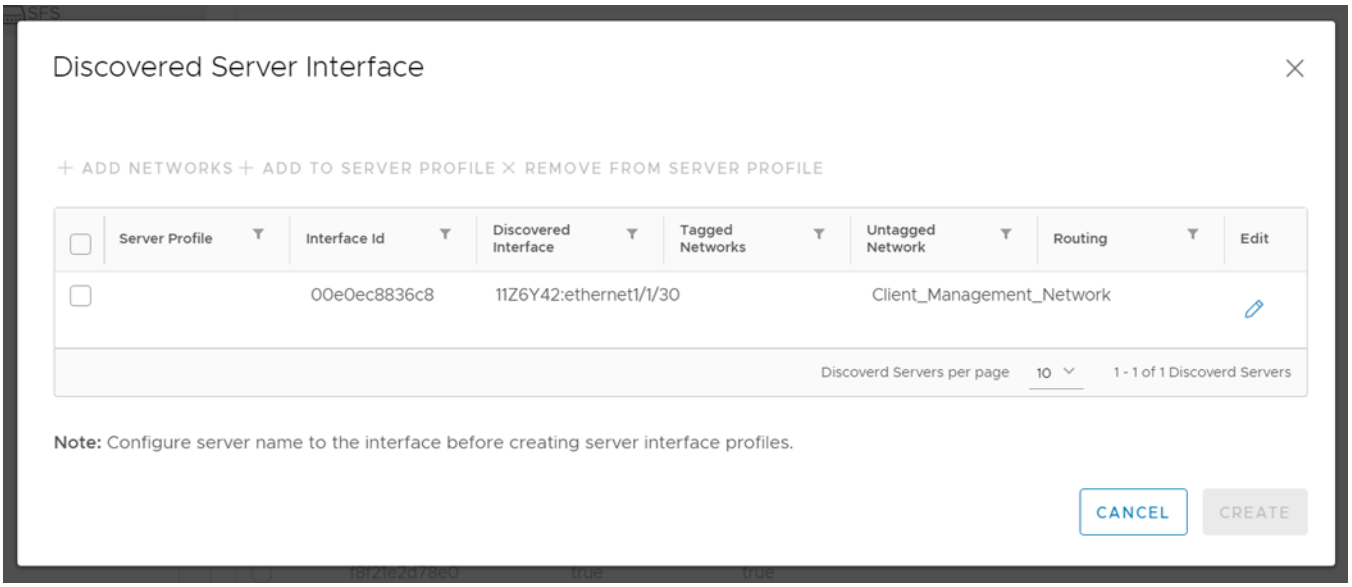
Automate onboarding of server interface profile by importing:

Profiles that are discovered by the SmartFabric—SFS discovers the following types of servers apart from VxRail:

- PowerStore-X
- PowerStore-T

Use this feature to onboard new servers that support the Dell-specific LLDP TLVs. When the servers are connected to the fabric, SFS discovers the servers automatically, and the OMNI onboards the discovered servers as part of this workflow. OMNI retrieves a list of server interfaces that are discovered by the SFS.

1. Select **Service Instance** > **Server Interface**.
2. Click **Import from Fabric**. **Discovered Server Interface** window appears with the list of discovered interfaces.



NOTE: The interface that is already associated with a server interface profile is not listed in the discovery table.

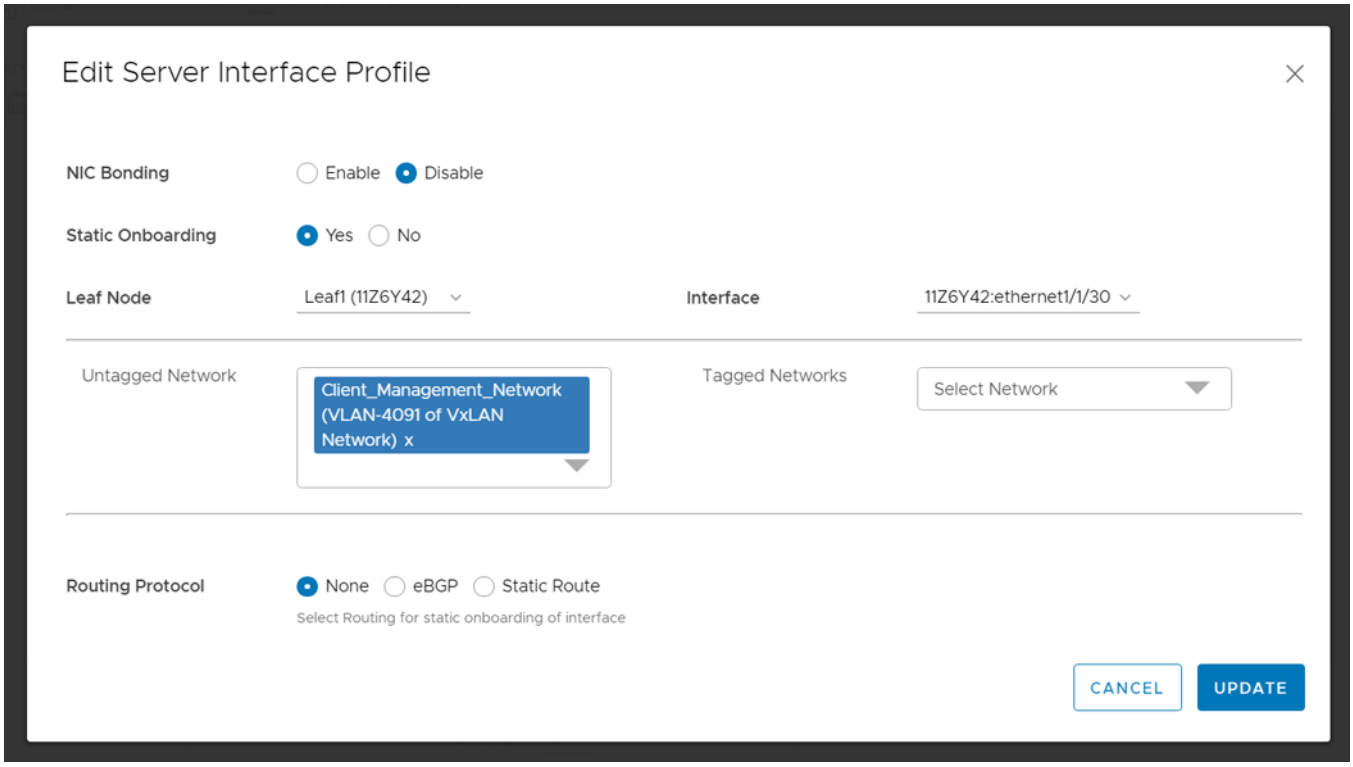
3. Edit the server profile information of each interface using the **Edit** option available at the end of each row.

   Edit the **NIC Bonding** configuration and **Static Onboarding**. If the static onboarding is **No**, select an **Untagged Network** and one or more **Tagged Networks** and click **Update**.

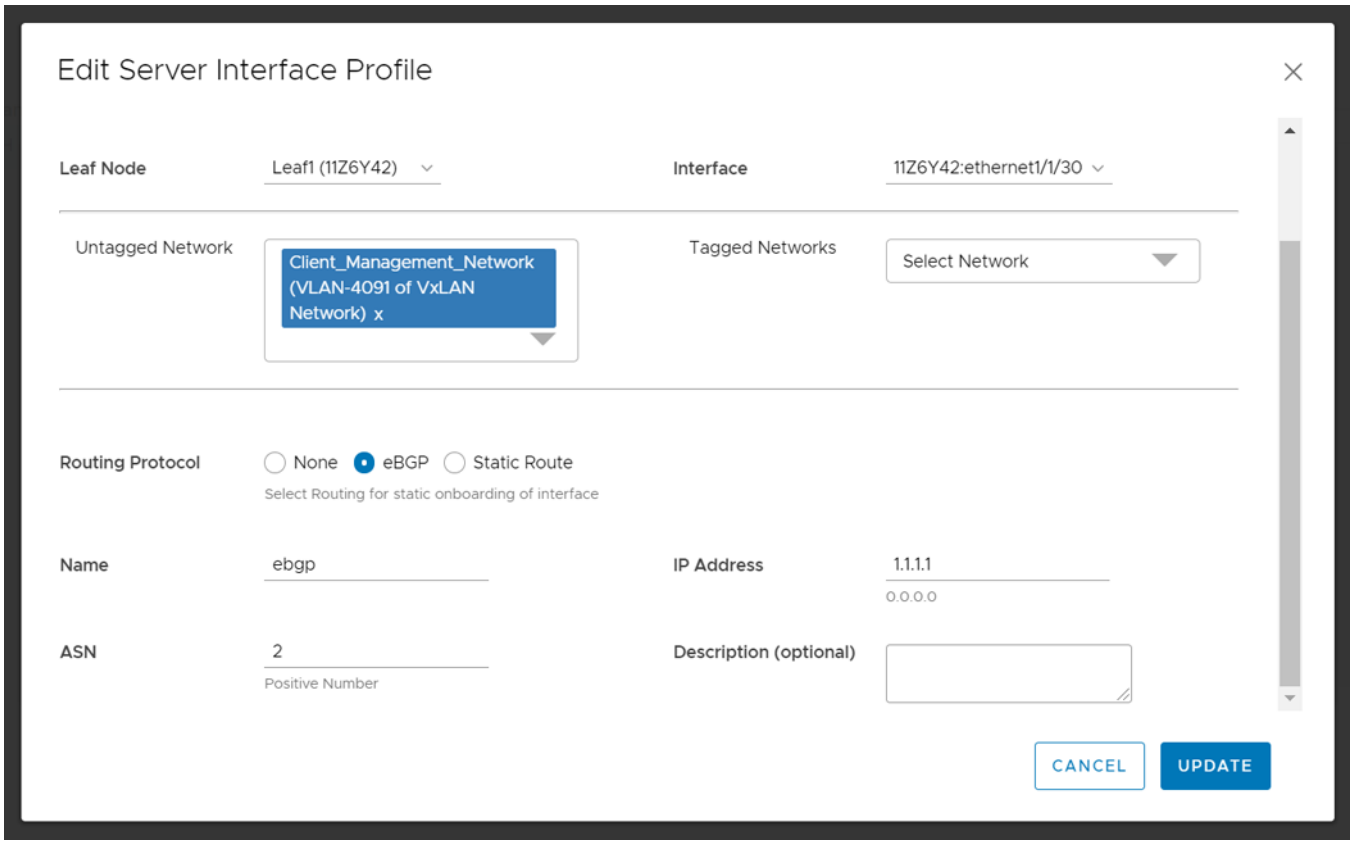
   NOTE: You cannot select same network for tagged and untagged network.

   (Optional) If static onboarding is **Yes**, select **Leaf Node** and **Interface** (where the server interface is connected), select the **Routing Protocol**.

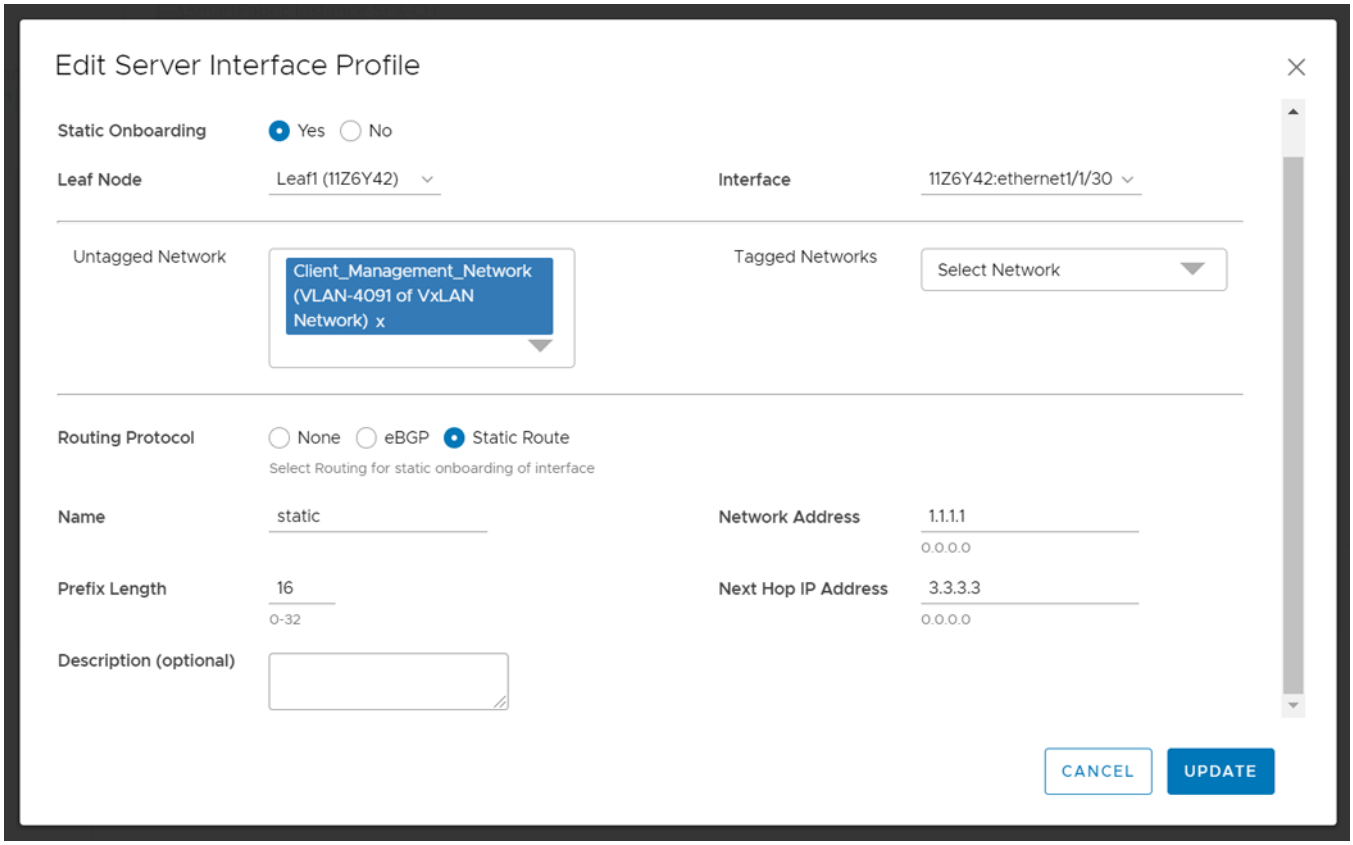
   - (Optional) Select the **Routing Protocol** as **None**, and click **Update**.



- (Optional) Select the **Routing Protocol** as **eBGP**, enter the **ASN** and **IP address**, and click **Update**.



- (Optional) Select the **Routing Protocol** as **Static Route**, enter the **Network Address** and **Next-Hop Address**, and click **Update**.

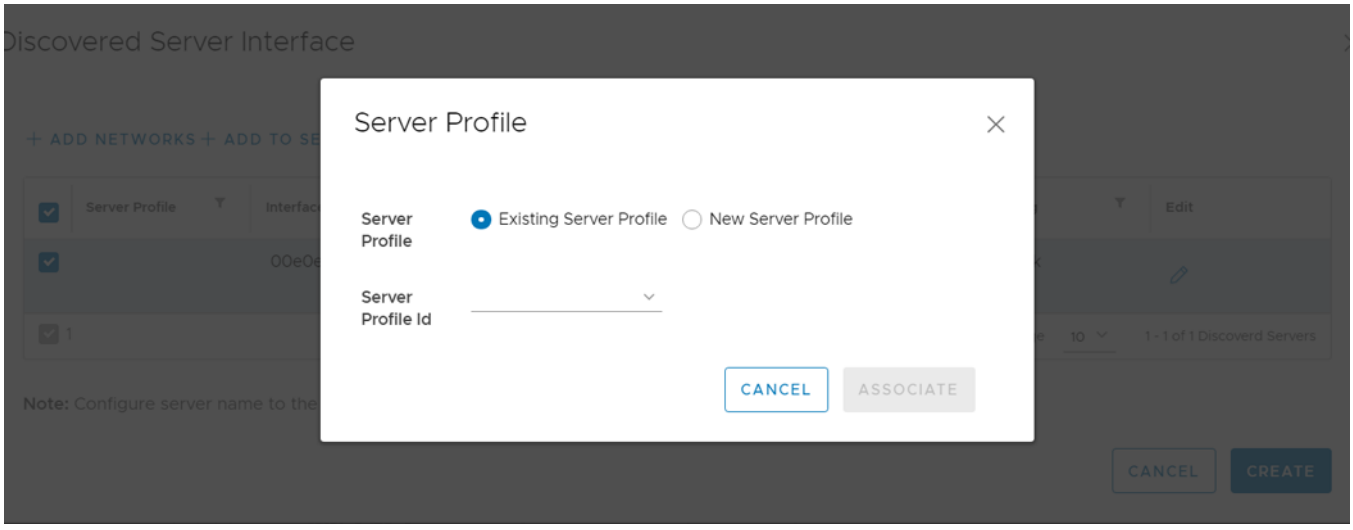


4. Select one or multiple discovered interfaces, add the service profile and networks, and click **Update**. For more information about adding server profile and networks, see *Add to Server Profile* and *Add networks* sections.

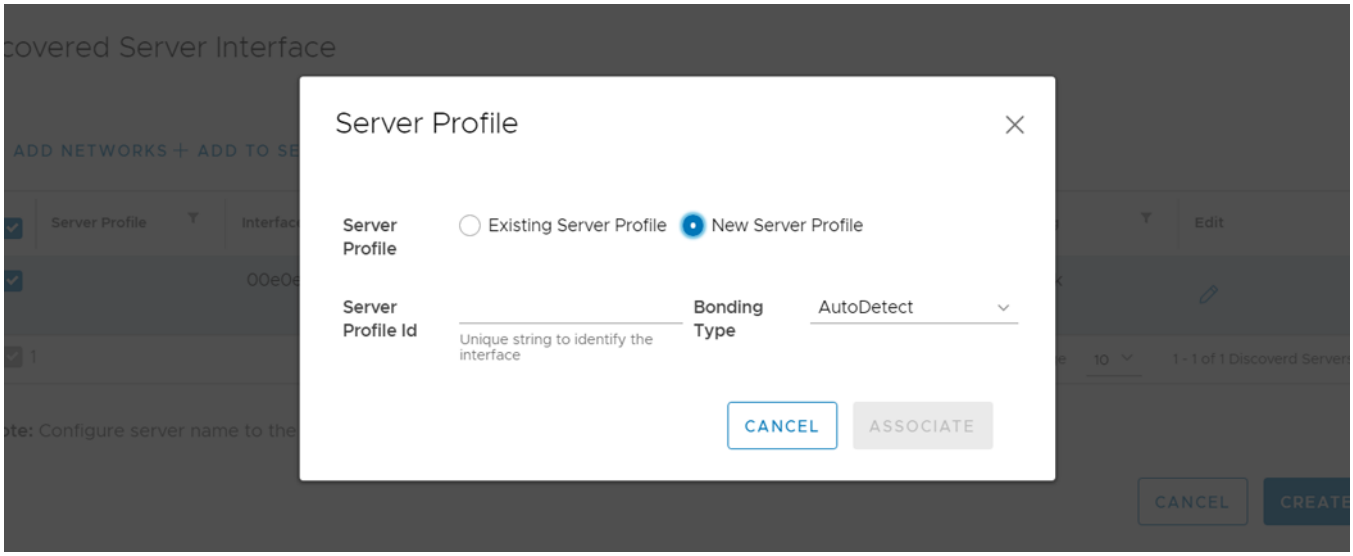
Add to Server Profile

To add the discovered interfaces to a new or existing server profile:

1. Select one or more discovered interfaces, and click **Add to Server Profile**.
2. Select the server profile to which you want to add the discovered server interfaces.
   - Select **Existing Server Profile**—Select the **Server Profile Id** to associate the interface with the existing server profile, and click **Associate**.



   - Select **New Server Profile**—Enter the **Server Profile Id** and **Bonding Type** to associate the interface with the new server profile, and click **Associate**.

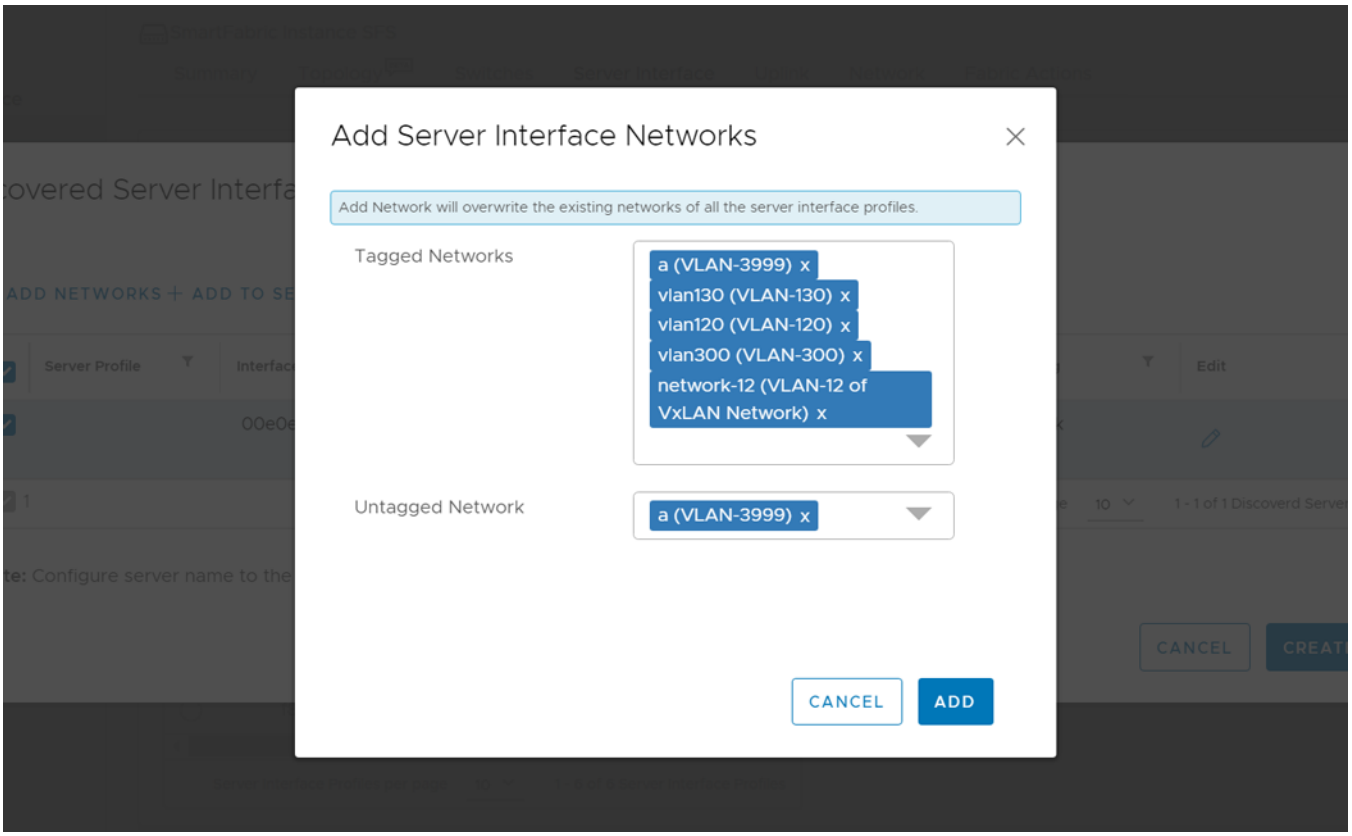


3. The system displays the server interface profile association success message.

Add Networks

To add the networks to the discovered interfaces:

1. Select one or more interfaces from the list, and click **Add Networks**.
2. Associate the networks with the discovered interfaces, and click **Add**.
   - Select one or multiple networks for **Tagged Networks**.
   - Select a single network for **Untagged Network**.



NOTE: Add networks overwrite the existing networks of all the server interface profiles.

3. The system displays the server interface networks addition success message.

Remove from server profile

To remove the interface from the server profile, select one or more interfaces from the list, and click **Remove from Server Profile**.

Configure and manage uplinks

Configure an uplink and manage the uplinks that are available in the service instance.

Using the **Uplinks** tab, you can:

- View the list of uplinks created in the service instance.
- Create an uplink.
- Edit network and port configuration for an uplink.
- Delete a created uplink.

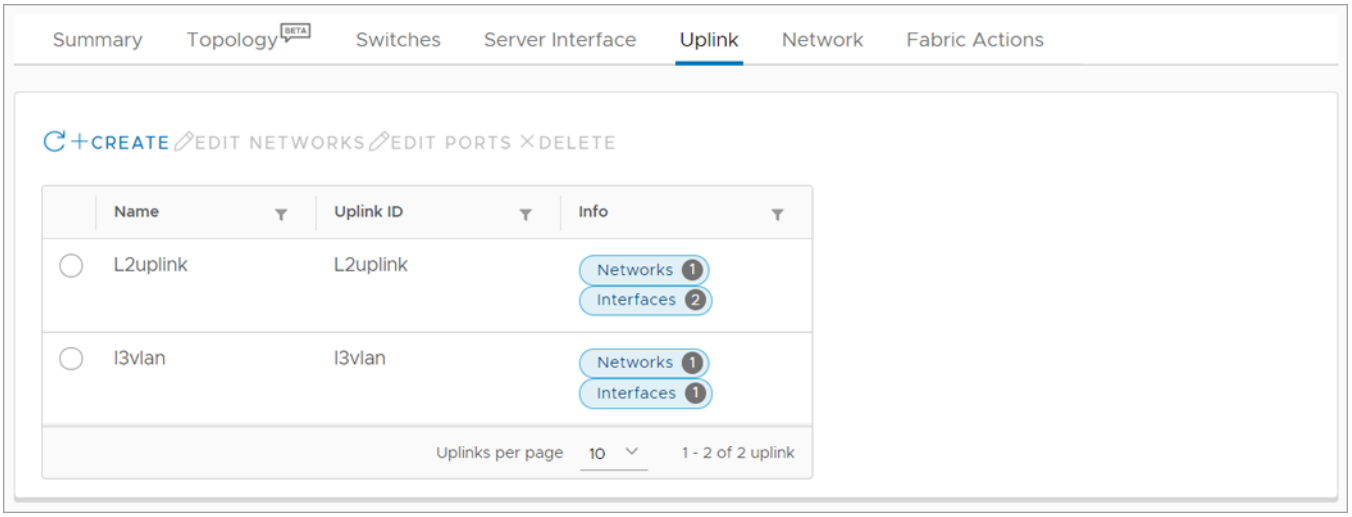
You can create uplinks with available interfaces which are not part of an existing uplink, server connected ports, part of a fabric automation, or jump port.

There are two types of uplinks—L2 and L3, and there are two types of L3 uplinks—L3 VLAN and L3 routed interface. Once you have created an uplink, you can then associate networks to the uplink and change or modify interfaces. These user-managed uplinks require configuration of networks through SmartFabric vCenter.

NOTE: If you delete an uplink, any unused networks and ports can be used for future use.

View Uplinks summary

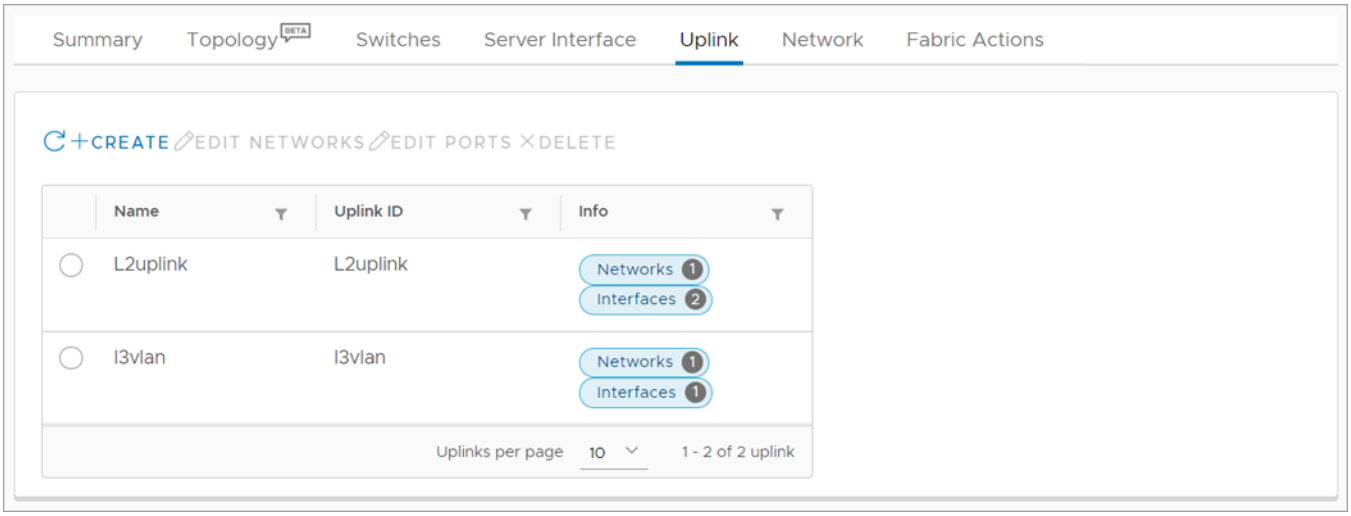
From the left pane, select the **Service Instance**, then select **Uplink**.



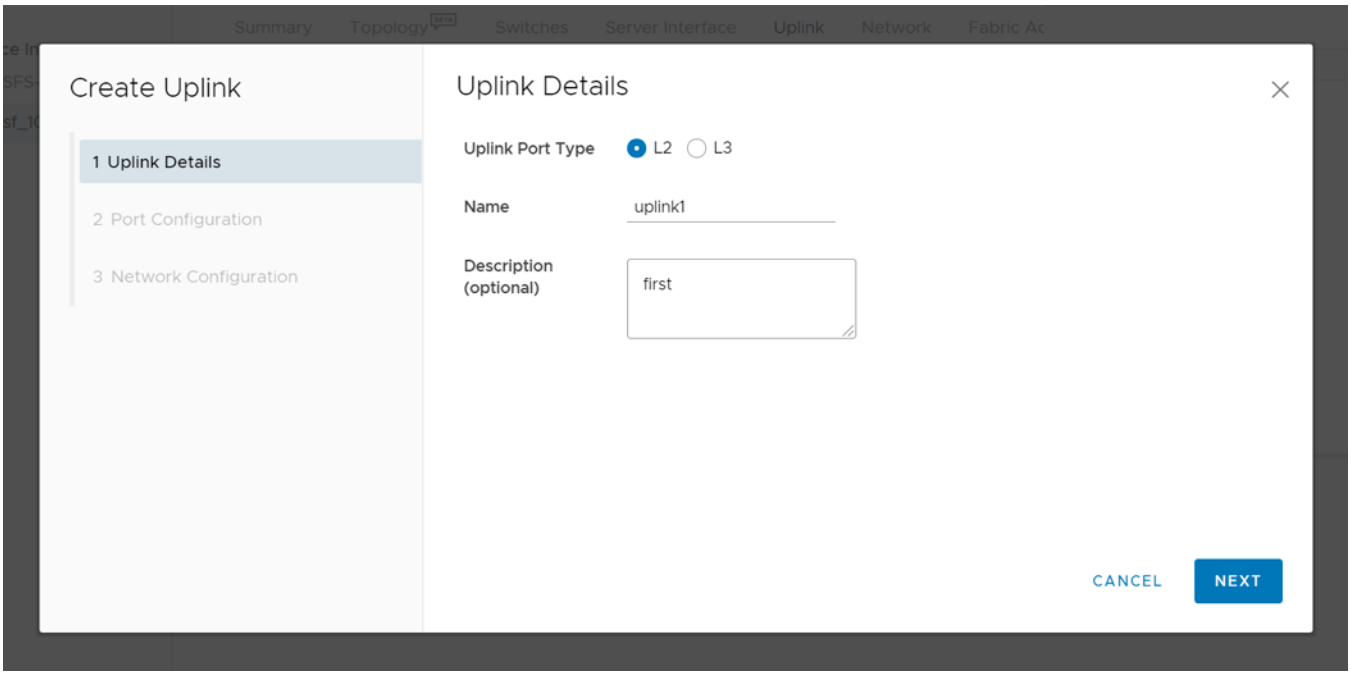
Create L2 Uplink

You can create an uplink by selecting the fabric with a unique name, and select the interfaces, and networks to create a user uplink.

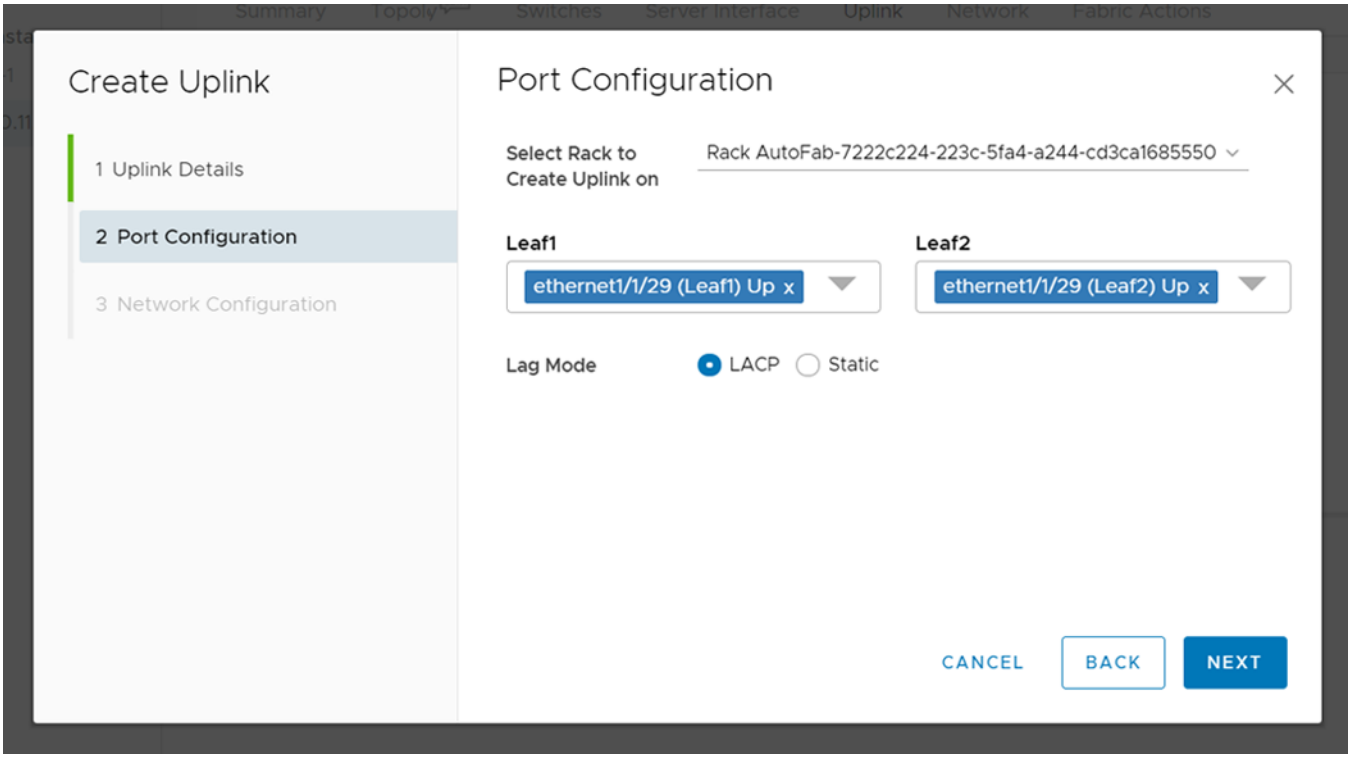
1. Select **Uplink**, then click **Create**.



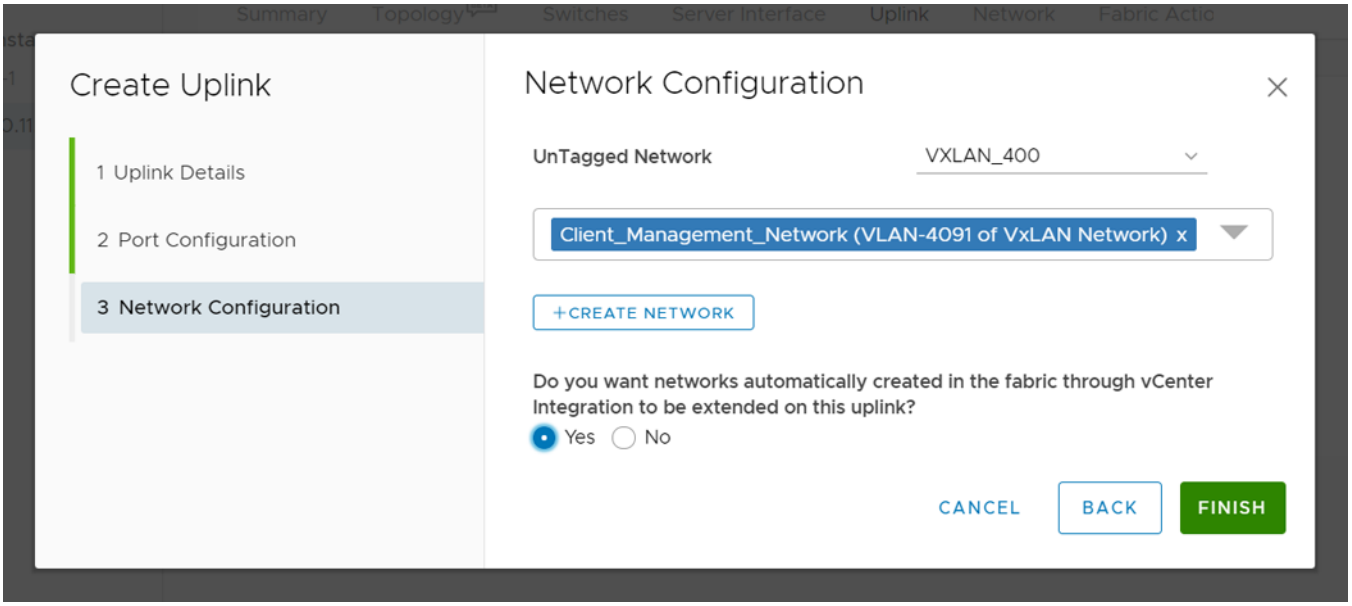
2. Enter the uplink port type as **L2**, a **Name**, an optional description, then click **Next**.



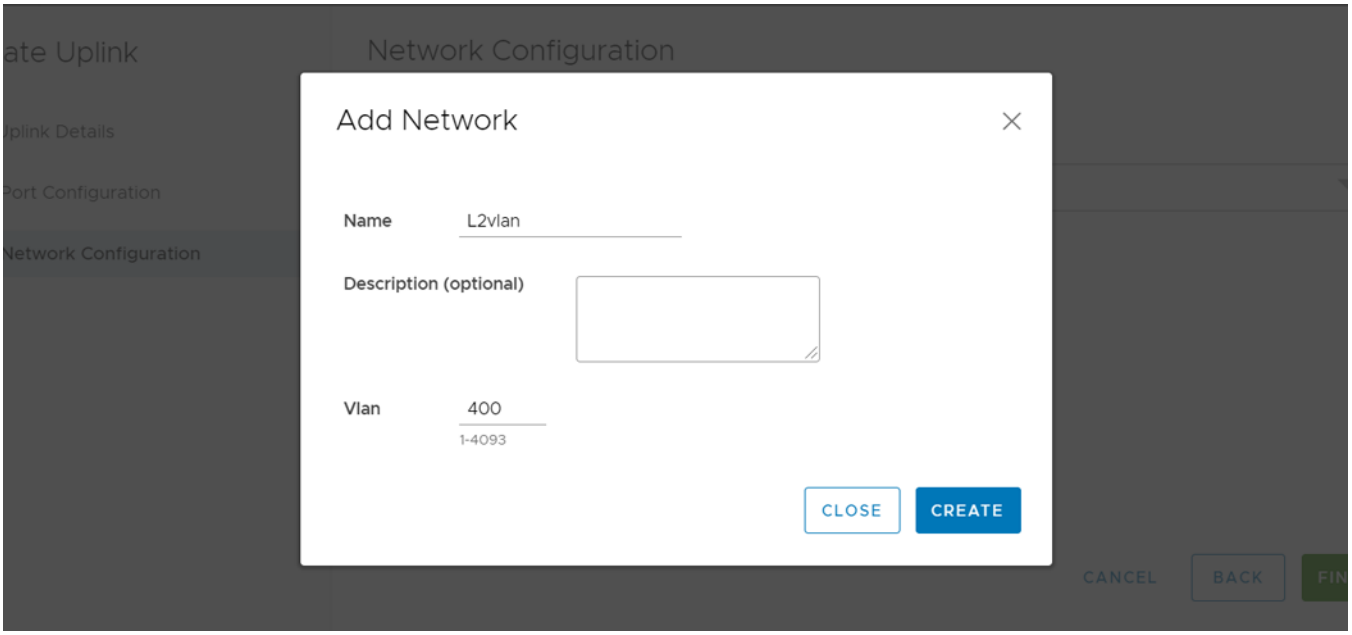
3. Enter the port configuration by selecting the rack to create the uplink on, select the interfaces, the **LAG Mode** (LACP or Static), then click **Next**.



4. Select the untagged network, the OMNI network, and Select **Yes** or **No** to integrate the networks that are created automatically in the fabric through vCenter on this uplink.



5. (Optional) Click **Create Network** to associate a network with the uplink. Enter the name of the network, optional description, and the VLAN number.



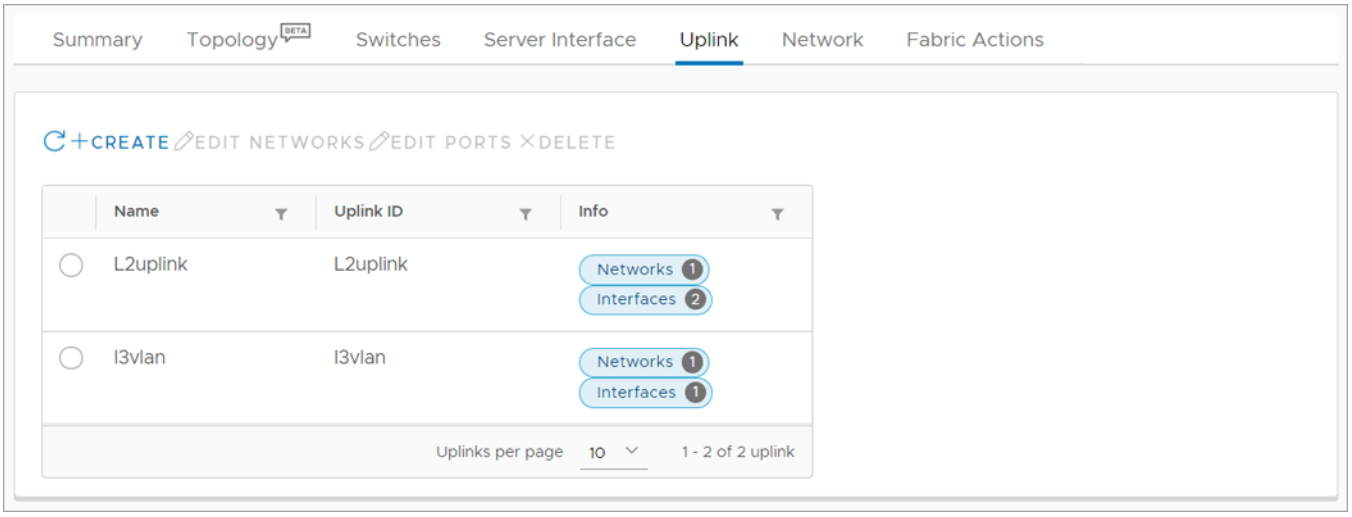
6. Click **Finish** to complete the L2 uplink creation.
7. The system displays user uplink creation success message.

Create L3 Uplink

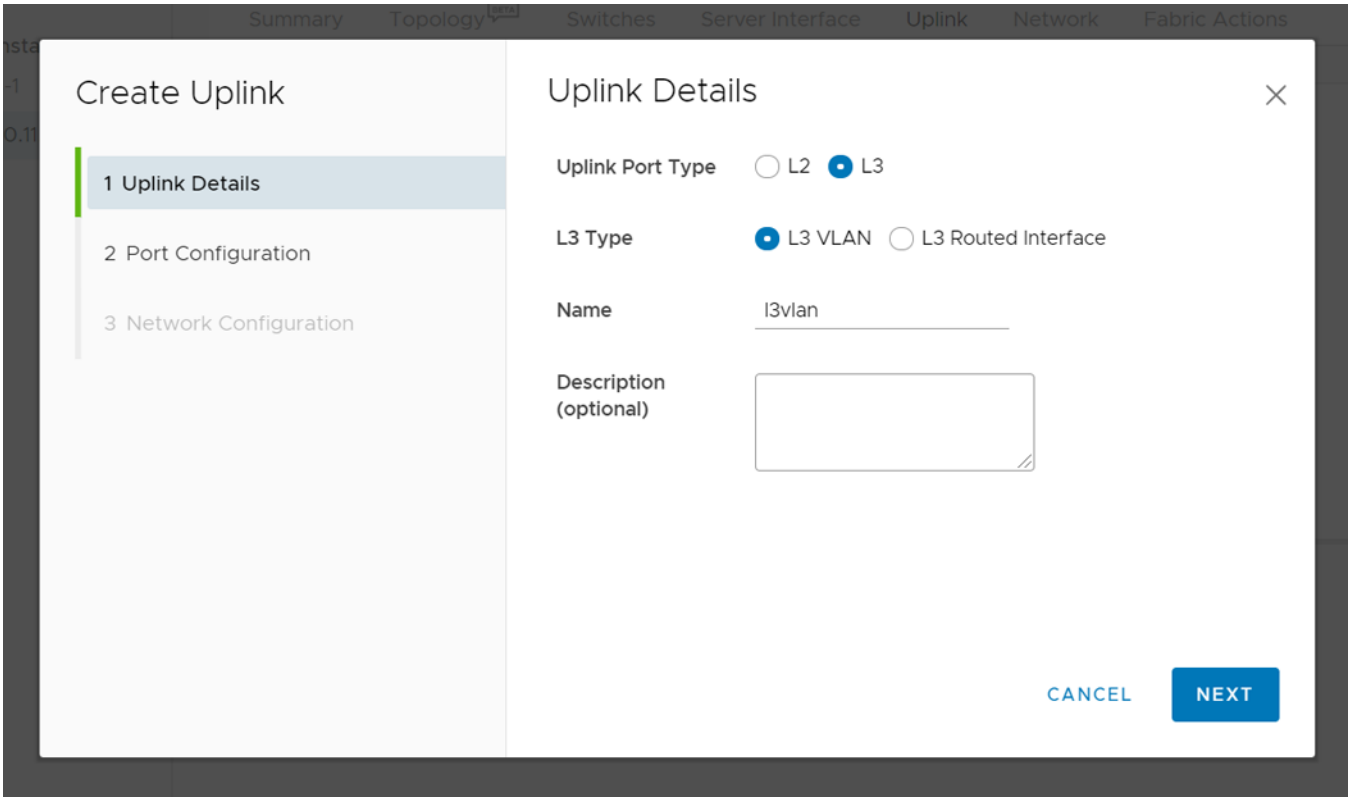
Create an L3 uplink of L3 VLAN or L3 routed interface types.

Create L3 VLAN uplink

1. Select the **Service Instance** > **Uplink**, and click **Create**.

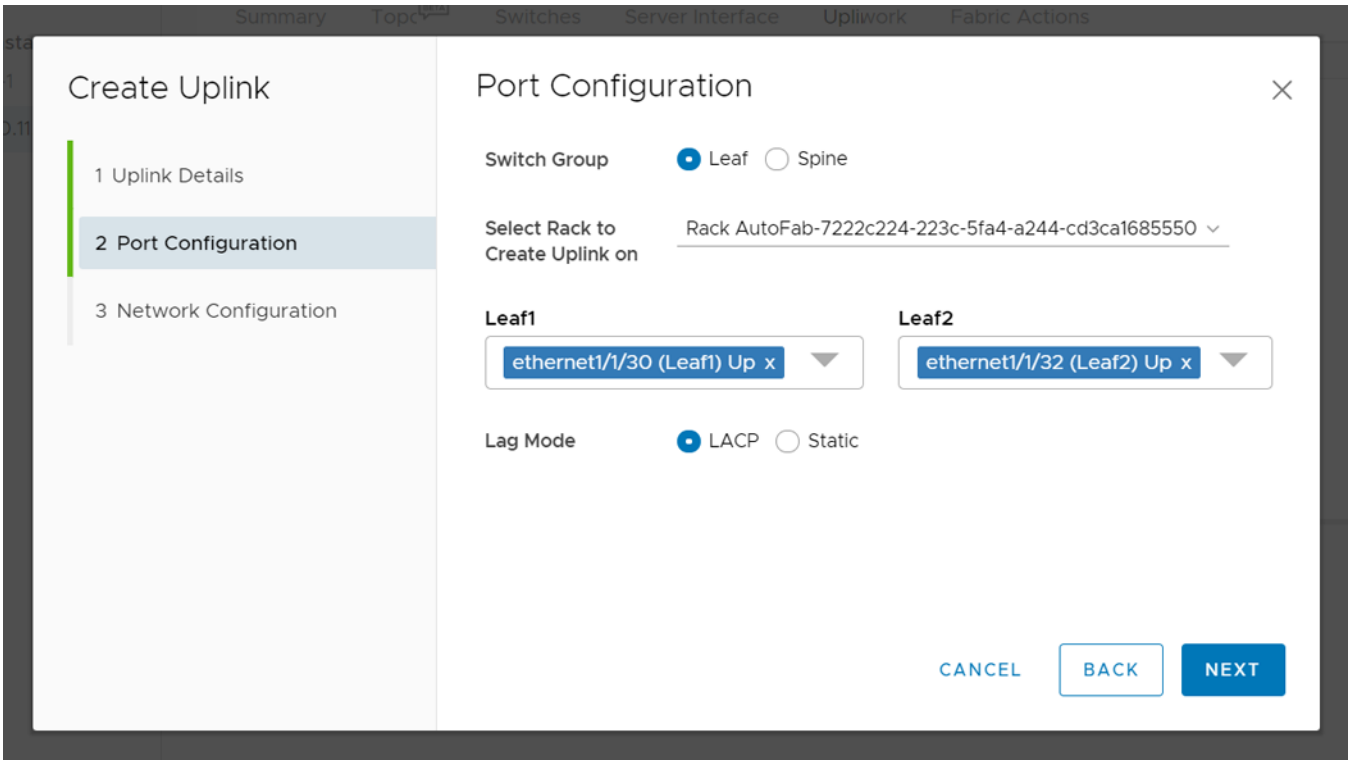


2. Select **L3** for the uplink port type, select **L3 VLAN**, enter the **name** for the uplink, and optional description, then click **Next**.

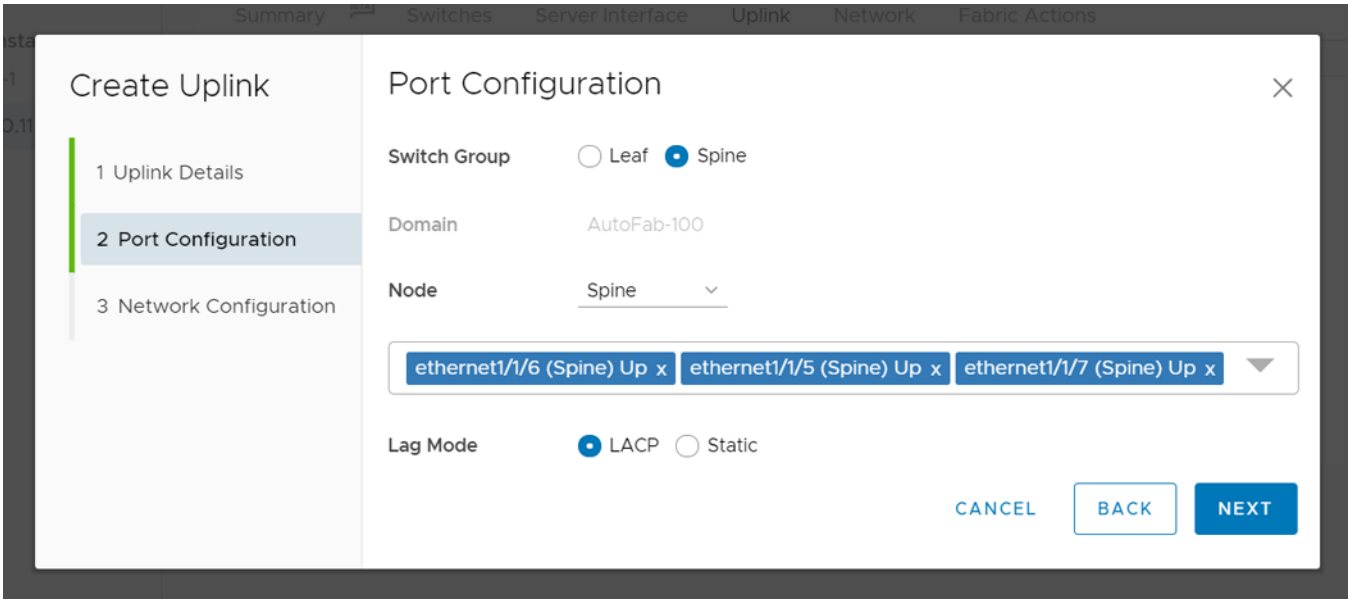


3. Select the **Switch group** (Leaf or Spine), select the **rack** to create the uplink on, select the **interfaces**, select **LACP** for the LAG mode, then click **Next**.

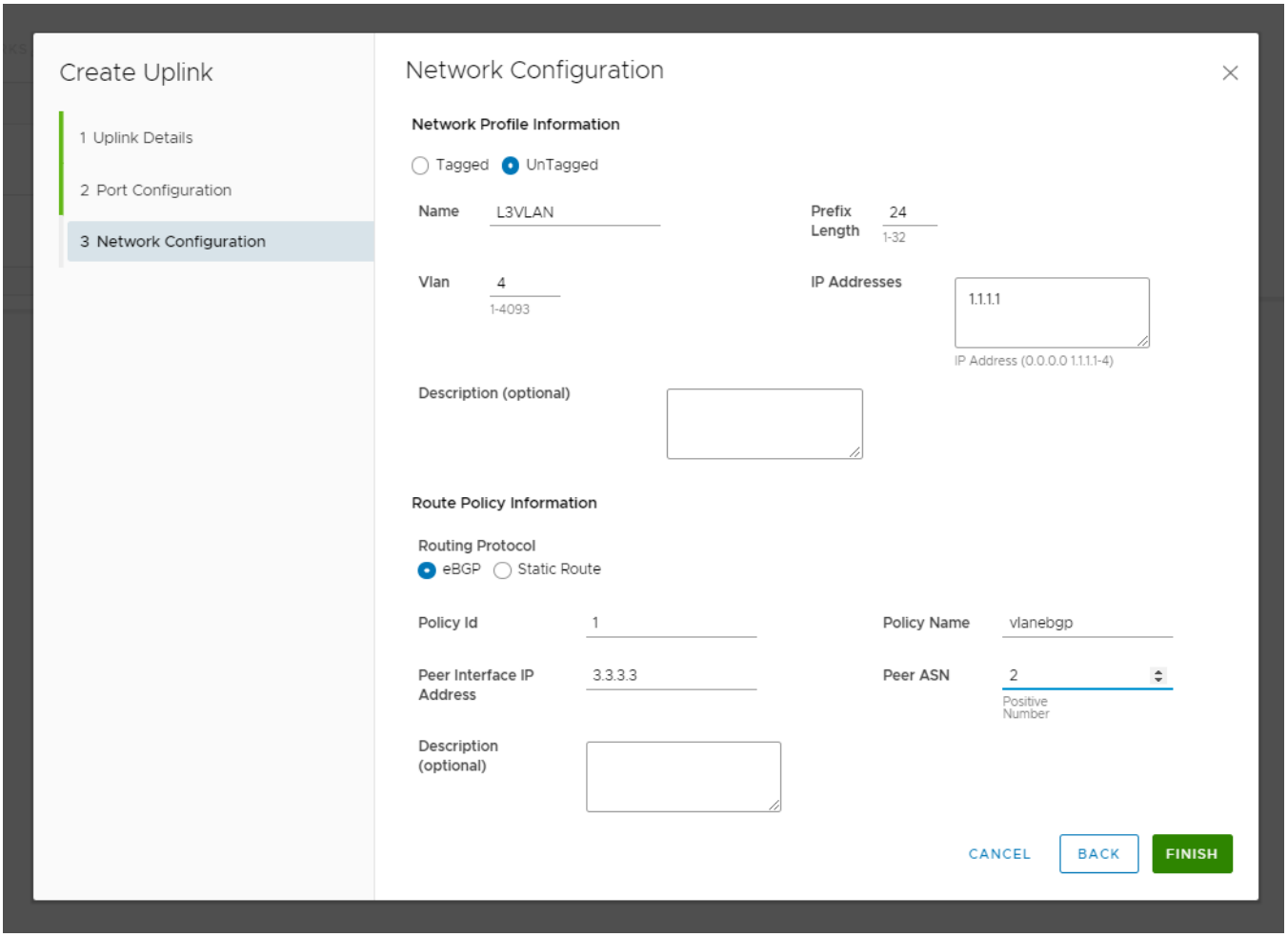
   Leaf:



   Spine:



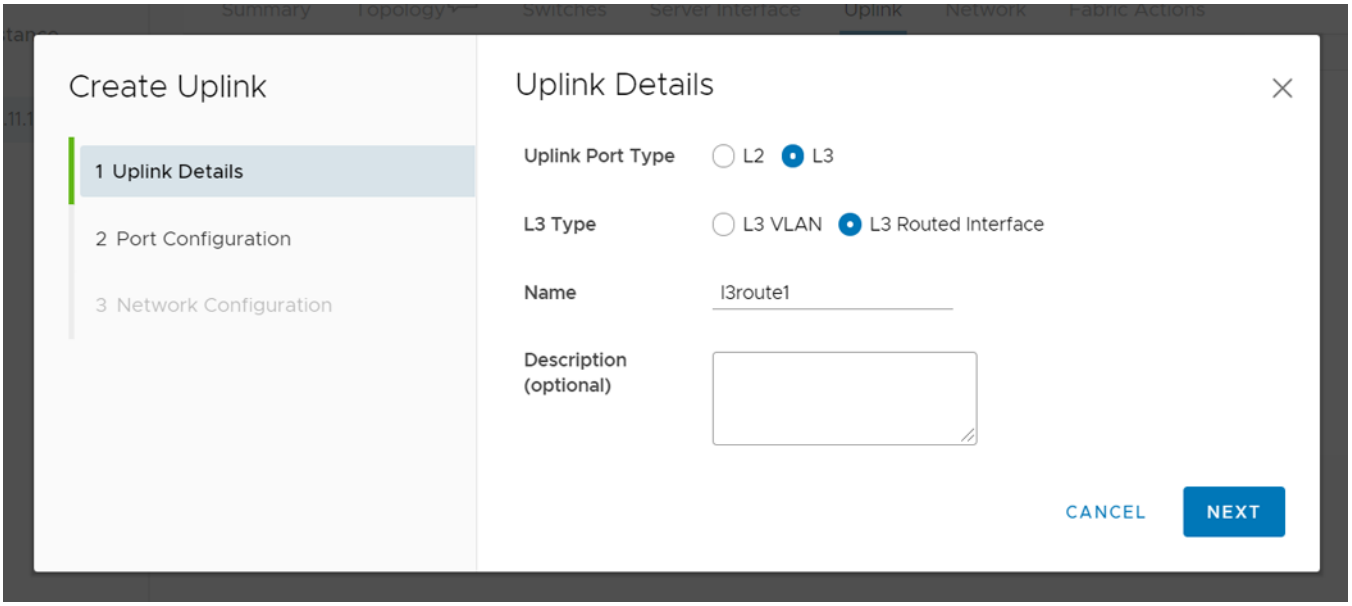
4. Select **UnTagged** network, select the **OMNI network**, enter an optional description, select either **eBGP** or **Static Route** for the routing protocol, enter the routing policy information, then click **Finish**.



5. A route is associated with the nodes that are configured in the port configuration. The system displays uplink creation success message.

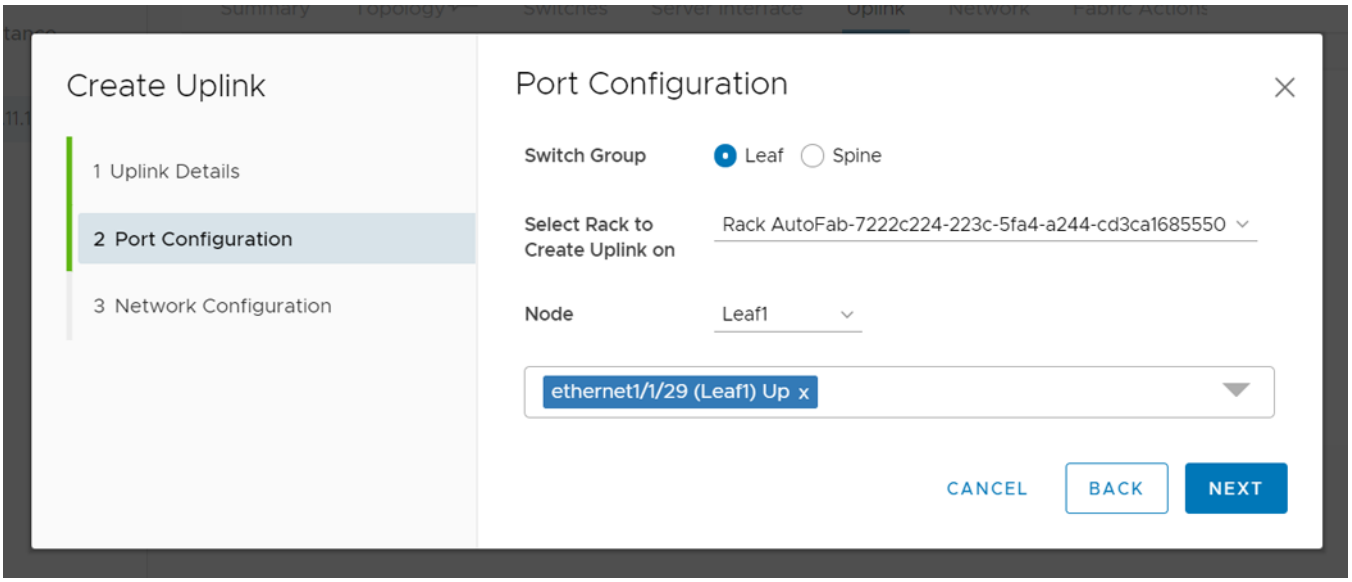
Create L3 routed interface uplink

1. Select the **Service Instance** > **Uplink**, and click **Create**.
2. Select **L3 routed interface**, enter the **Uplink name**, and optional description, then click **Next**.

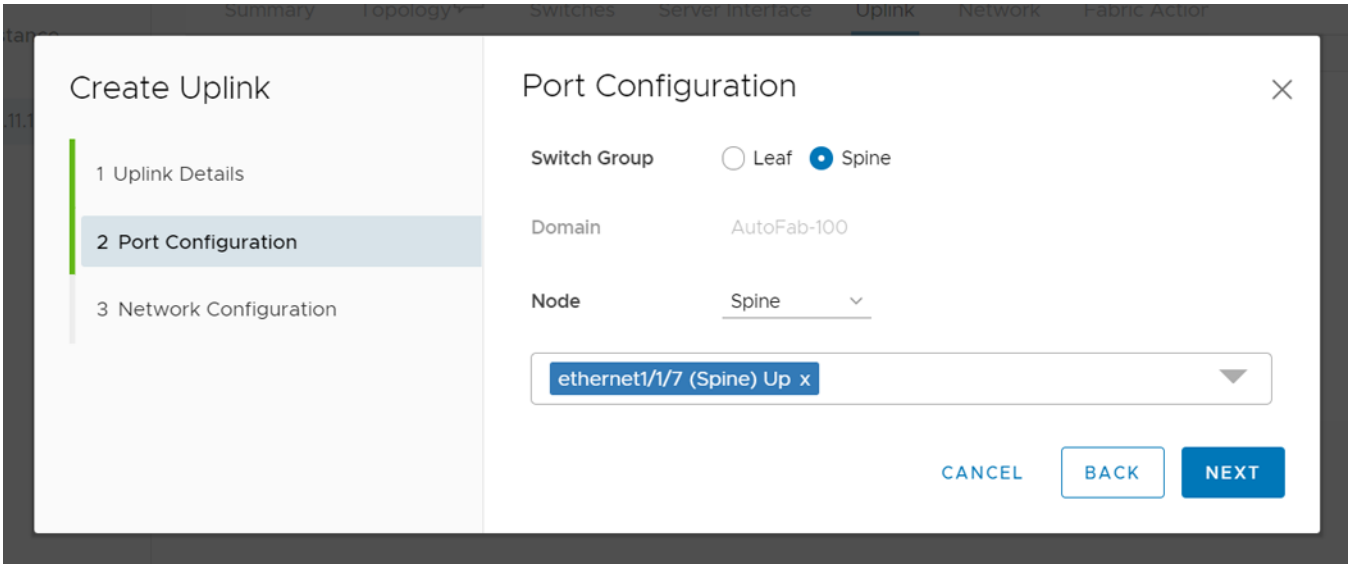


3. Select the Switch group (Leaf or Spine), the **rack** to create the uplink on, select the **interfaces**, then click **Next**.

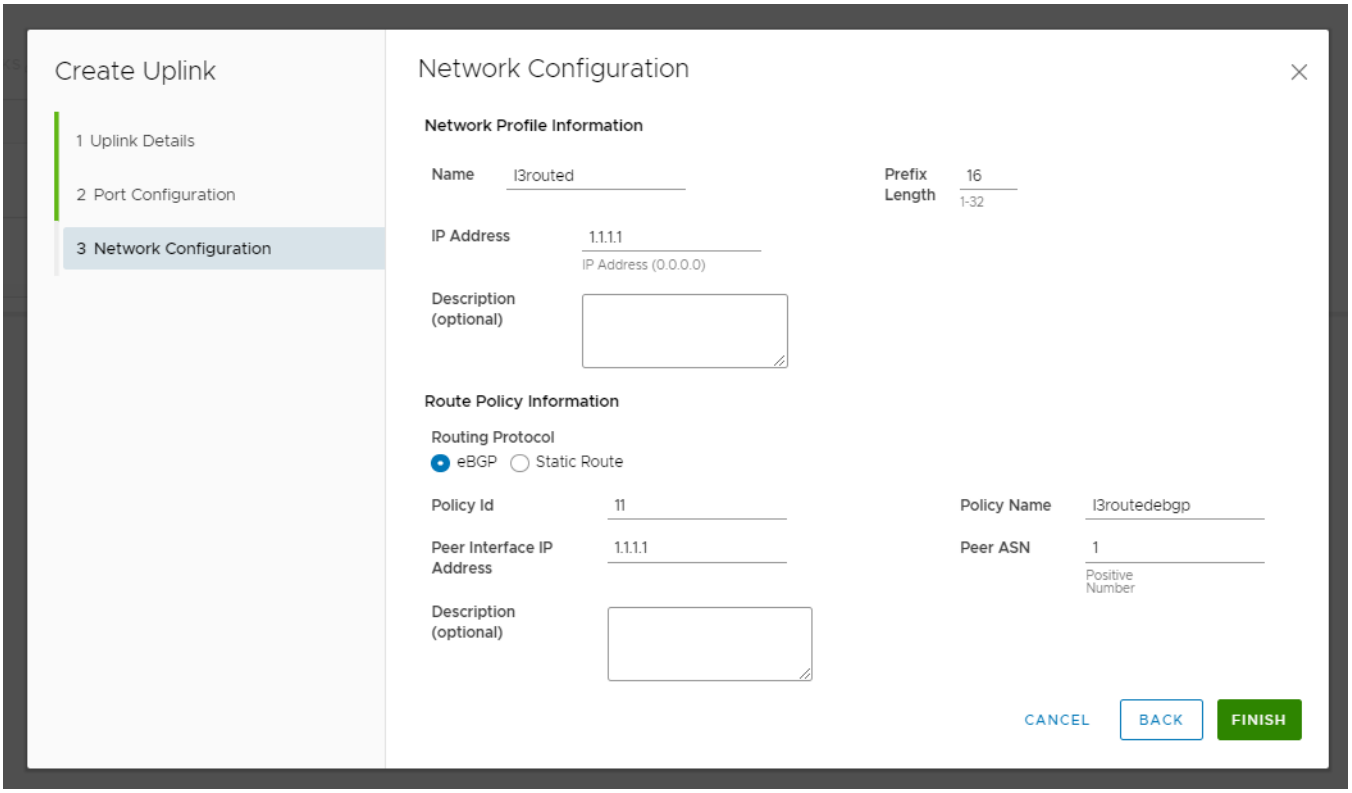
   Leaf:



   Spine:



4. Enter the network profile information and routing policy information for the uplinks, then click **Finish**.



5. The system displays L3 routed uplink creation success message.

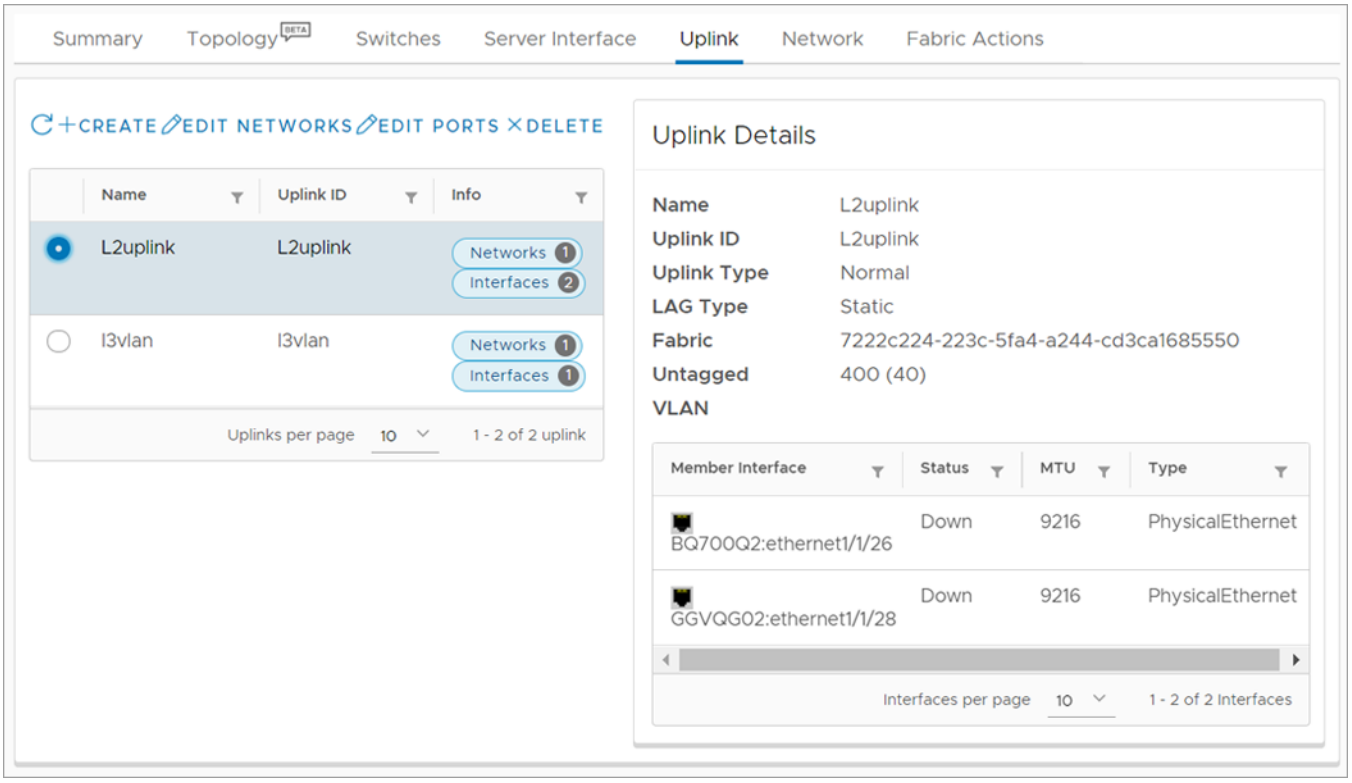
Edit networks and ports in an uplink

You can edit the network and port configuration for an uplink, and also view the detailed information of the uplink.

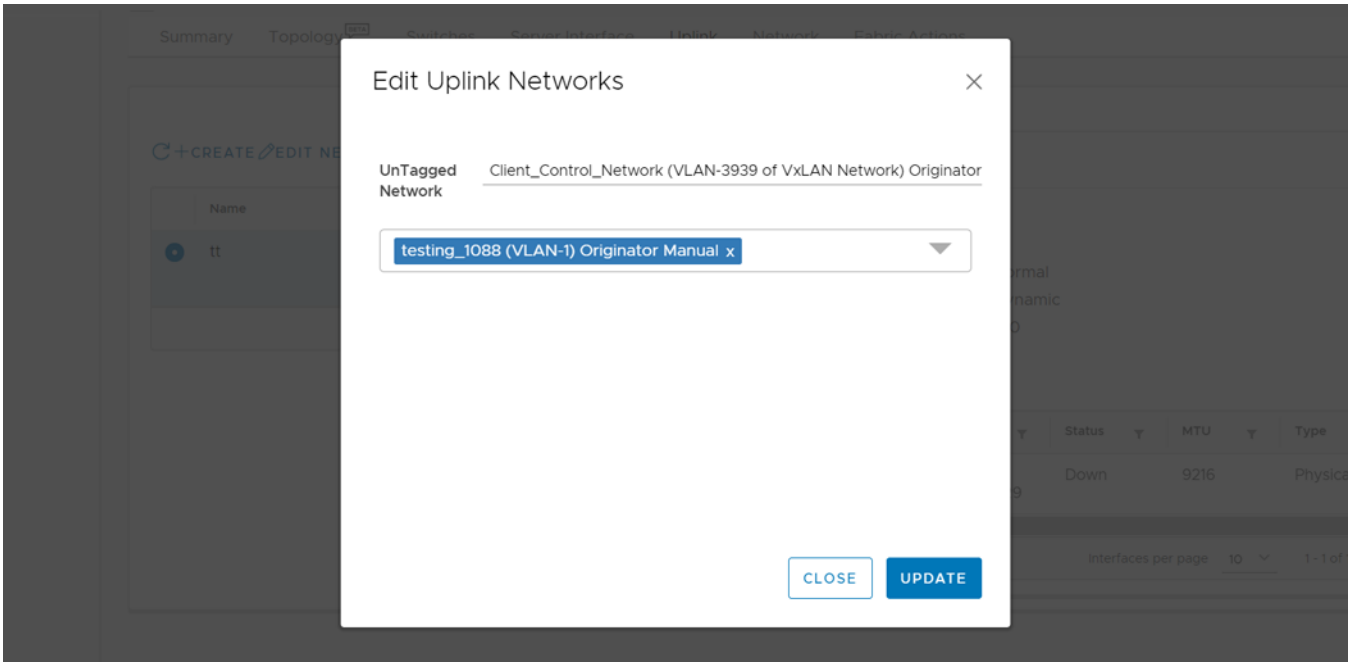
Select the uplink from the displayed list to view the details of the uplink on the right.

Edit networks

1. Select the uplink from the list, and click **Edit Networks**.



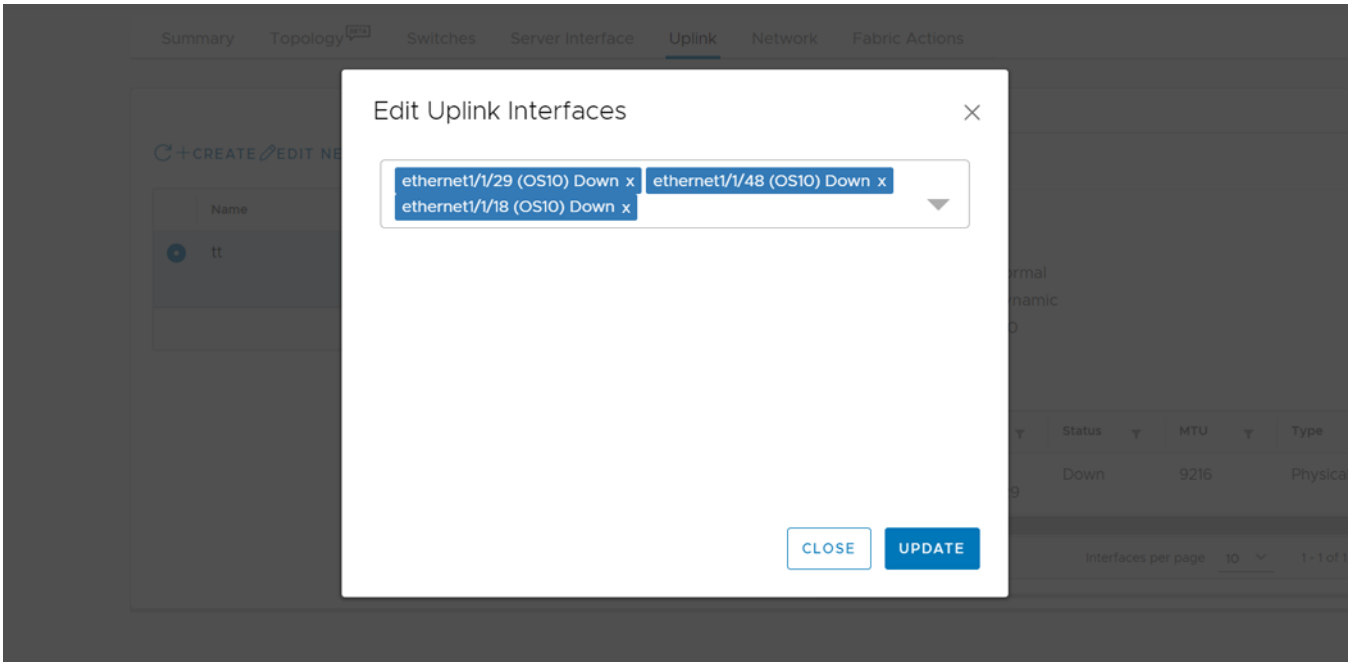
2. Edit the **Untagged Network** associated with the uplink, and click **Update**.



3. The system displays the uplink interface edit success message.

Edit ports

1. Select the fabric uplink from the list, and click **Edit Ports**.

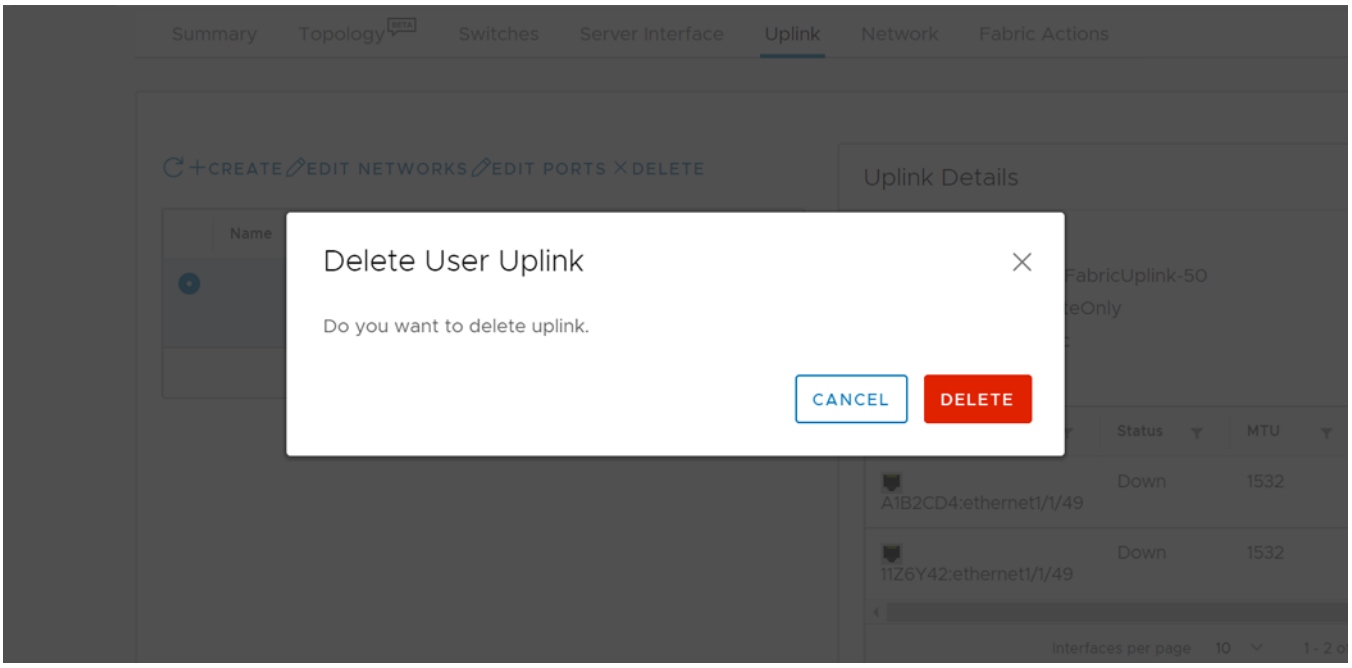


2. Edit the networks associated with uplink interfaces, and click **Update**.
3. The system displays the uplink interface edit success message.

Delete an uplink

You can delete a user-created uplink. To delete:

1. Select the uplink from the displayed list, and click **Delete**.



2. Click **Delete** to confirm.

Configure networks and routing configuration

You can set up networks and routing configuration.

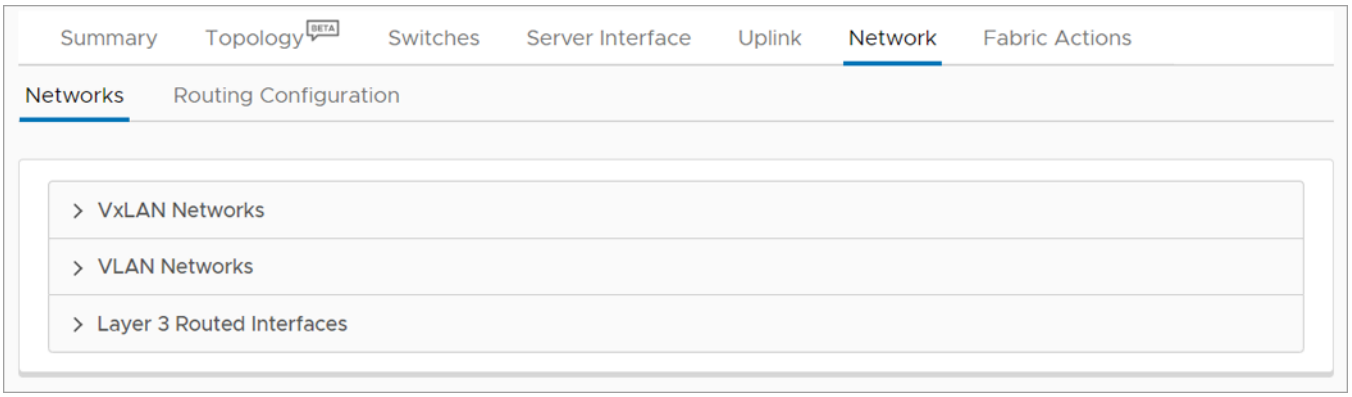
NOTE: Networks that are created by the OMNI user interface are considered *Manual*.

The OMNI vCenter `PortGroup` VLAN automation process does not add *Manual* networks to auto uplinks, and does not remove them from SmartFabric. Add *Manual* networks to uplinks using the OMNI portal if needed. The OMNI VLAN automation process uses *Manual* networks for `ServerInterfaces`. If you are using the VLANs for the OMNI registered vCenter `PortGroup`, it is not recommended to use the OMNI portal to create a network. OMNI automation manages those VLANs or networks by itself. For complete information, see OMNI vCenter integration.

You can configure three types of networks including VXLAN networks (for L2 and L3 profiles), VLAN networks (for L2 and L3 profiles), and L3 routed interfaces (for L3 profiles only).

View Networks summary

Select the **Service Instance**, and click **Network**.



Configure networks

You can manage VXLAN and VLAN networks, and L3 routed interfaces.

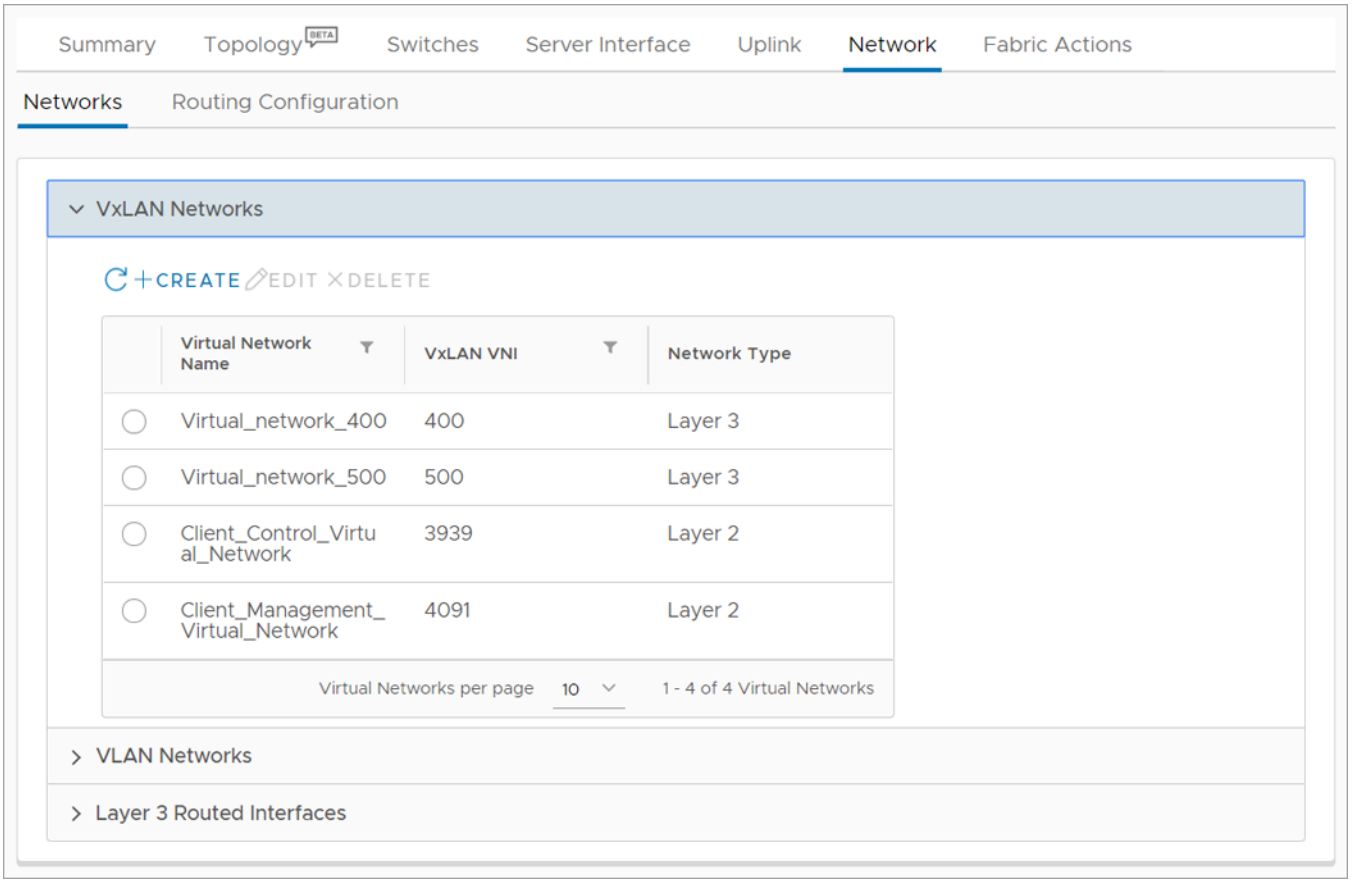
VXLAN network

From **Network** tab, you can create, edit, and delete VXLAN and VLAN networks, and L3 routed interfaces.

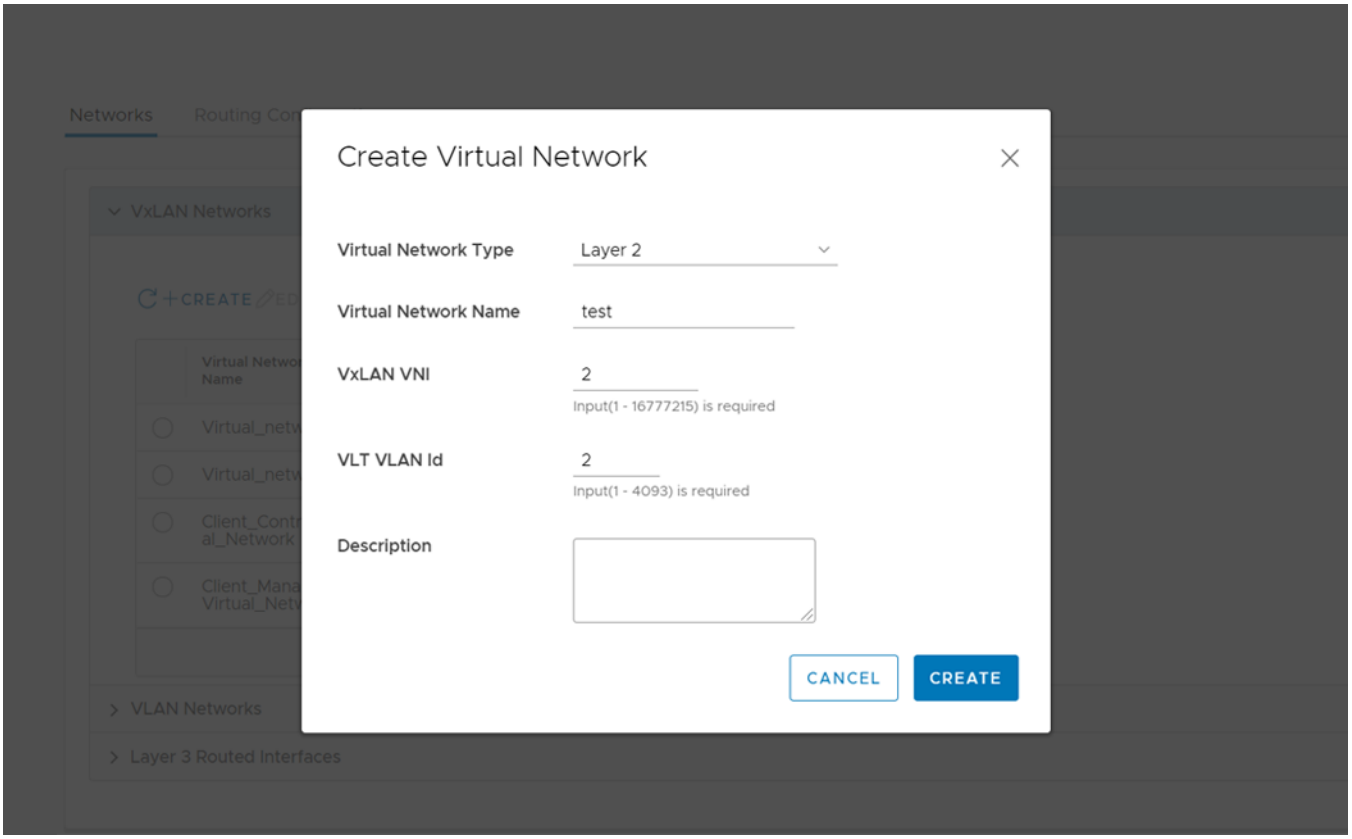
Create VXLAN network

Virtual network for L2 profile:

1. Select Network from the Network tab, then click **Networks** > **VxLAN Networks**. The page displays the list of the VXLAN networks that are configured in the service instance.



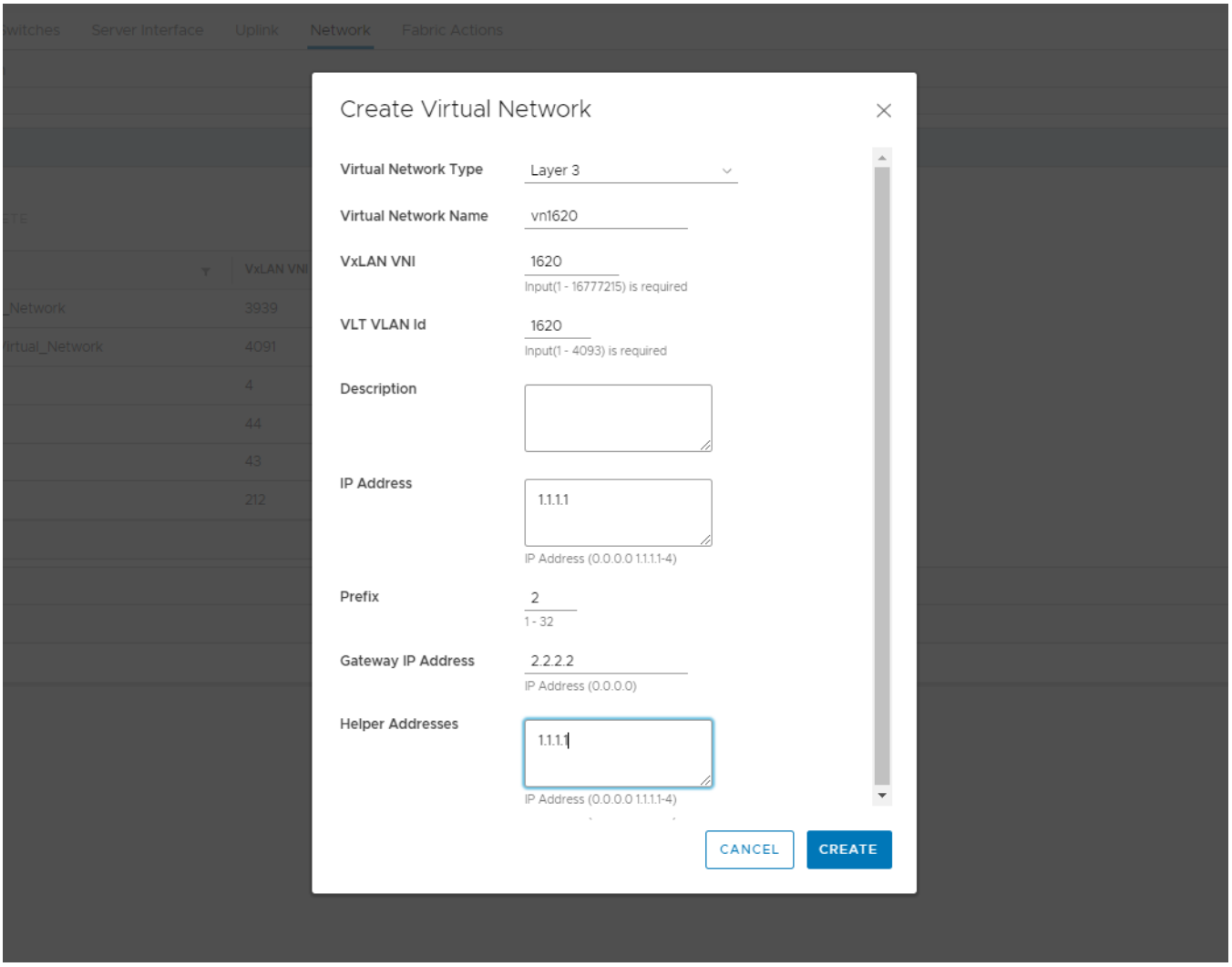
2. Click **Create**.
3. Verify **Layer 2** is selected as the **Virtual Network Type**.
4. Enter the text for **Virtual Network Name**, a value for the VxLAN VNI, and the VLT VLAN ID.
5. (Optional) Enter a description, and click **Create**.



6. The system displays virtual network creation successful message.

Virtual network for L3 profile:

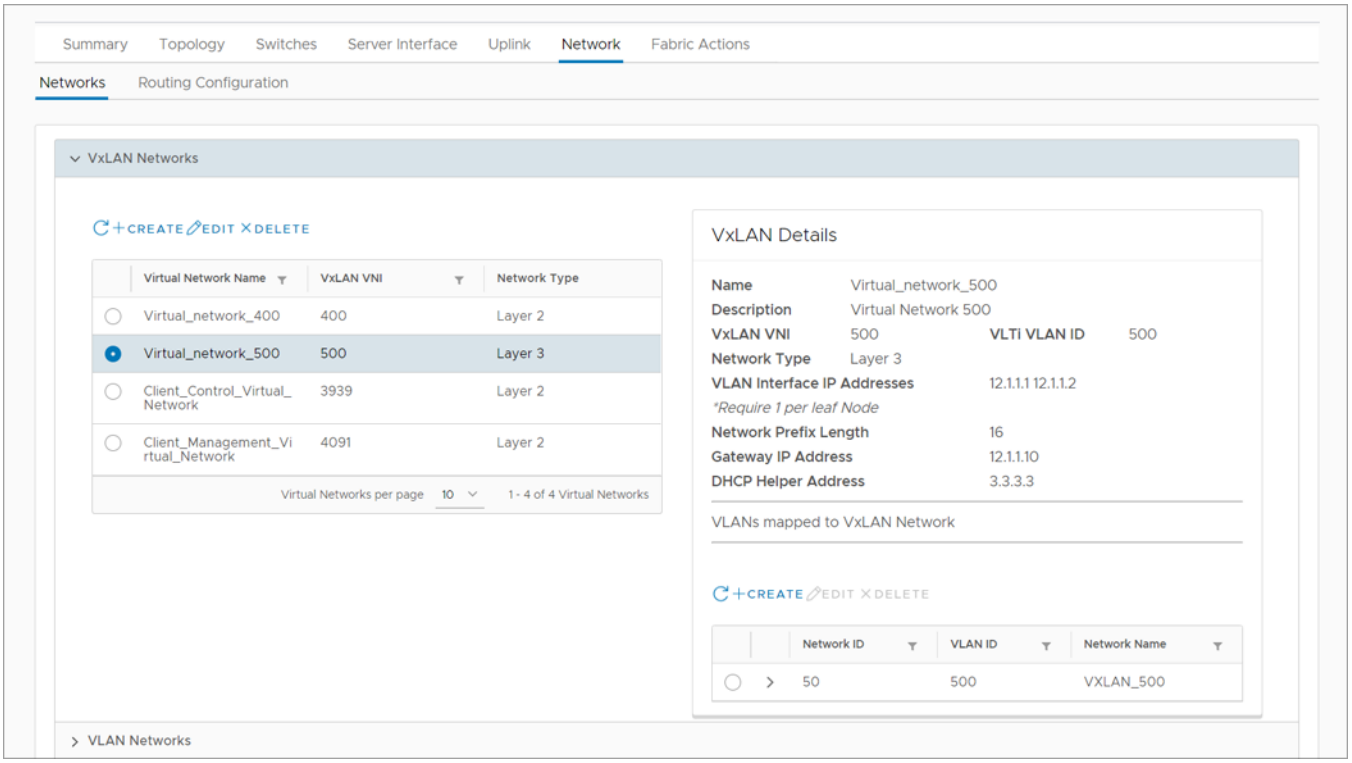
1. Select Network from the Network tab, then click **Networks** > **VxLAN Networks**. The page displays the list of the VXLAN networks that are configured in the service instance.
2. Click **Create**.
3. Select **Layer 3** as the **Virtual Network Type**.
4. Enter the text for **Virtual Network Name**, a value for the VxLAN VNI, the VLT VLAN ID, prefix, gateway IP address, and helper IP address. Click **Create**.



5. The system displays virtual network creation successful message.

View VxLAN network details

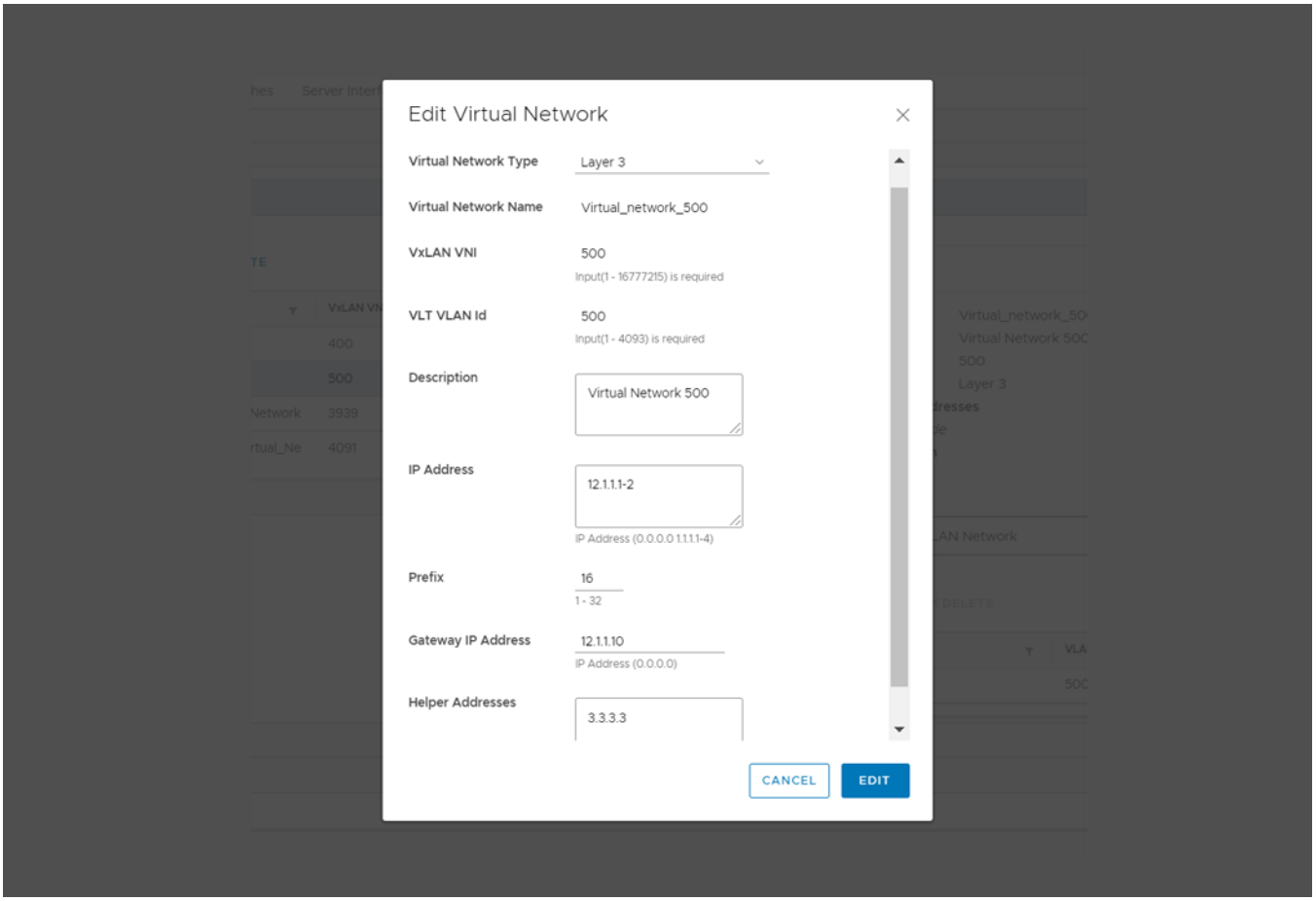
The VxLAN networks display a list of mapped VLANs. Select a VxLAN network to view details pertaining to that specific network including network ID, VLAN ID, and network name.



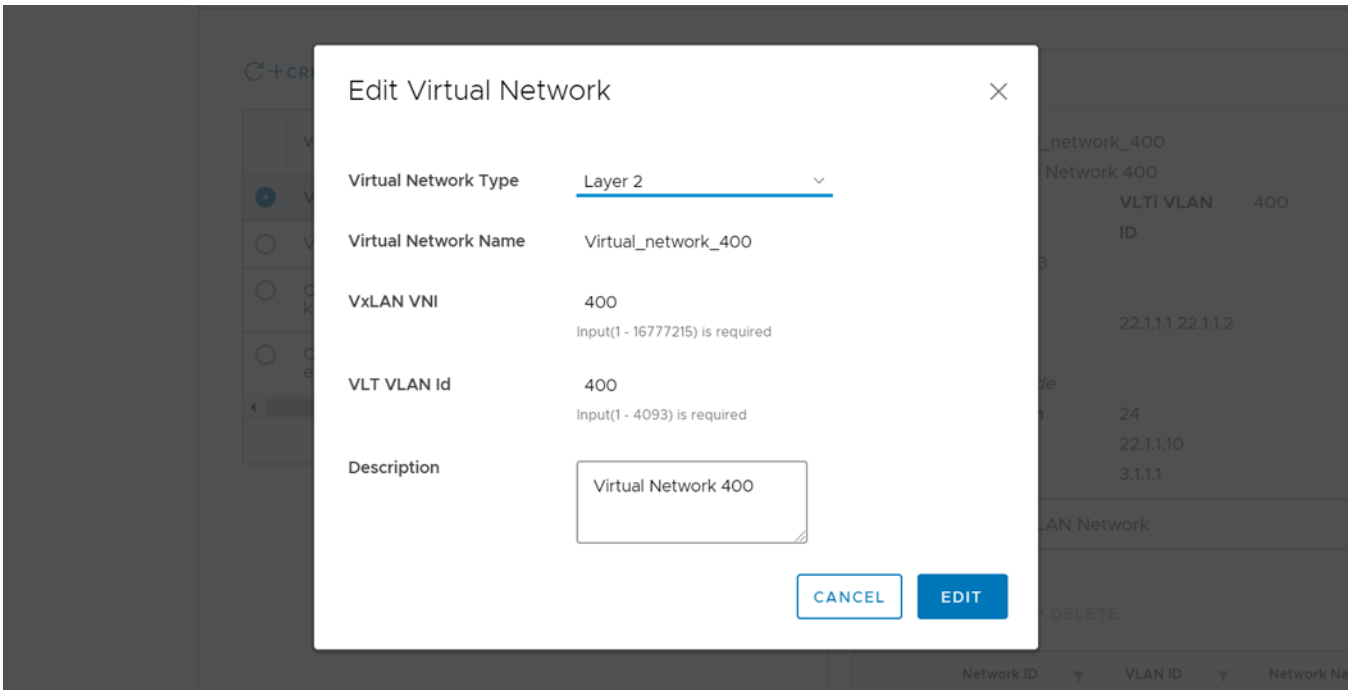
Edit VxLAN network

You can edit the configuration of VXLAN network:

1. Select a virtual network from the list, then click **Edit**.



2. Modify the Virtual Network Type.
3. Enter the Prefix, Gateway IP Address, IP address, then click **Edit**.

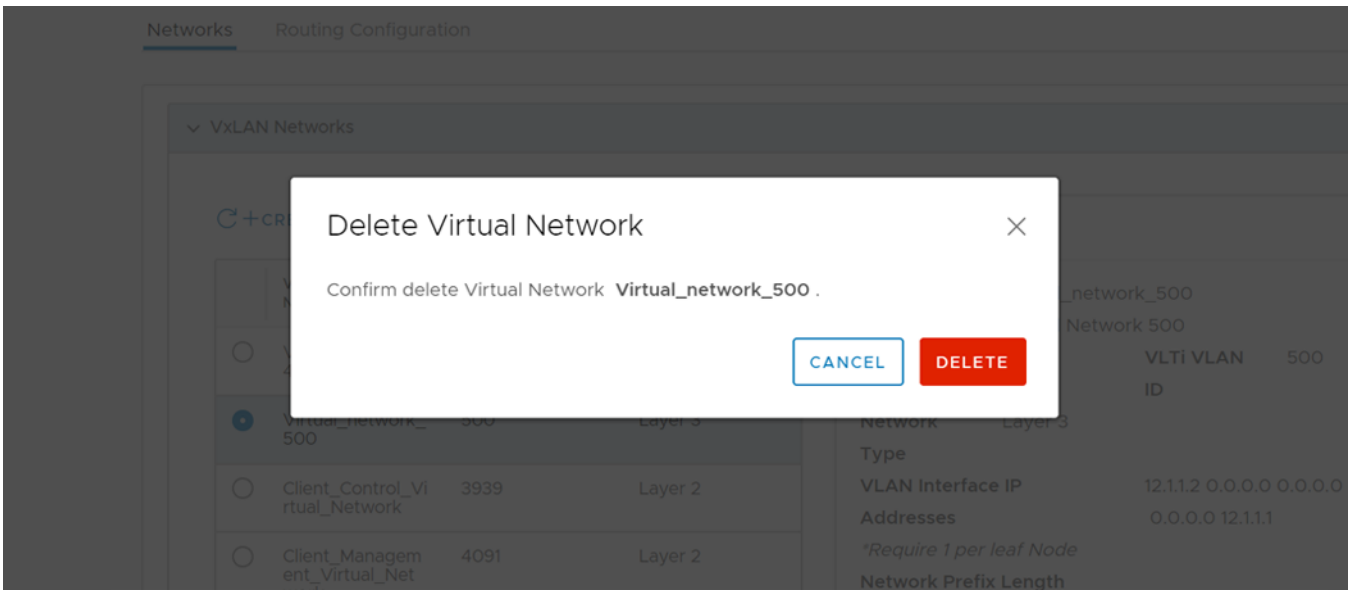


4. The system displays virtual network edits success message.

Delete VXLAN network

To delete a VXLAN network, first delete the mapped VLAN or VLANs if associated, and delete the virtual network.

1. Select the Virtual Network Name, select the Network to remove, then click **Delete**.



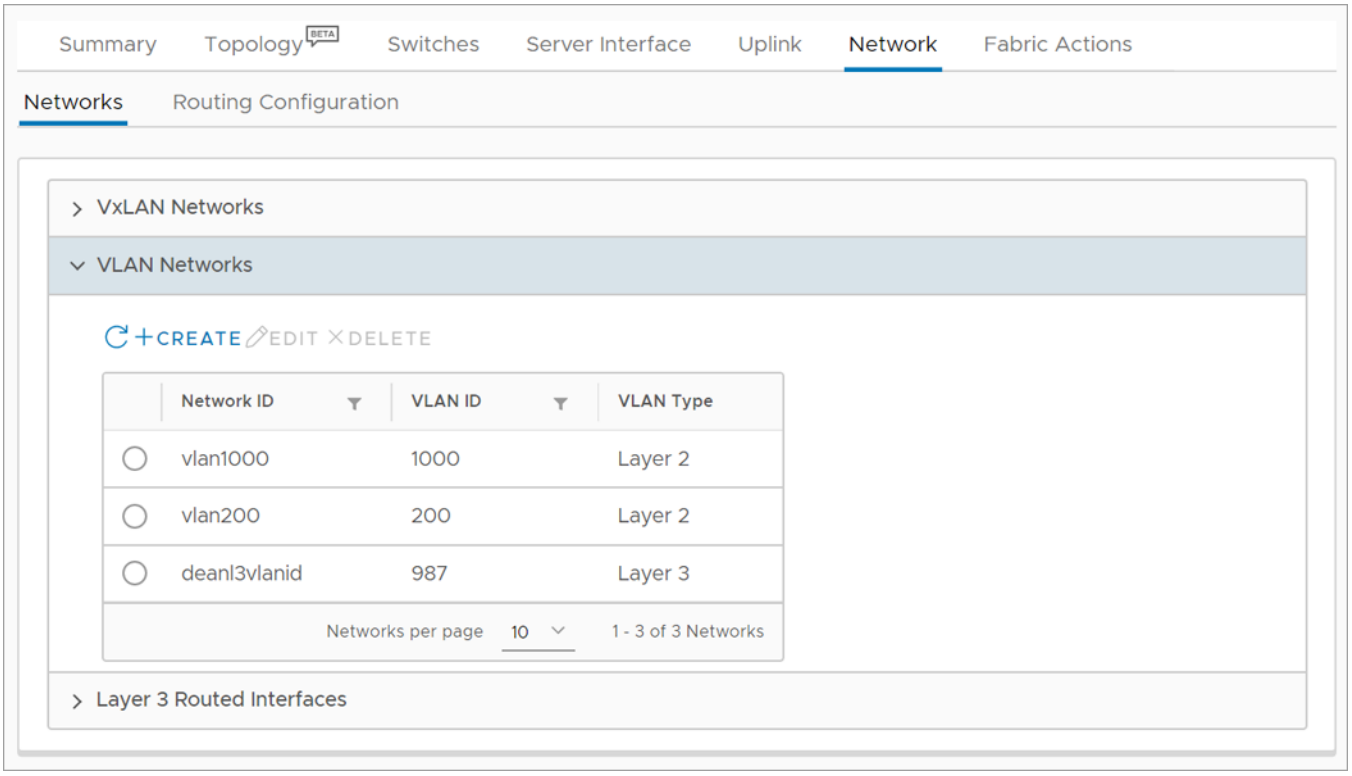
2. Click **Delete** to confirm.
3. The system displays network deletion success message.

VLAN networks

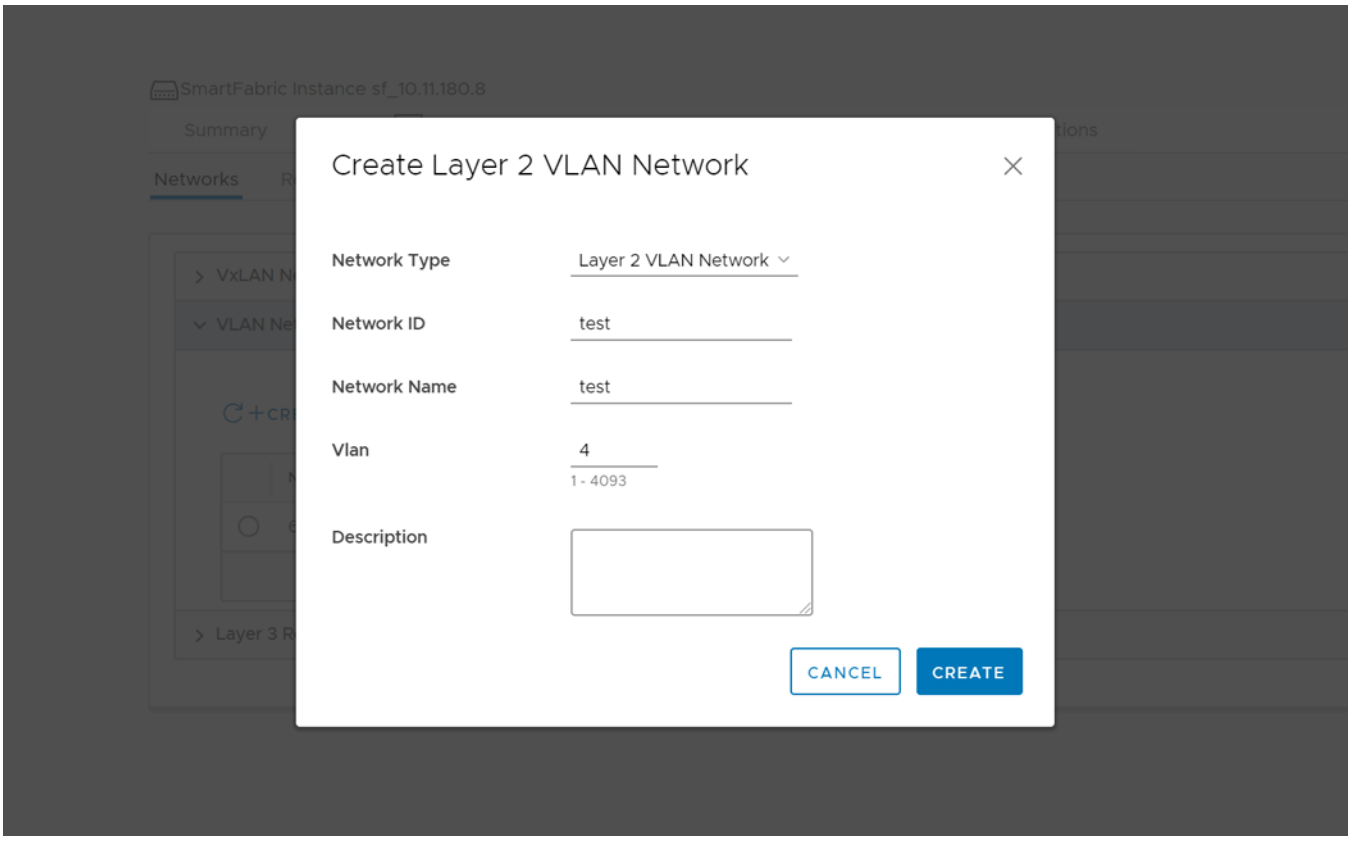
Create L2 VLAN or L3 VLAN network

VLAN networks for L2 profile:

1. Select **Networks** > **VLAN Networks**, and click **Create**.



2. Select the Network Type as **Layer 2 VLAN Network** is selected as the Network Type, enter the **Network ID**, **Network Name**, enter 1 to 4093 for the VLAN, enter an optional description, then click **Create**.

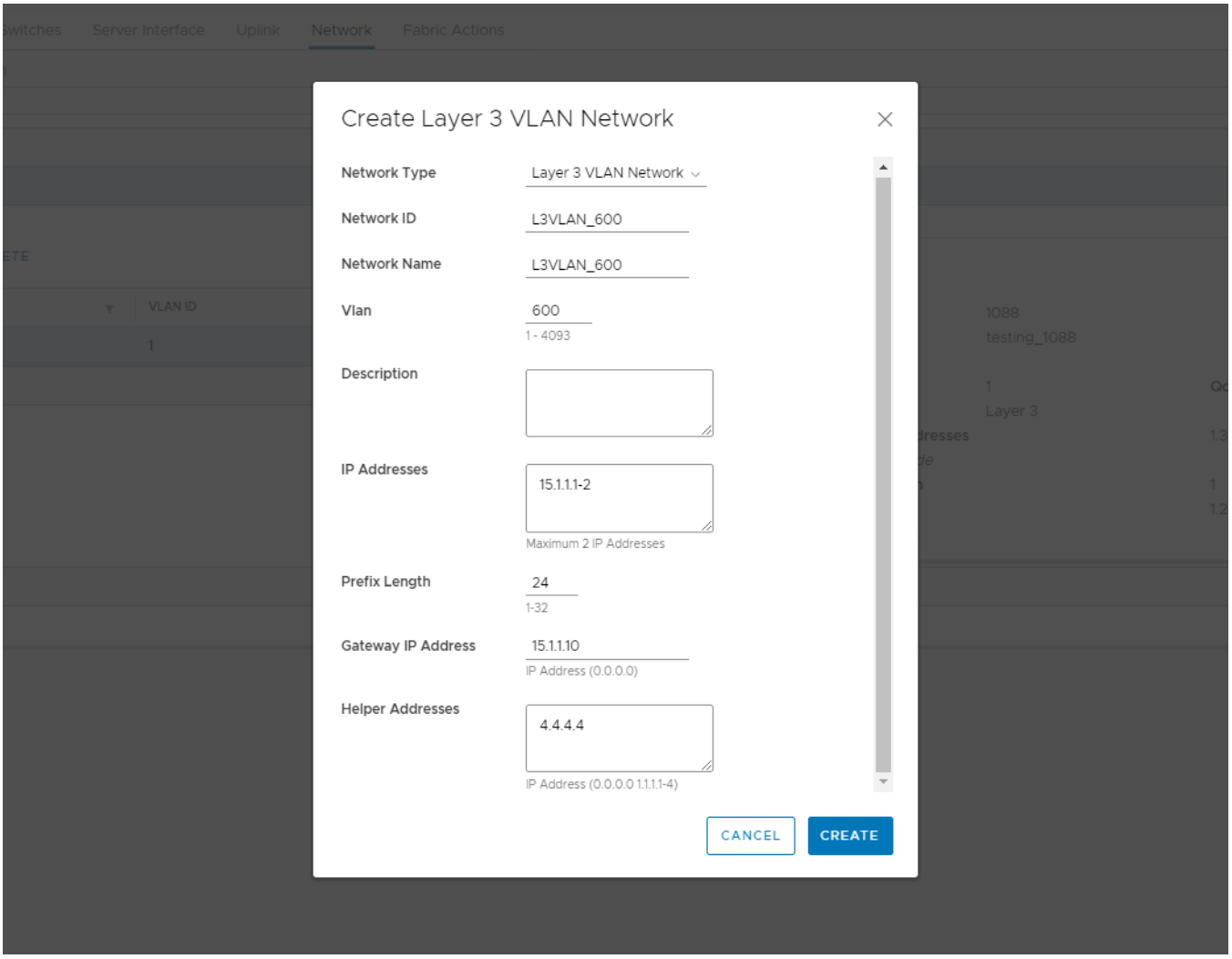


3. The system displays VLAN network creation success message.

VLAN networks for L3 profile:

1. Select **Networks** > **VLAN Networks**, and click **Create**.

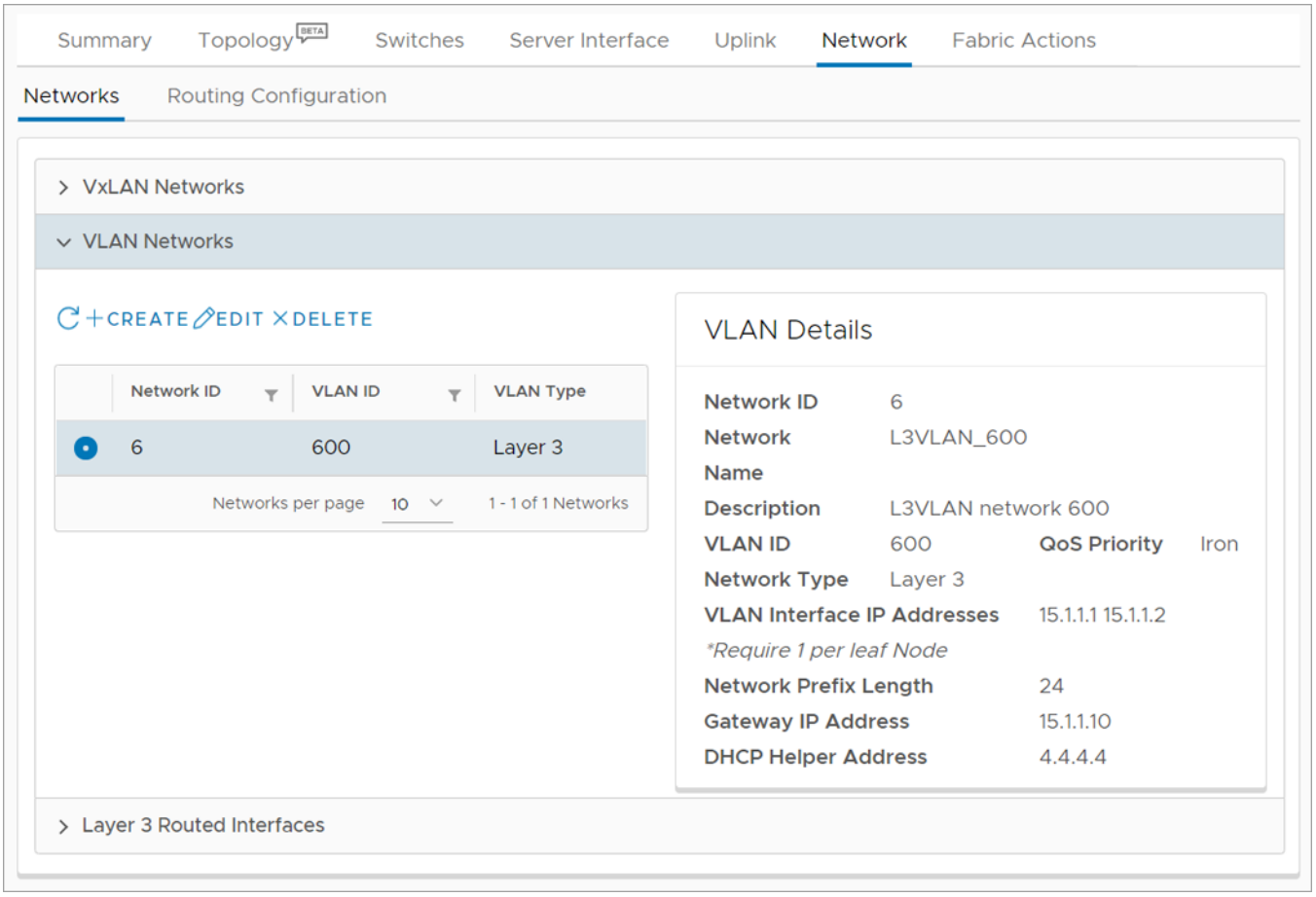
2. Select the Network Type as **Layer 3 VLAN Network** is selected as the Network Type, enter the **Network ID**, **Network Name**, enter 1 to 4093 for the VLAN, enter an optional description, then click **Create**.



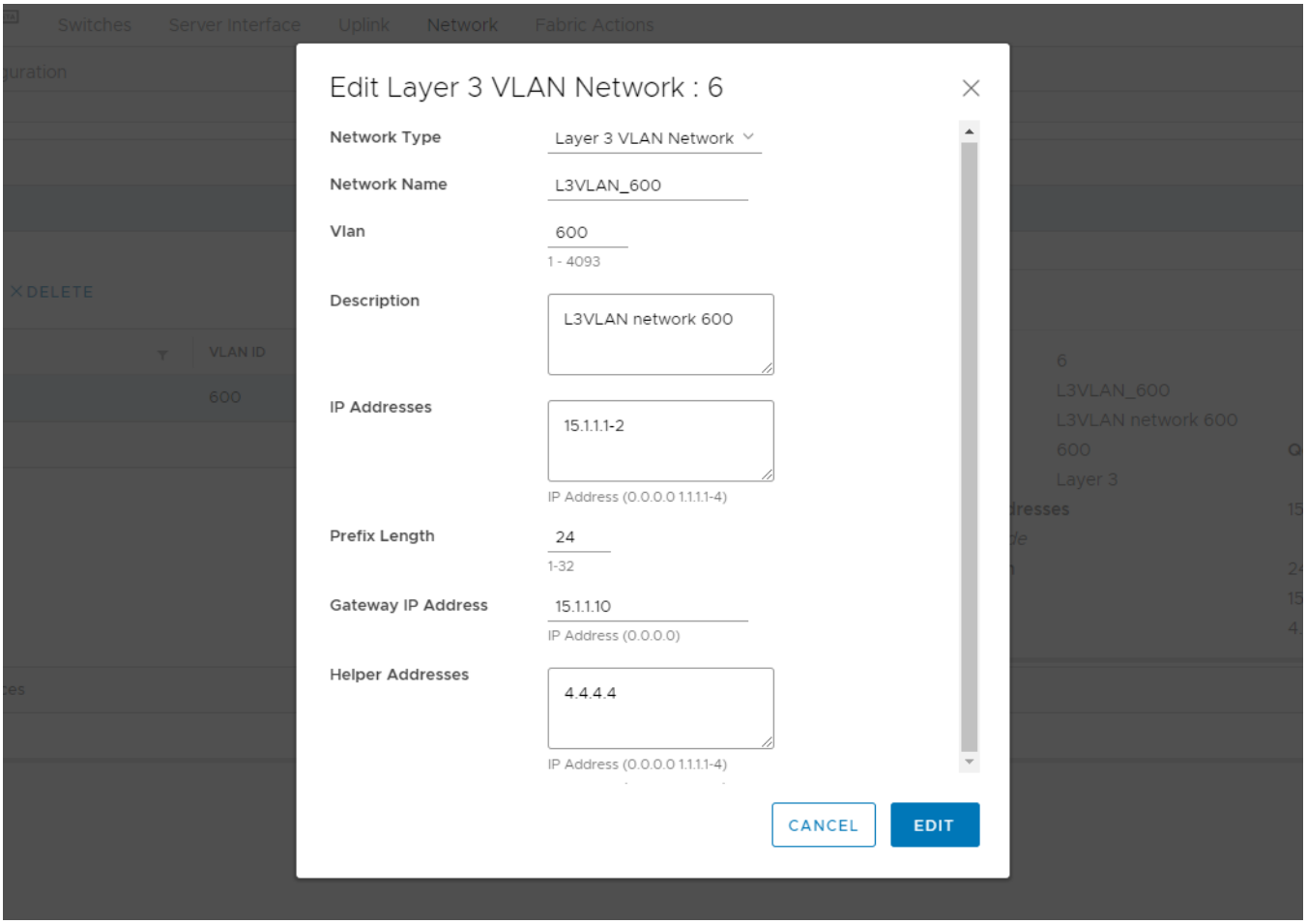
3. The system displays VLAN network creation success message.

Edit network

1. Select a network ID from the list, and click **Edit**.



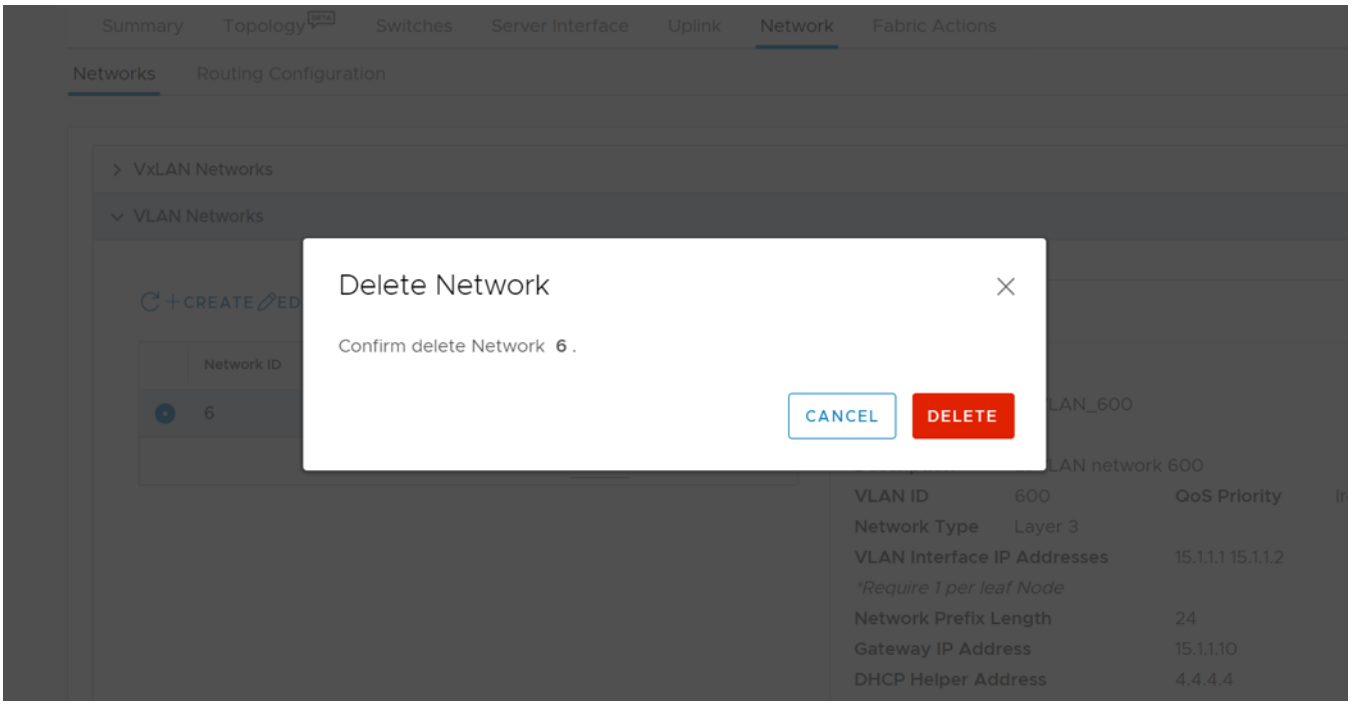
2. Modify the details, edit the configuration as necessary, and click **Edit**.



3. The system displays edit network success message.

Delete network

1. Select the VLAN network to remove, then click **Delete**.



2. Click **Delete** to confirm.

3. The system displays network deletion success message.

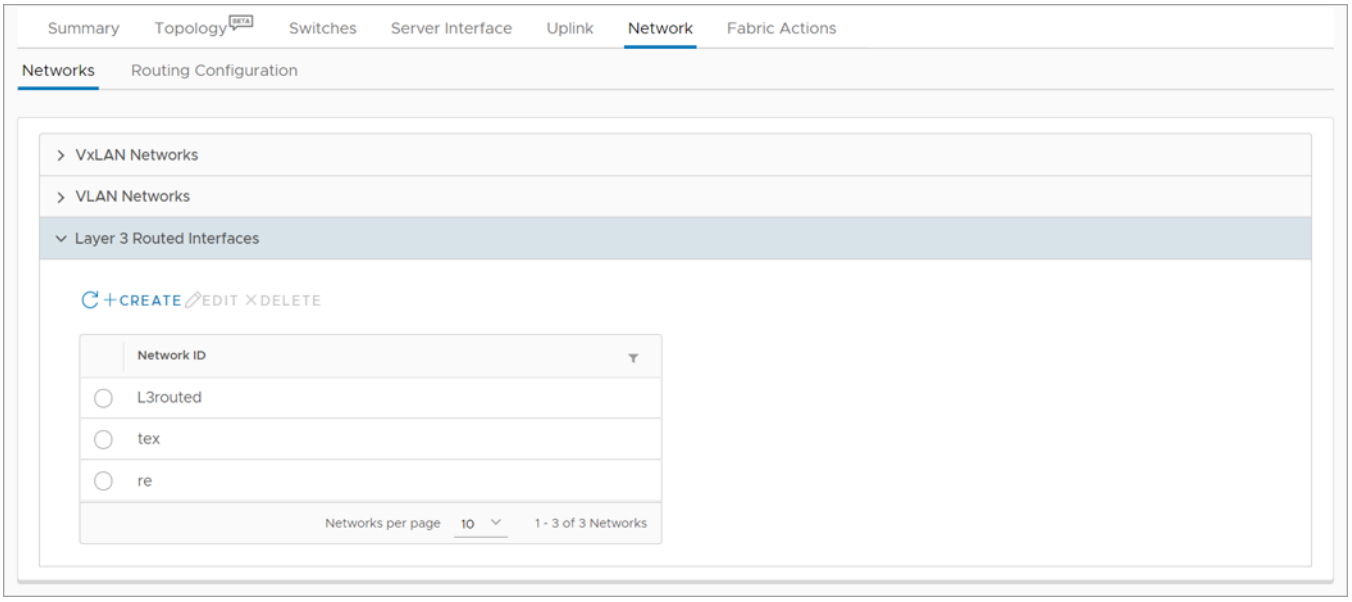
L3 routed interfaces

This information explains how to create and delete Layer 3 routed interfaces.

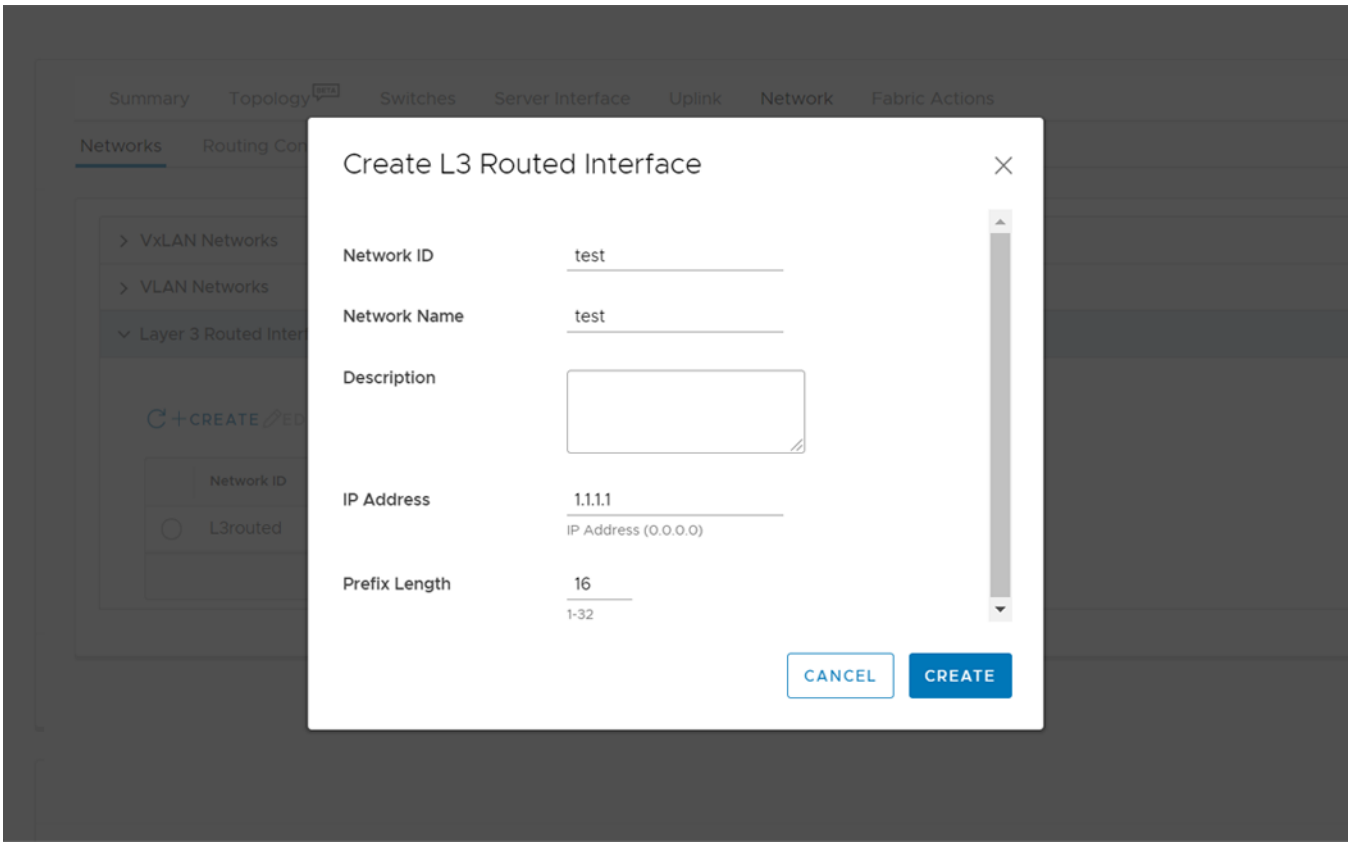
Create L3 routed interface

To create an L3 routed interface:

1. Select **Networks** > **Layer 3 Routed Interfaces**, and click **Create**.



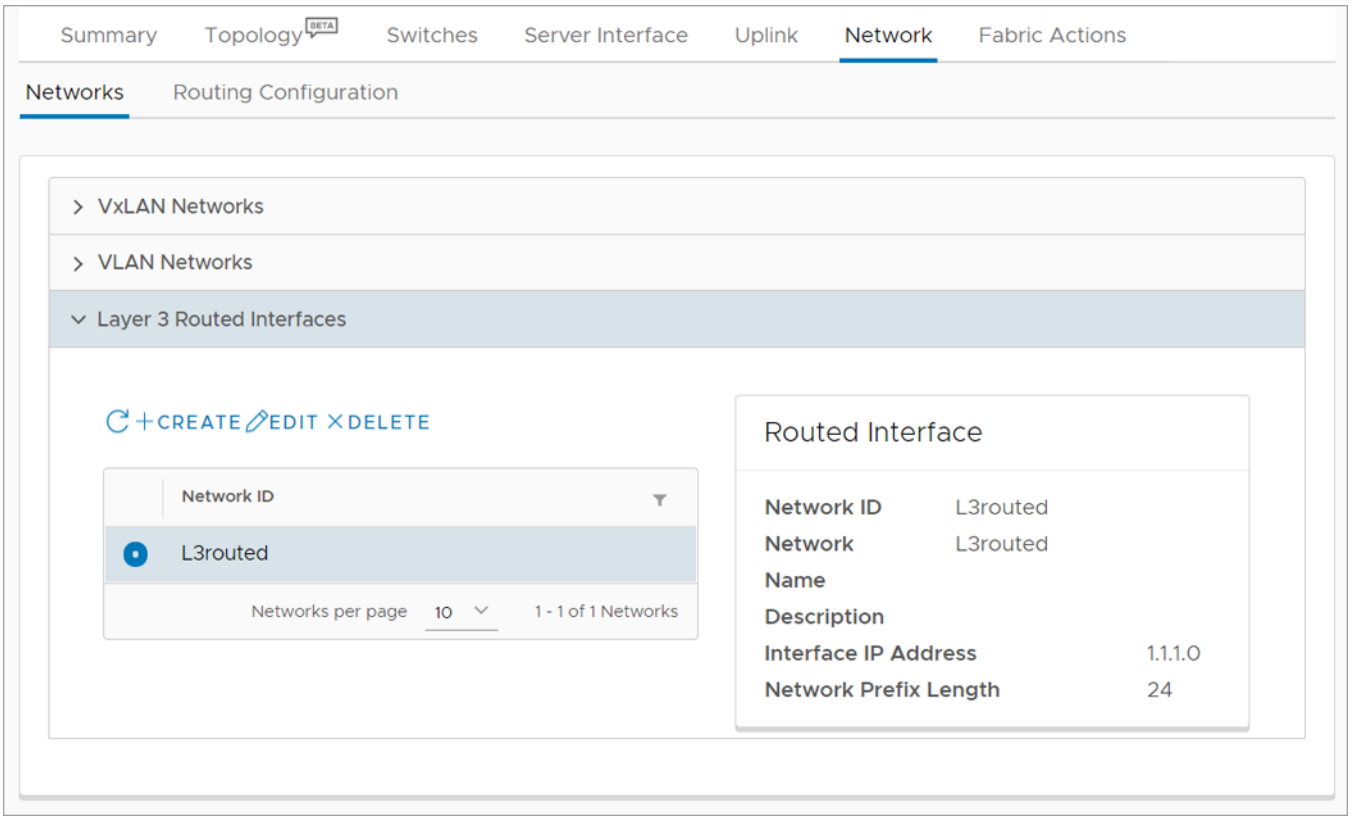
2. Enter the **Network ID**, **Network Name**, select the **Prefix Length**, select the **IP Address**, enter an optional description, then click **Create**.



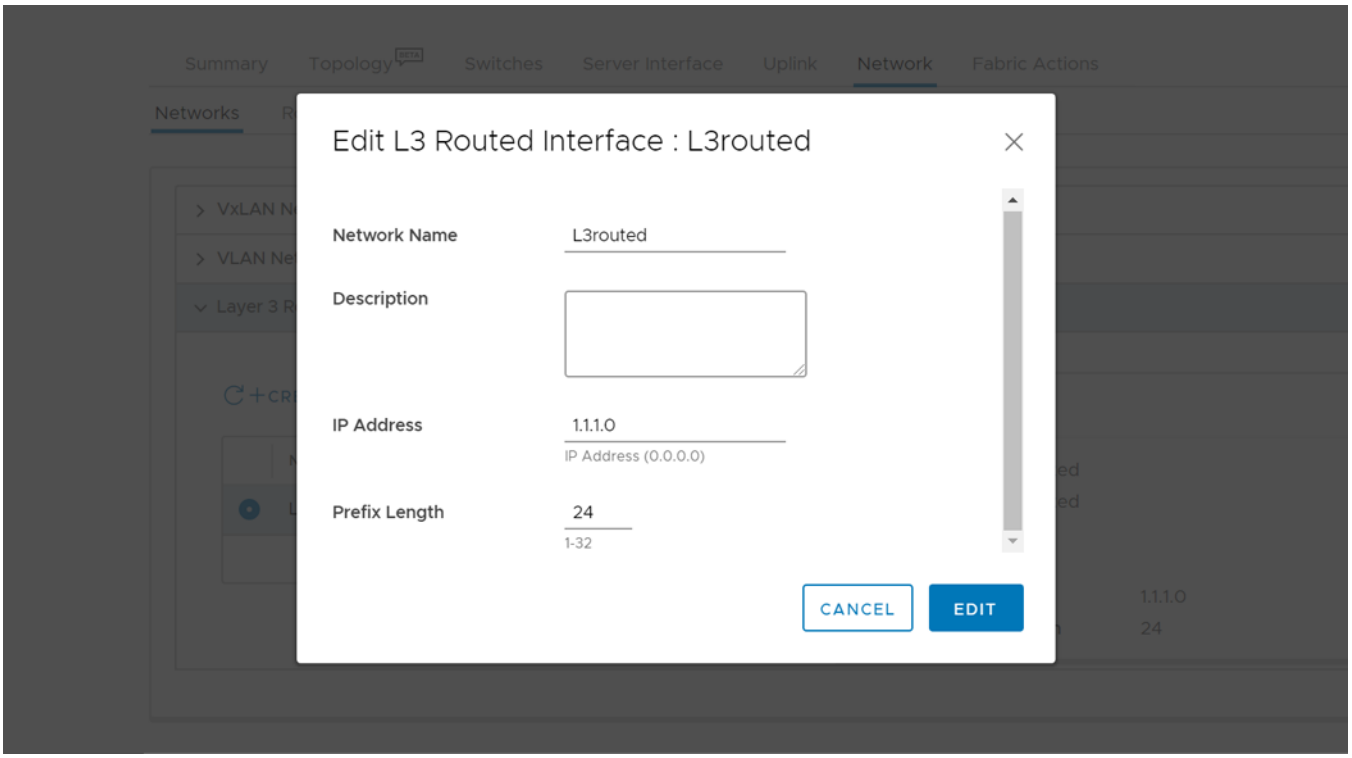
3. The system displays network creation success message.

Edit network

1. Select the **Network ID** from the list, and click **Edit**.



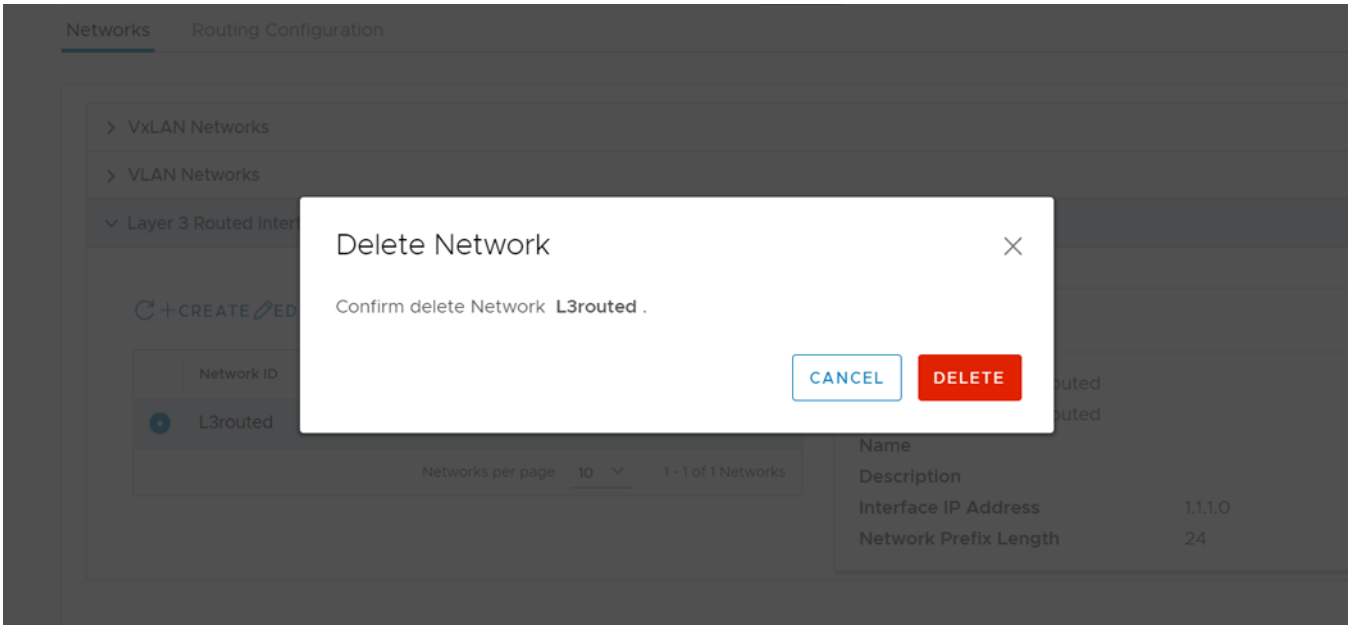
2. Edit the configuration, and click **Edit**.



3. The system displays edit network success message.

Delete network

1. Select the network ID to remove, and click **Delete**.



2. The system displays network deletion success message.

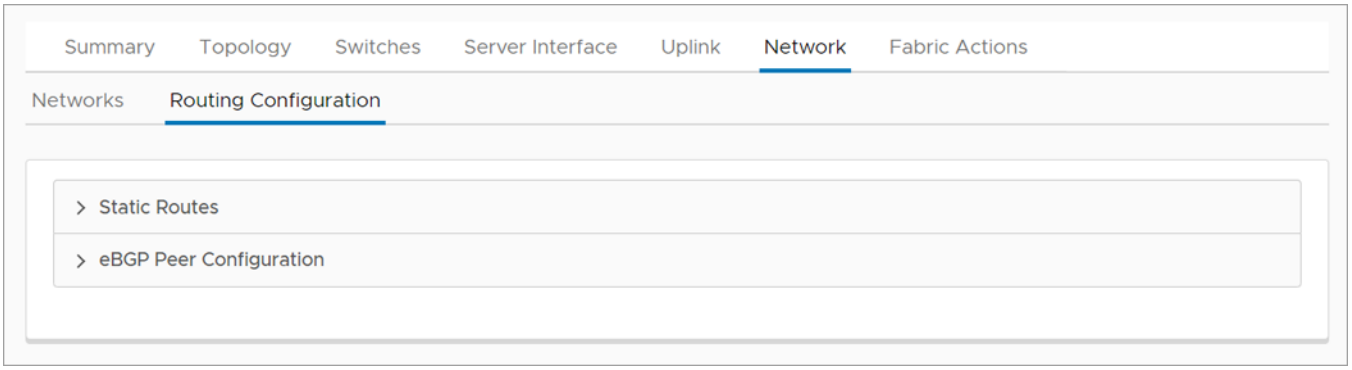
Configure Routes

You can configure static routes and eBGP peer routes for a network.

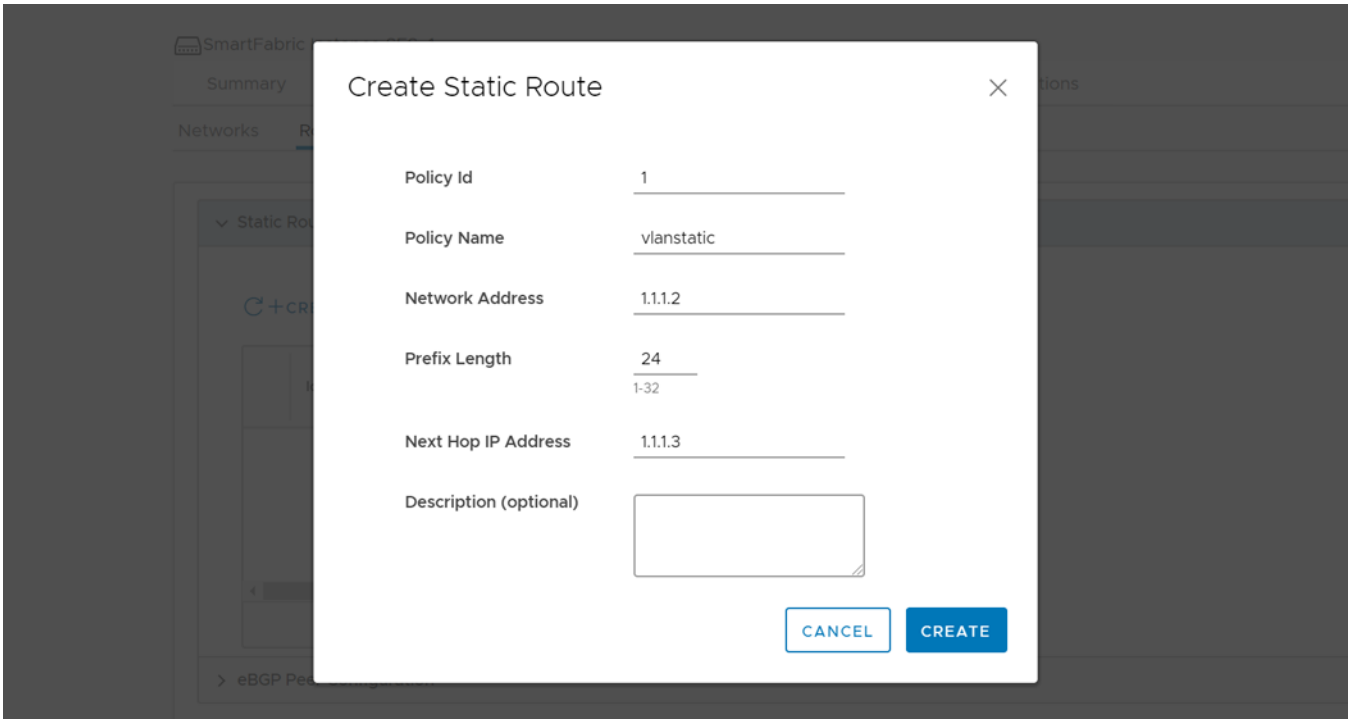
Configure static routes

Create static route

1. Select **Network** > **Routing Configuration**.



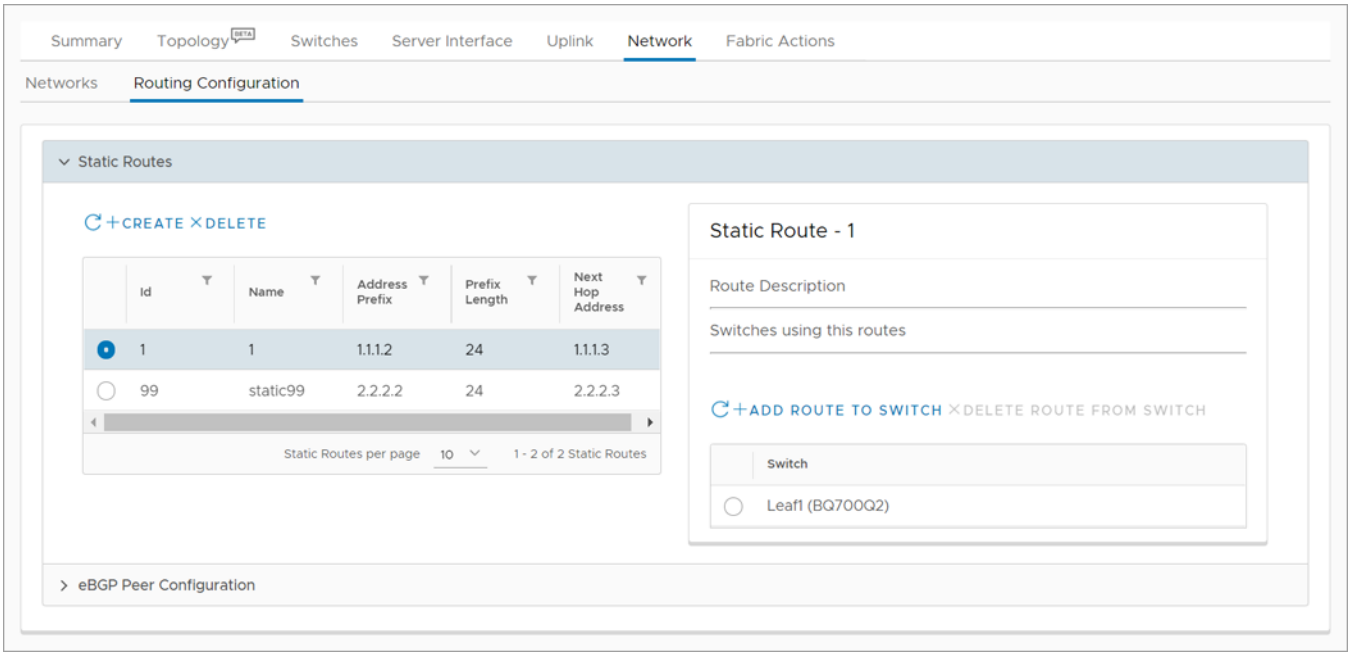
2. Select **Static Routes**, and click **Create** to add a new static route.
3. Enter the relevant details and click **Create**.



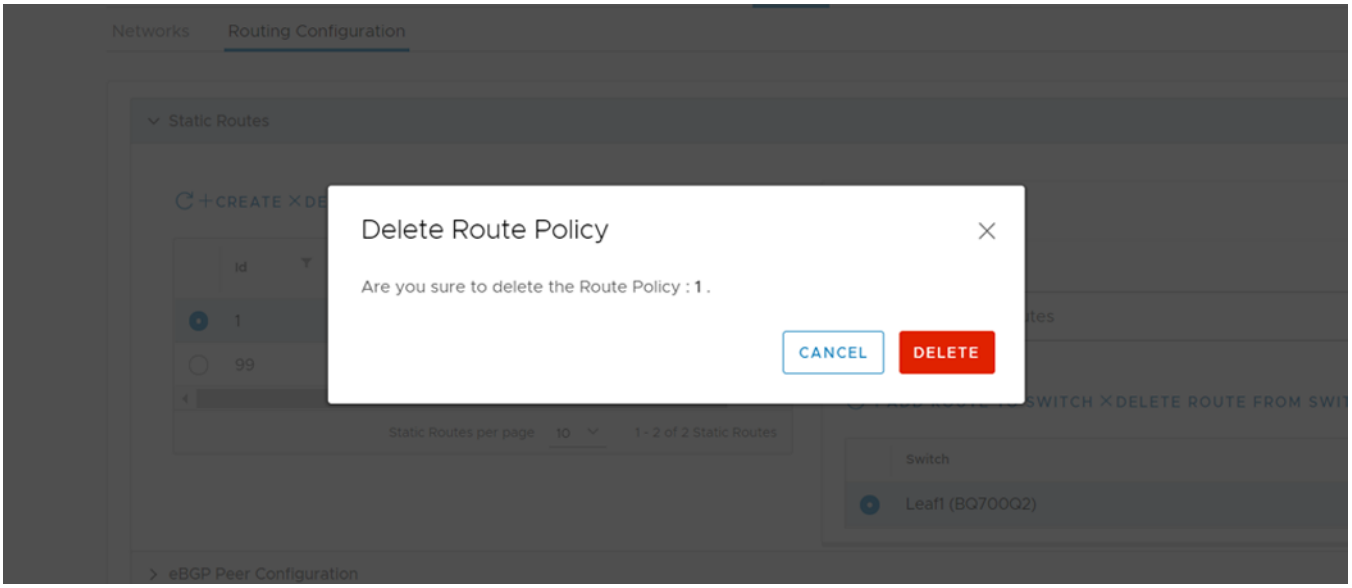
4. The system displays static route creation is successful.

Delete static route

1. Select the static route to delete, and click **Delete**.



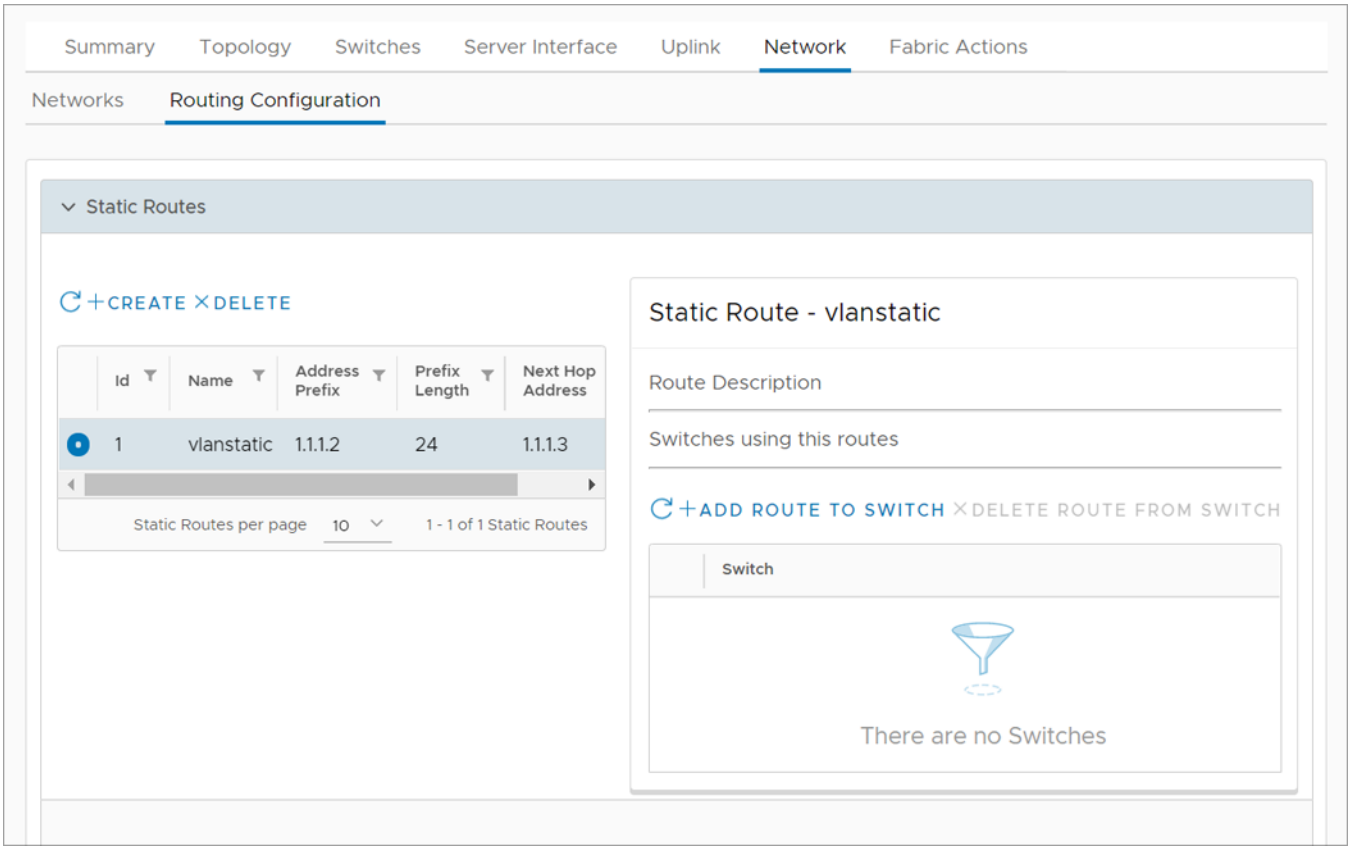
2. Click **Delete** to confirm.



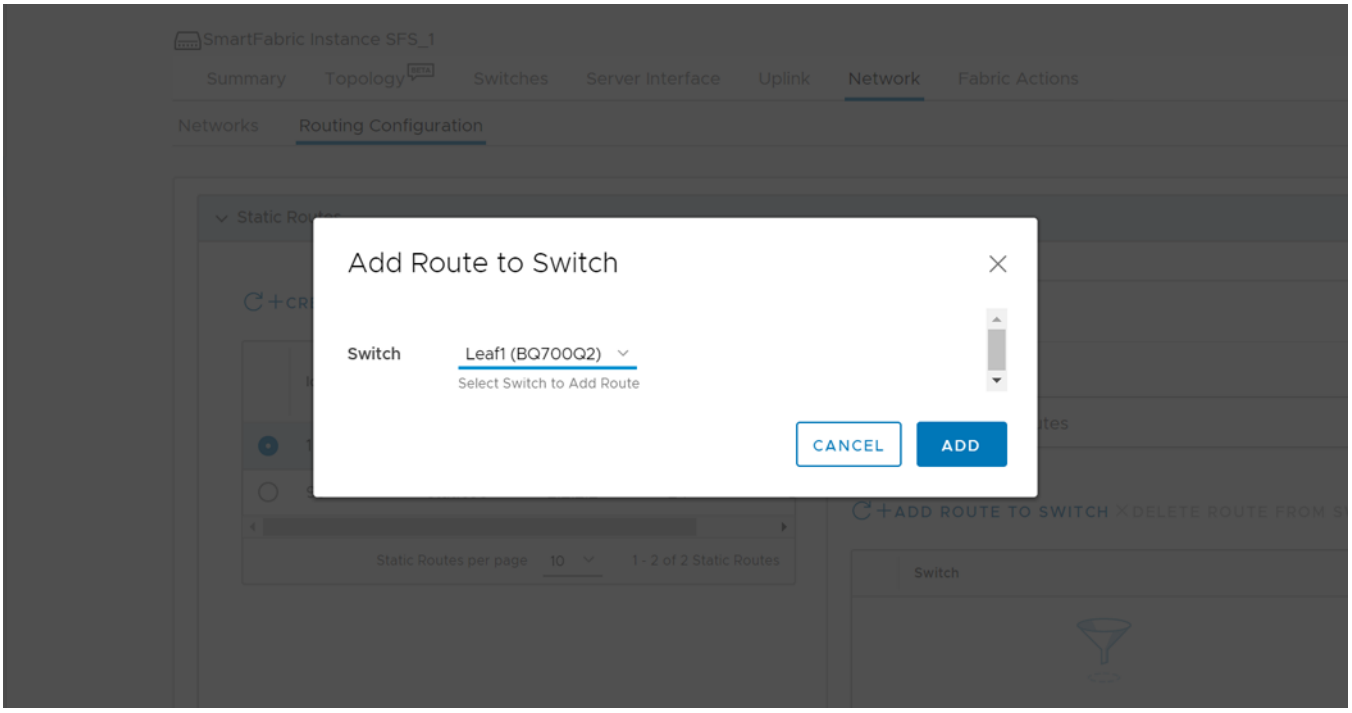
3. The system displays static route deletion is successful.

Add route to switch

1. Select **Routing Configuration** > **Static Routes**.
2. Select a static route, and click **Add Route to Switch**.



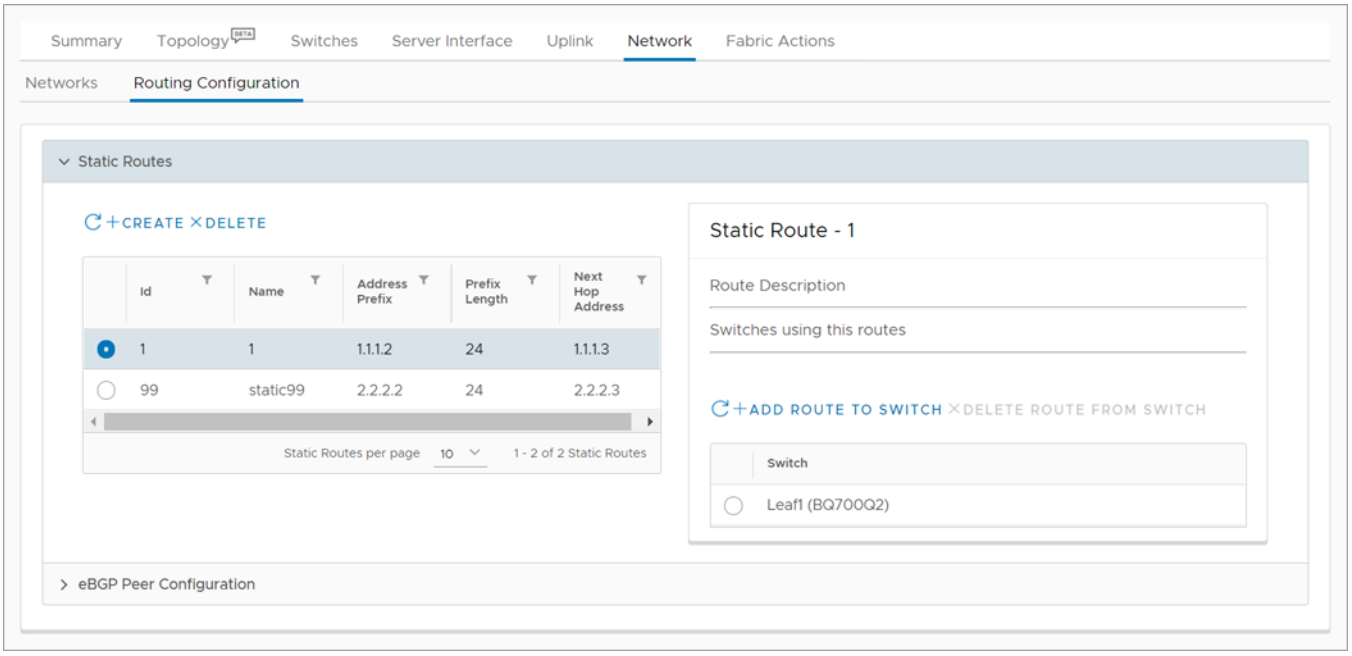
3. Select the switch to map to this route, and click **Add**.



4. The system displays the route added success message.

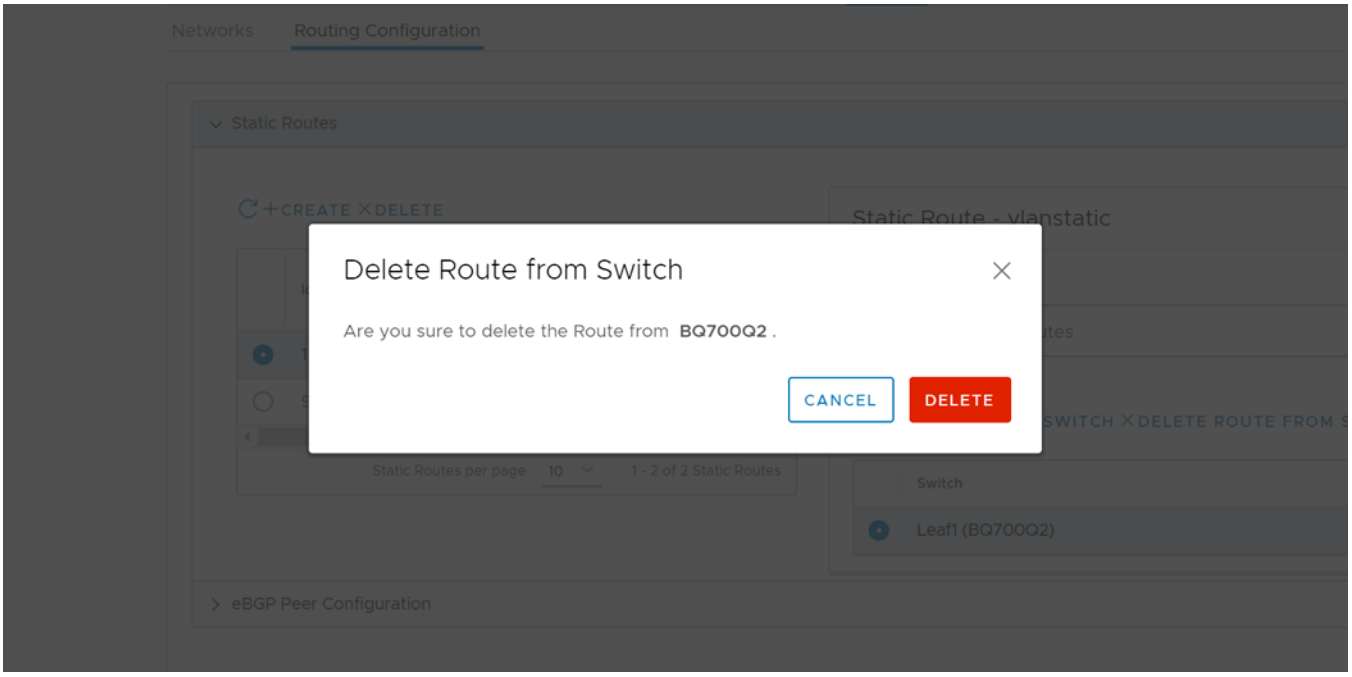
Static route details

The static route details display a list of mapped routes. Select a static route to view details pertaining to that specific route including the switch ID.



Delete route from switch

1. Select the route to delete, and click **Delete Route**.
2. Click **Delete** to confirm the removal of the route from the switch.

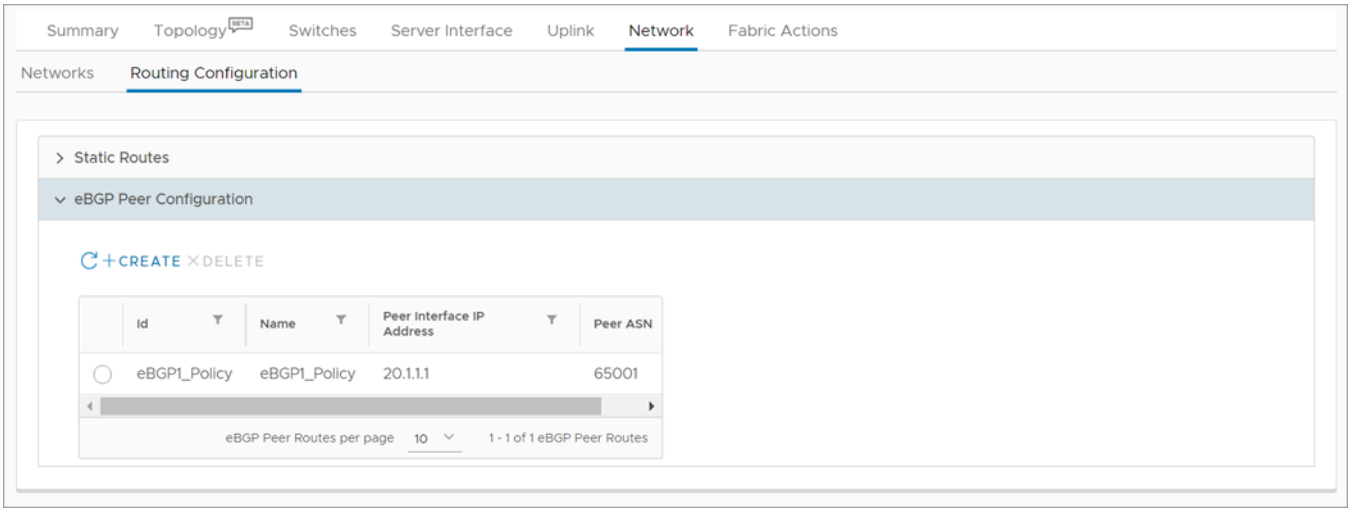


3. The system displays route policy deletion success message.

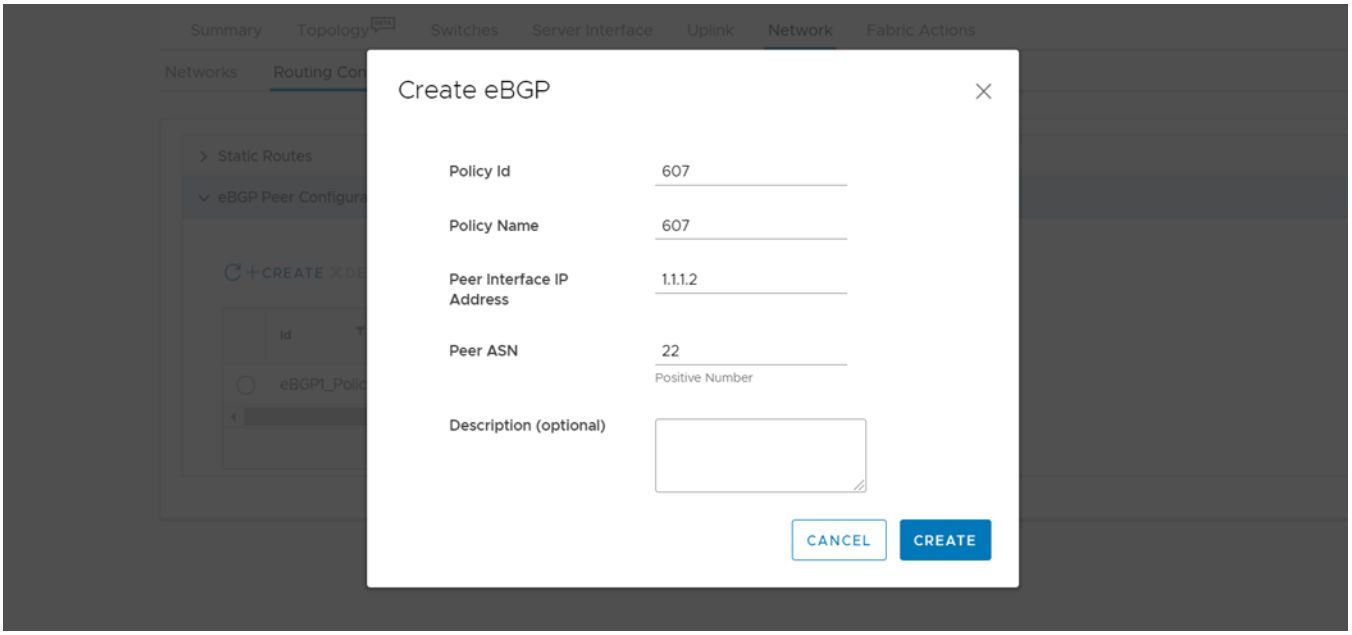
Configure eBGP peer route

Create eBGP route

1. Select **Network** > **Routing Configuration**, and click **eBGP Peer Configuration**.



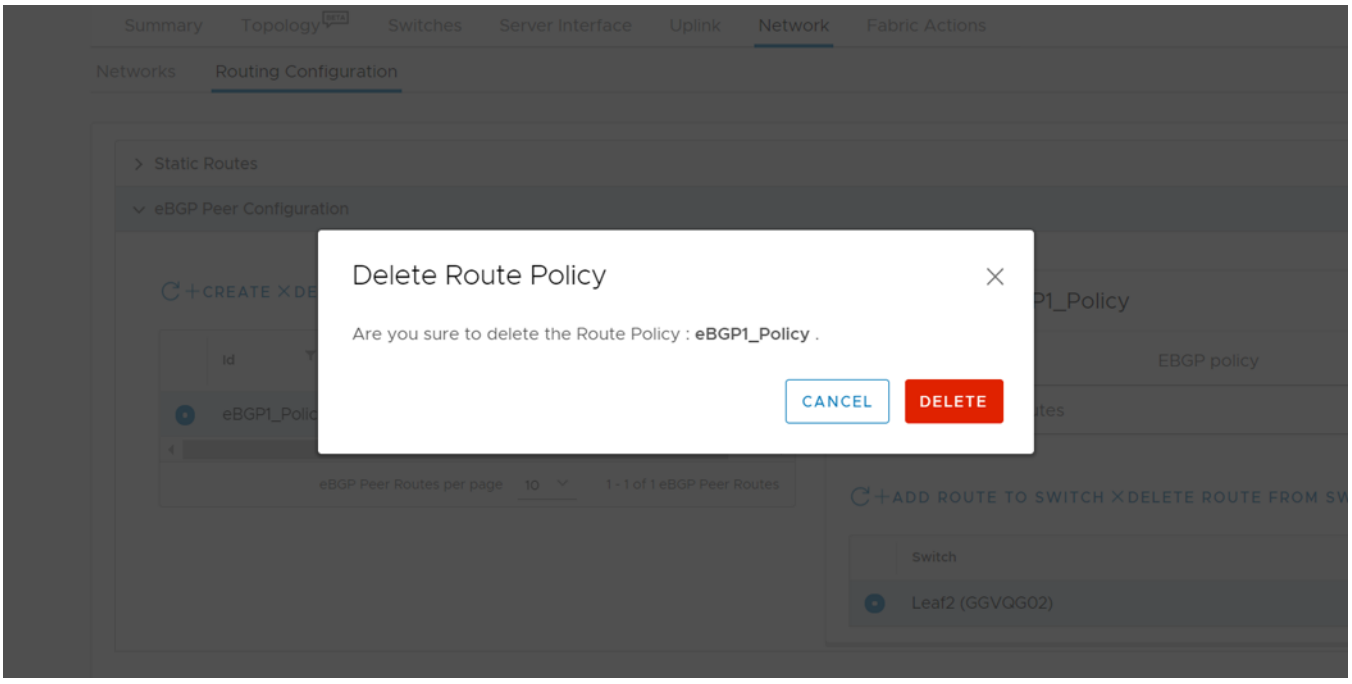
2. Click **Create** to add an eBGP peer route.



3. Enter the relevant details and click **Create**.
4. The system displays eBGP peer route creation is successful.

Delete eBGP route

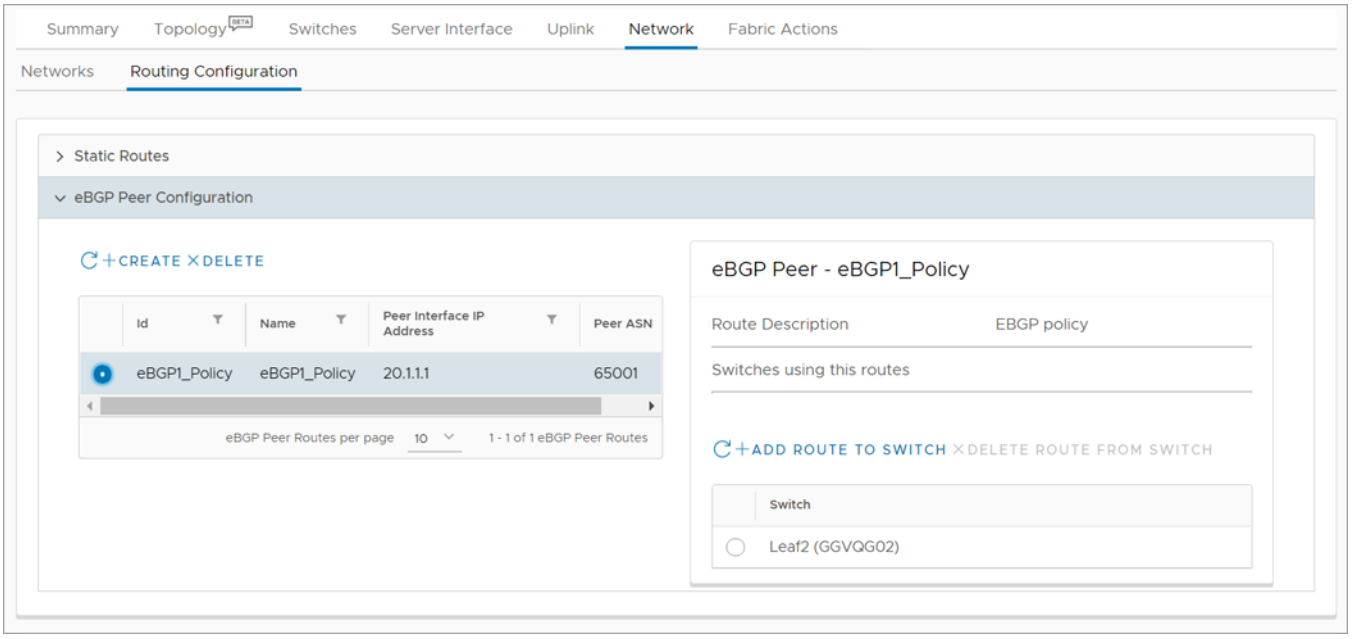
1. Select the eBGP route to delete, then click **Delete**.
2. Click **Delete** to confirm.



3. The system displays route policy deletion success message.

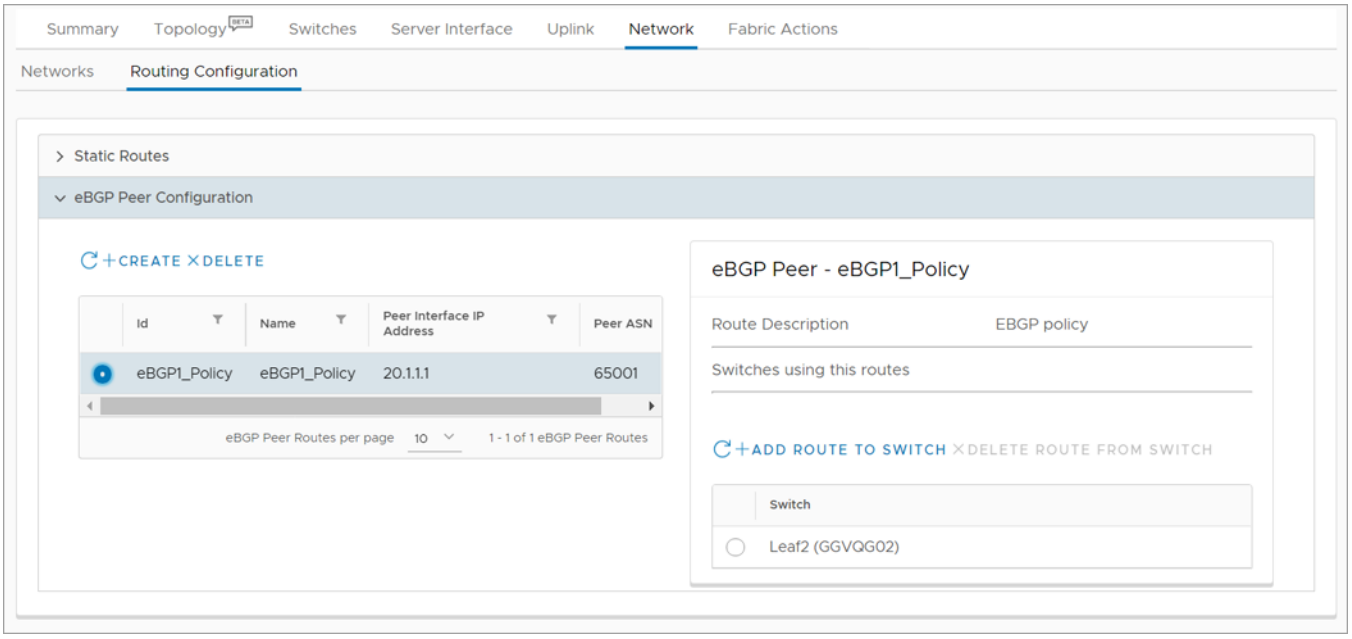
View eBGP peer details

The eBGP peer details display a list of mapped routes. Select an eBGP route to view details pertaining to that specific route including the switch ID.

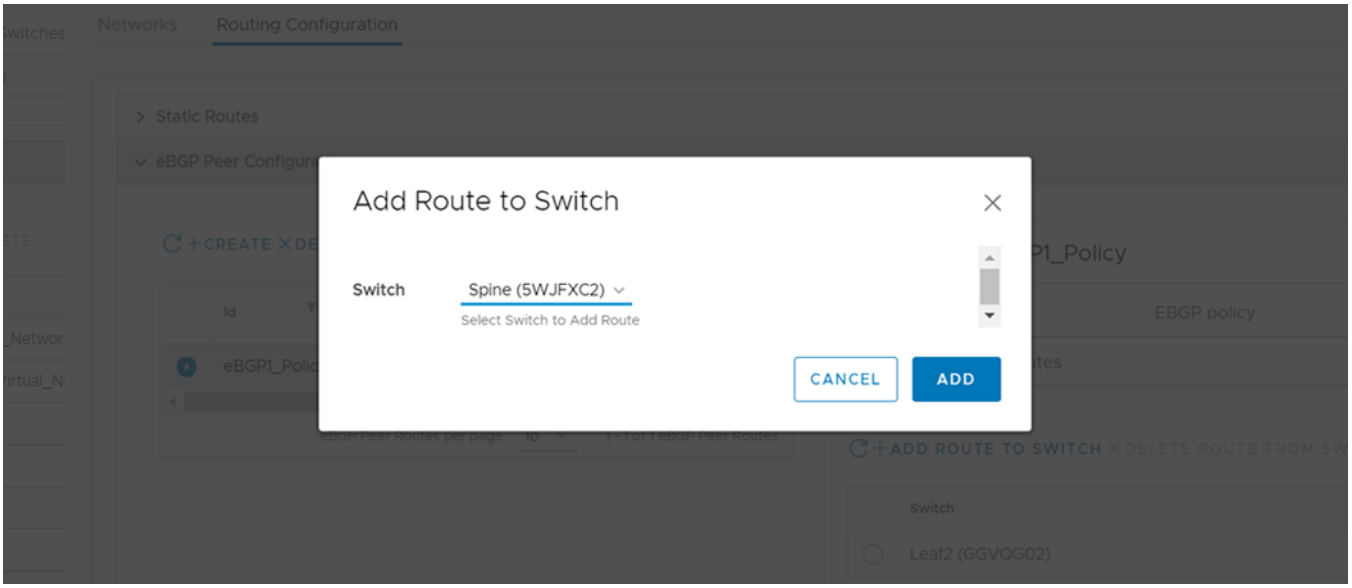


Add eBGP route to switch

1. Select an eBGP route, then click **Add Route to Switch**.



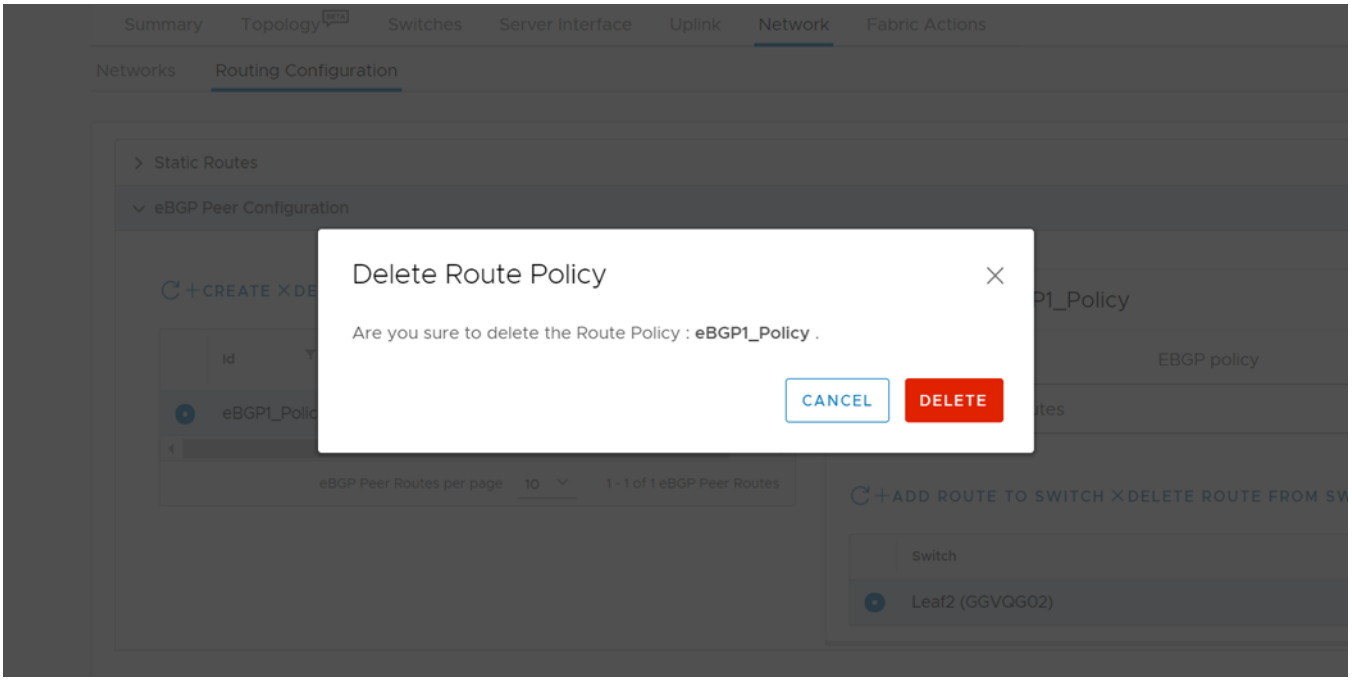
2. Select the switch, then click **Add**.



3. The system displays the route to switch addition success message.

Delete eBGP route from switch

1. Select an eBGP route, then click **Delete Route**.

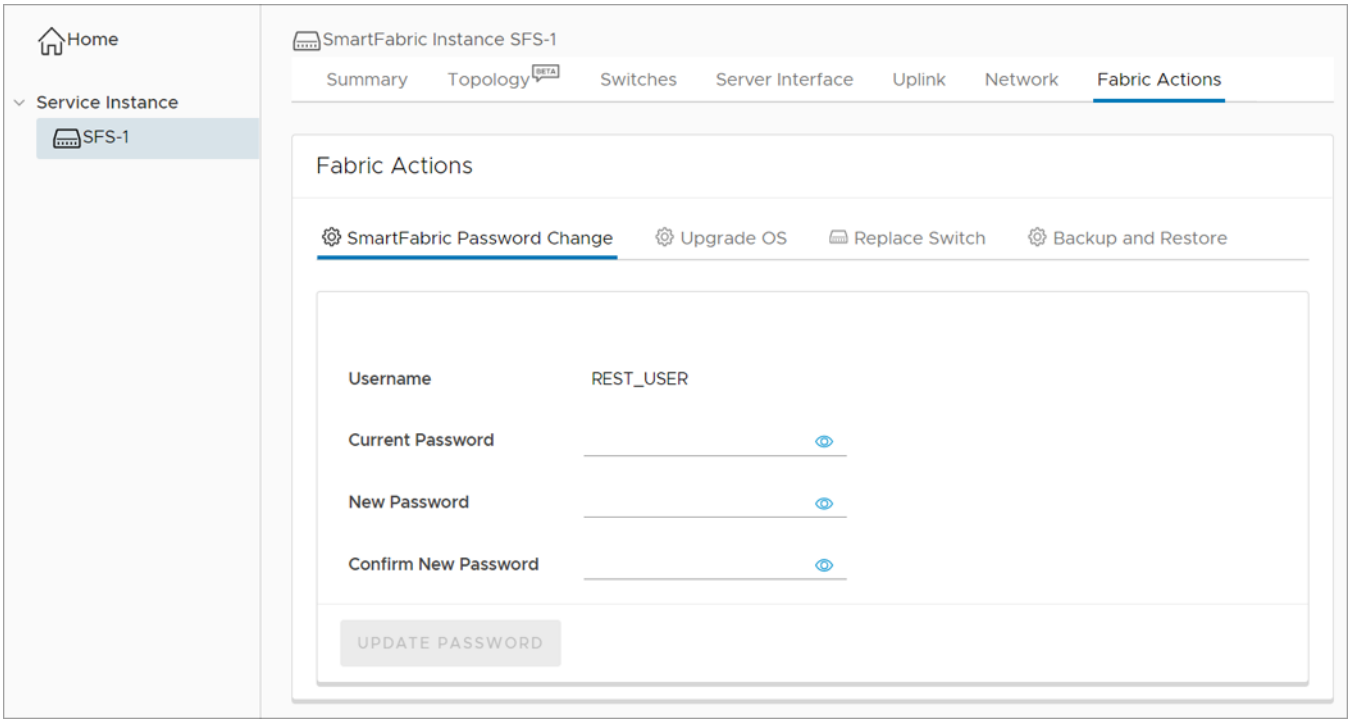


2. Click **Delete** to remove the route from the switch.
3. The system displays route deletion success message.

Configure fabric management actions

From **Fabric Actions** pane, you can:

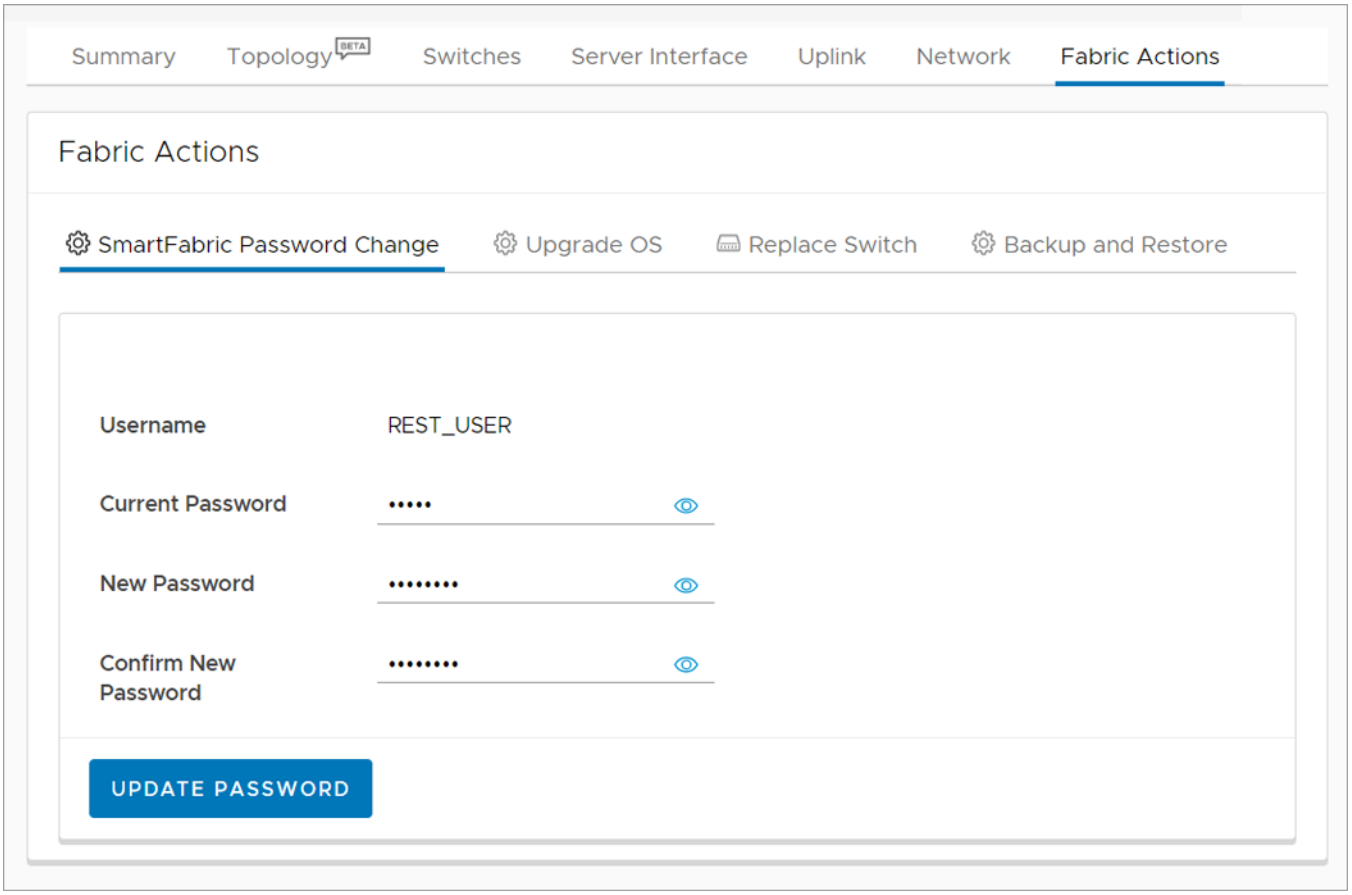
- Change SmartFabric password.
- Upgrade SmartFabric OS10 image, see Upgrade SmartFabric OS.
- Replace a switch in a network fabric, see Replace switch in a fabric.
- Fabric backup and restore, see Back up and Restore fabric configuration.



Change SmartFabric password

To change the SmartFabric password:

1. Select the **Service Instance** > **Fabric Actions** > **SmartFabric Password Change**.



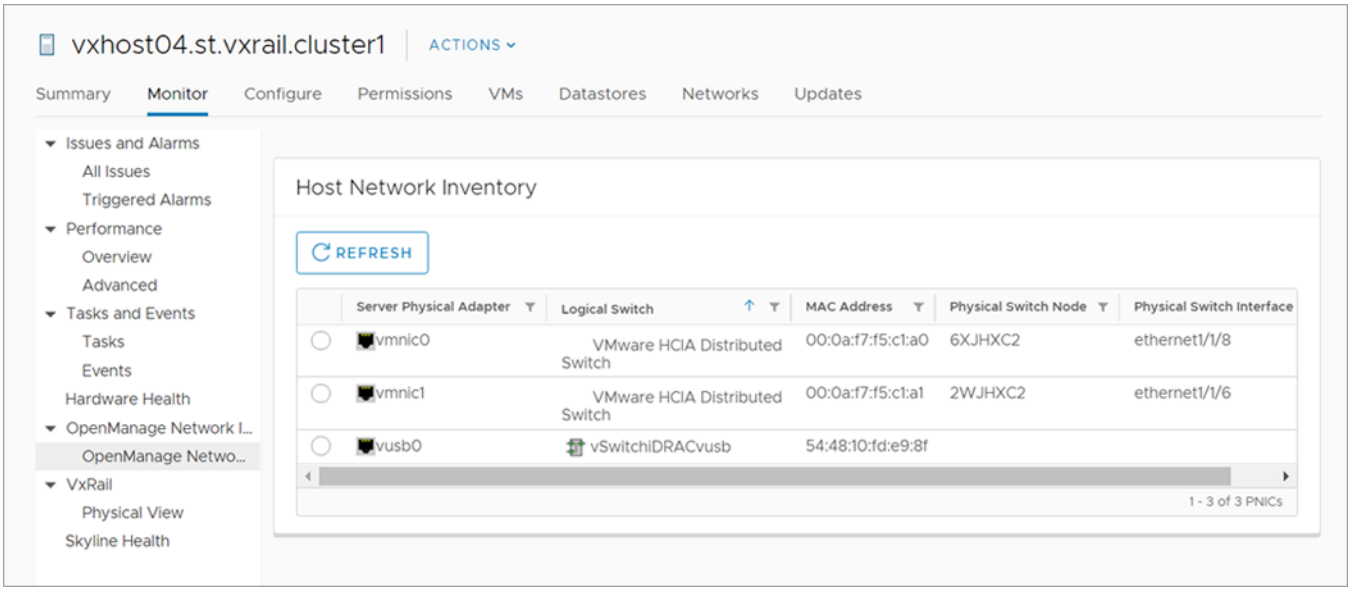
2. Enter the current password for the REST_USER, the new password, confirm the new password, and click **Update Password**.
3. The system displays password update success message.

Host network inventory

You can view information about physical Dell EMC PowerSwitch infrastructure running SmartFabric OS10.

Host network inventory page

Select a host in vCenter, select the **Monitor** tab, then select **OpenManage Network Integration** (OMNI) in the monitor sidebar.



Refresh button

Click **Refresh** to update the host network inventory data and display updated contents.

Physical adapter table

Select a switch from the Host Network Inventory to view detailed information. The table is default-sorted by descending switch name to group physical adapters belonging to the same switch.

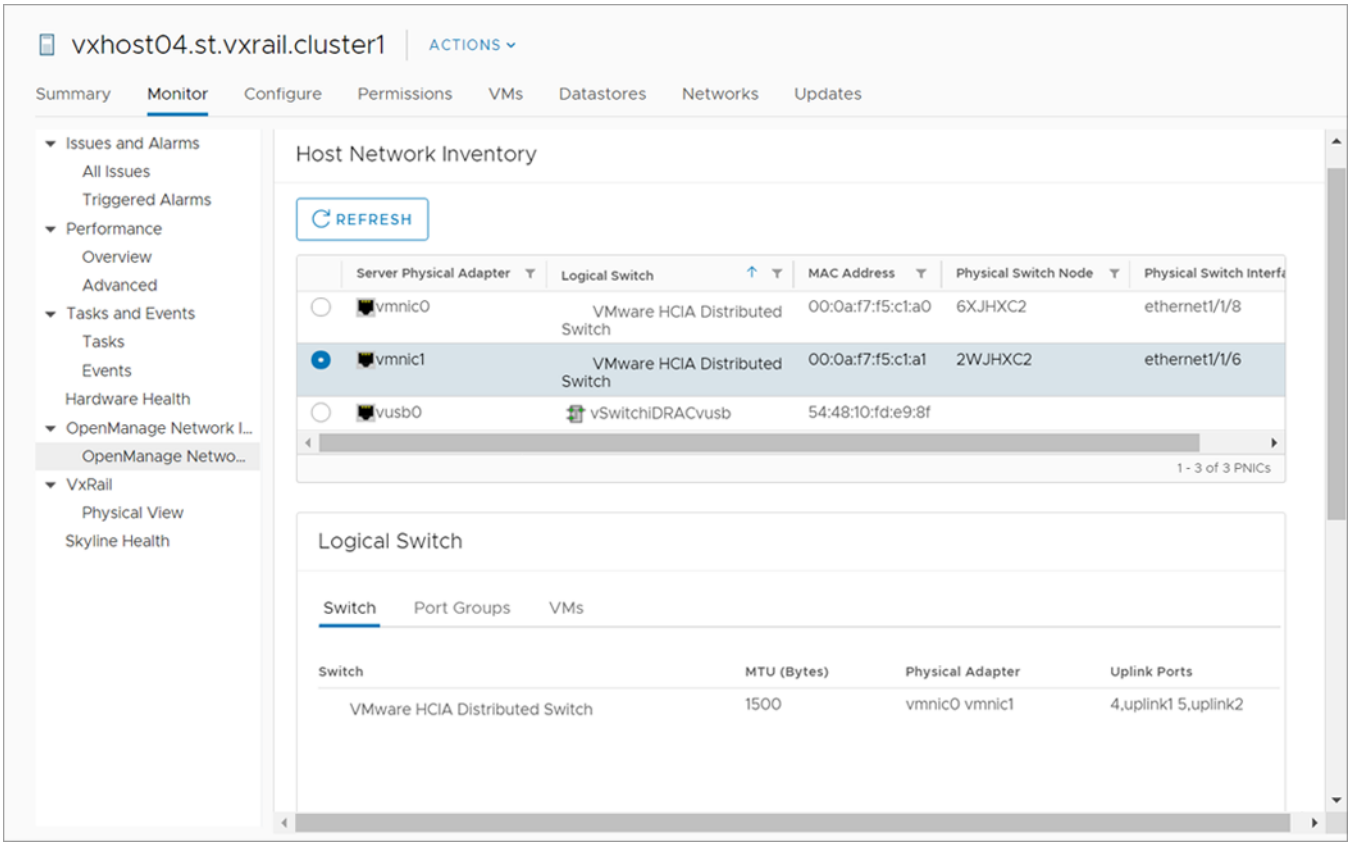
- Physical adapter — Name of the physical network adapter.
- Virtual switch — Name of switch the physical adapter is connected to.
- MAC address — MAC address of the physical adapter.
- Physical switch — Physical switch that is connected to the fabric.
- Physical switch interface — Physical switch port this server network adapter is wired to.

View logical switch details

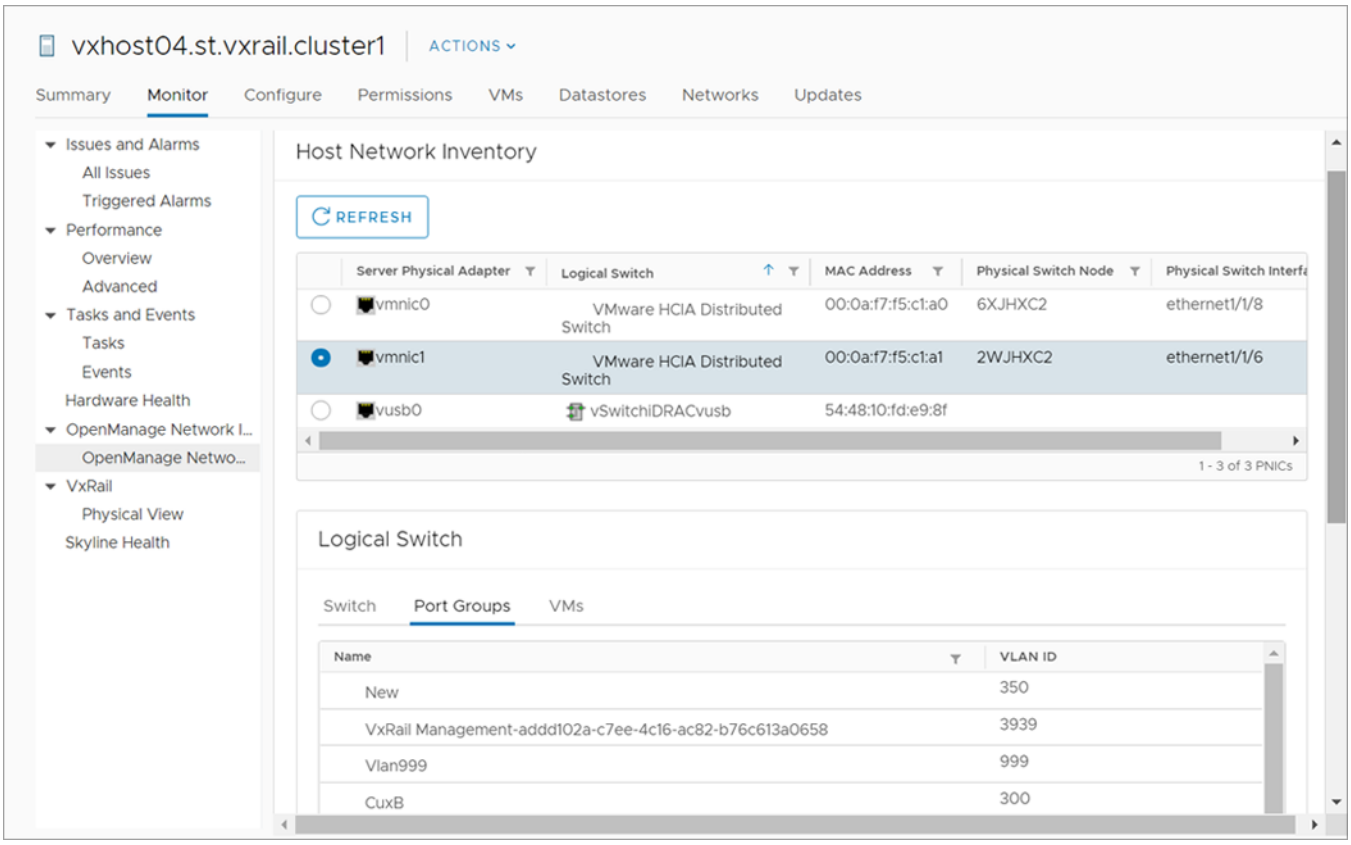
Displays information about the logical switch that is connected to the selected physical adapter.

When you select a switch from the Host Network Inventory, the page displays the logical switch information connected to the selected physical adapter.

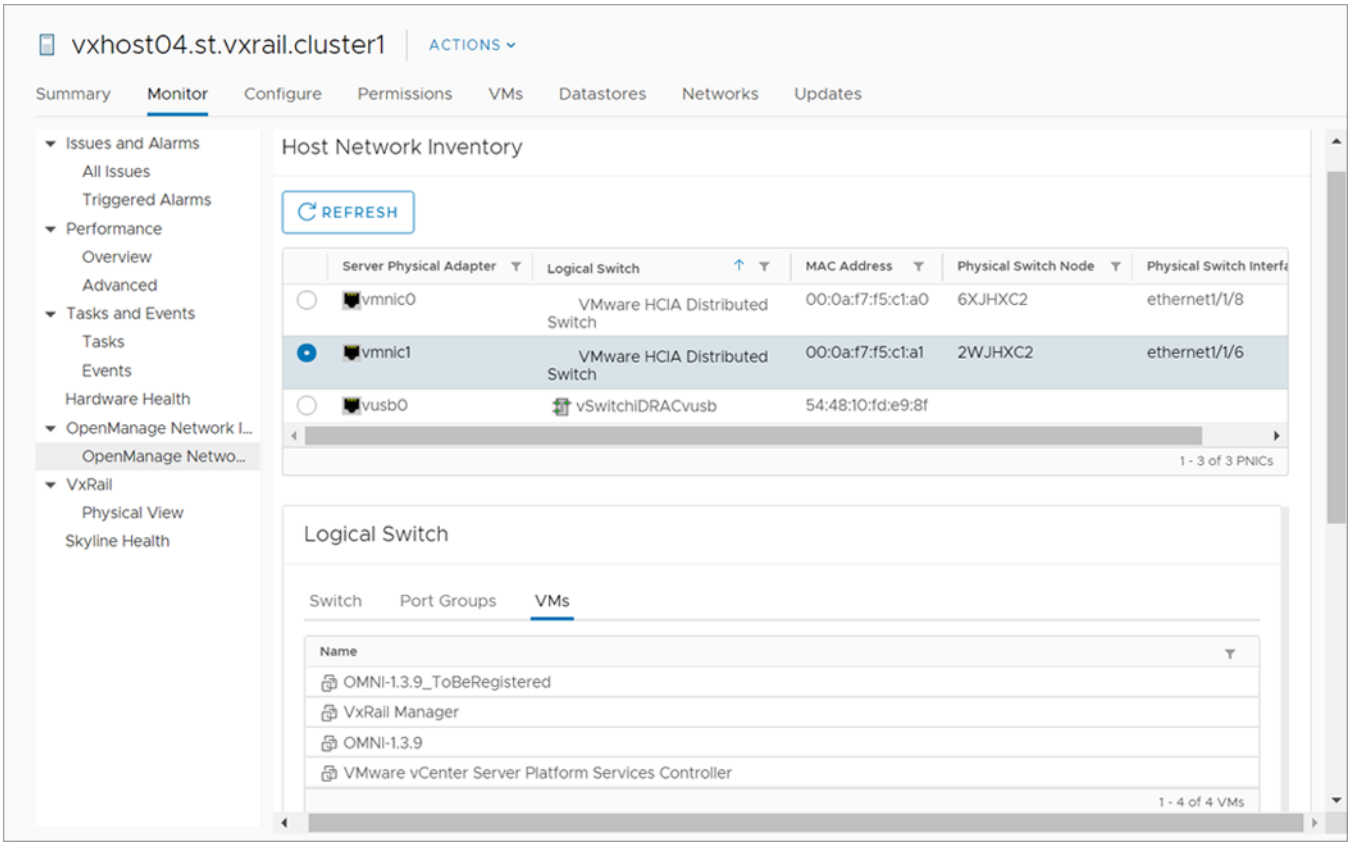
- Switch tab — includes name of switch, MTU in bytes of switch, physical adapters connected to the switch. and uplink ports on the switch



- Port groups tab — includes the name of port groups, and VLAN IDs for each port group



- VMs tab — includes the name of VMs of that host that is connected to a single virtual switch

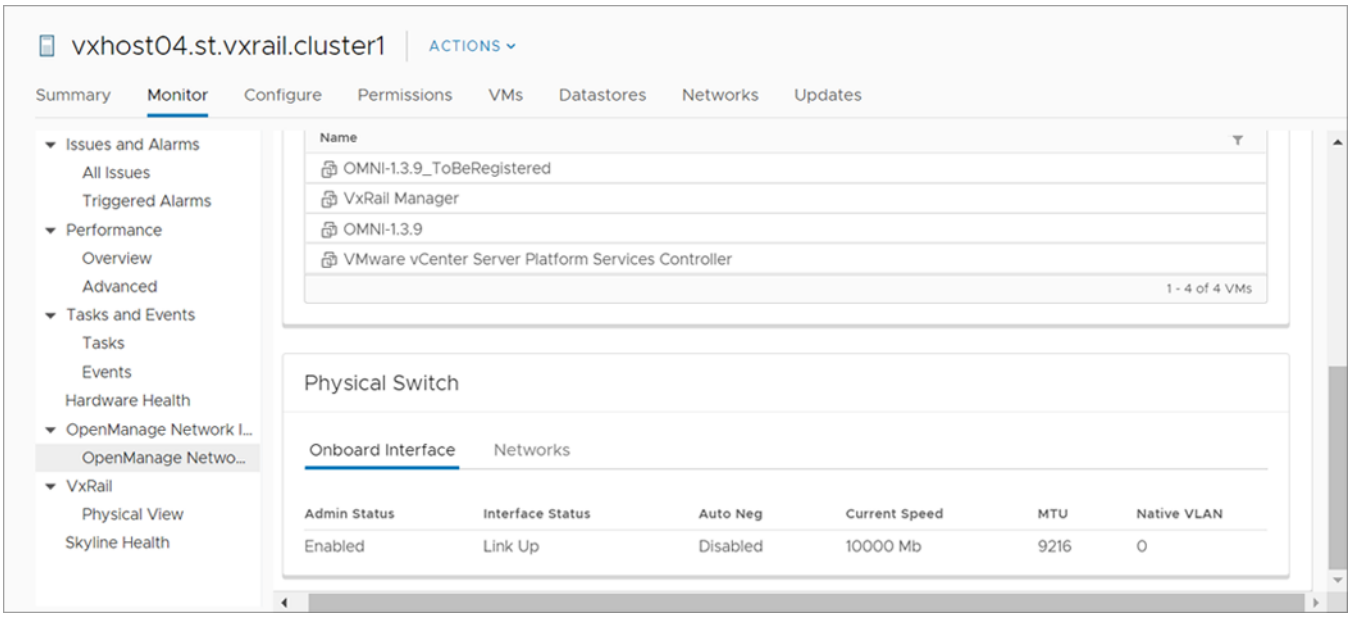


View physical switch details

Displays information about the onboard interface. This information displays only when there is a physical connection between the VxRail domains and OMNI.

When you select a switch from the Host Network Inventory, the page also displays the physical switch information connected to the selected physical adapter.

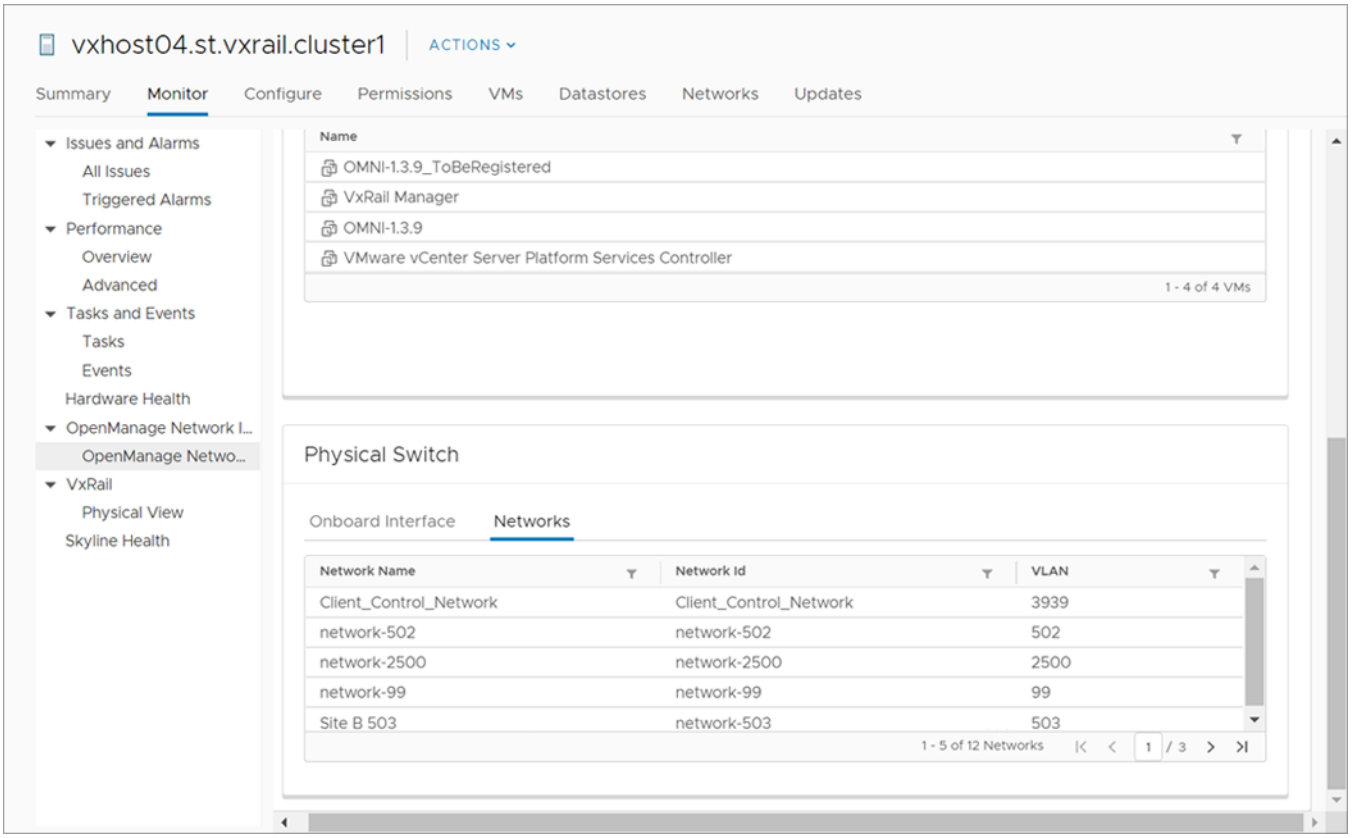
Onboard interface tab



- Admin Status — configured state of the physical interface
- Interface Status — current operations state of the physical switch port

- Auto Neg — negotiation status of the physical interface
- Current Speed — current operational speed of the physical interface
- MTU — maximum transmitting unit configured on the physical interface
- Native VLAN — untagged default VLAN for the physical switch

Networks tab



- Network Name — name of the VLAN network
- Network ID — unique identifier of the fabric network
- VLAN — tagged VLAN of the switch port

8

Lifecycle management

This chapter explains common lifecycle operations of upgrading the SmartFabric OS10, OMNI appliance, switch replacement, fabric backup, and restore.

Upgrade OMNI appliance

This section explains how to upgrade the OMNI appliance for major and minor releases.

Upgrade OMNI during major releases

To upgrade OMNI appliance from older version to 1.3:

1. **Prerequisite**

   Save the following details:

   - IP address or hostname of the SmartFabric instances that are manually added in the OMNI VM.
   - IP address or FQDN information of all the vCenters that are registered with the OMNI VM.
   - IP address or hostname of the OMNI VM.
   - Details of the `ens192` and `ens160` interface settings.
2. Unregister the older version of OMNI VM from the vCenter, see Manage vCenter with OMNI.
3. Shut down the older OMNI VM.
4. Deploy the new OMNI VM, see Create OMNI virtual appliance.
5. Configure the OMNI VM with the documented settings and complete the full setup, see OMNI setup.

Upgrade OMNI during minor releases

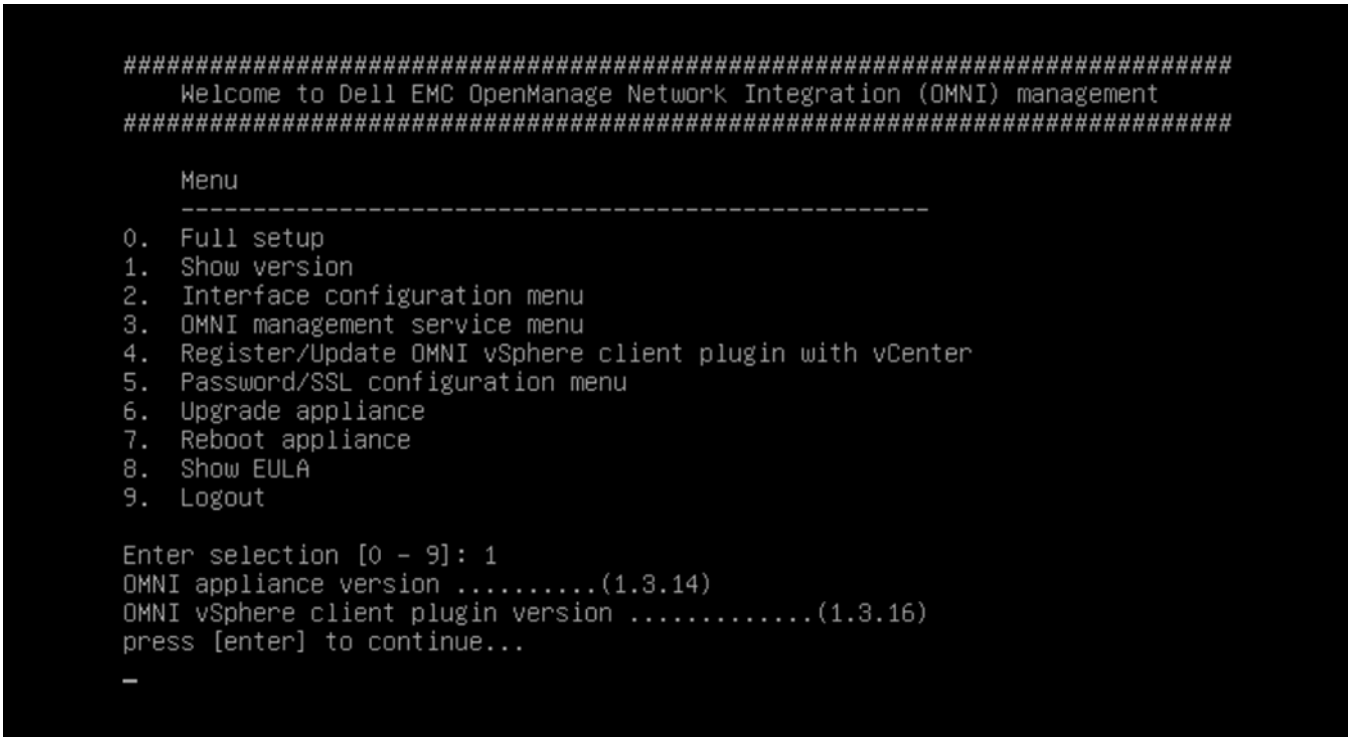
You must be in the OMNI VM Console to use these steps. After you upgrade the appliance, register the appliance with the vCenter Server then.

NOTE: The OMNI appliance upgrade information only applies to the OMNI minor release upgrade. For example, use this option to upgrade the OMNI VM from 1.3.16 to 1.3.18.

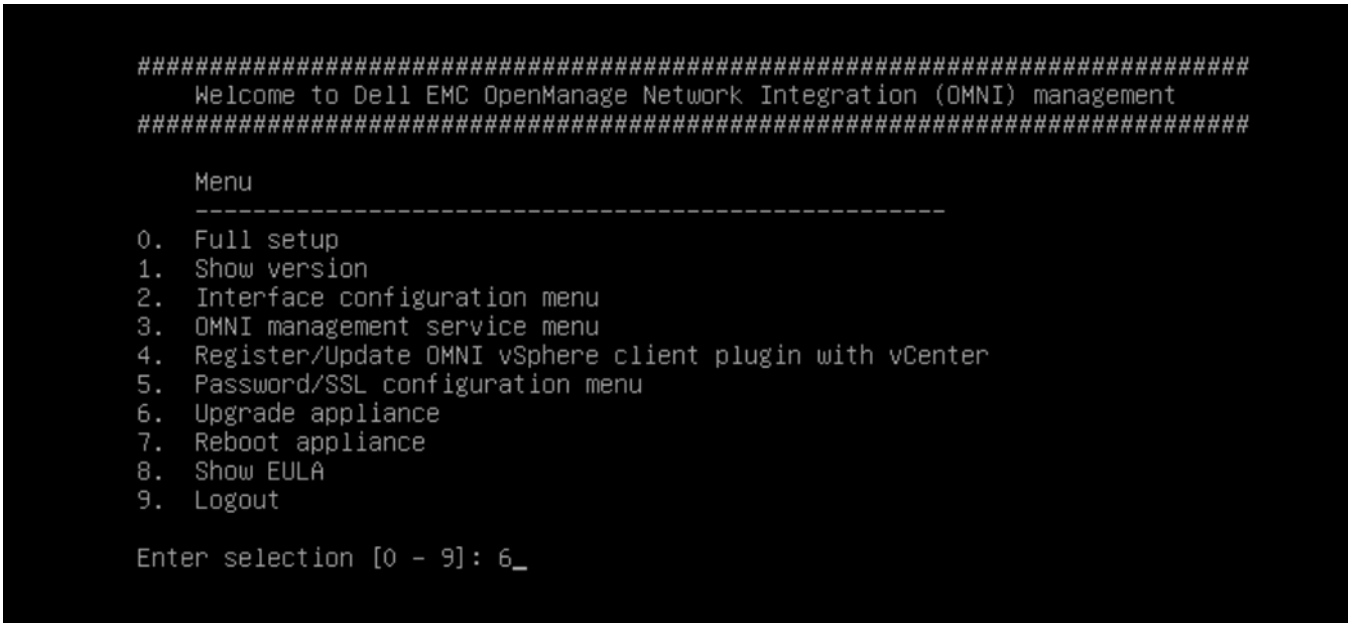
To upgrade OMNI appliance from one minor version to another:

1. Download the OMNI upgrade image from the Dell EMC Support portal and store the image on an SCP server.

   Check the existing version.



2. From the OMNI VM console, select the option **6. Upgrade Appliance**.



The display lists all the applications which can be upgraded along with the old and new versions. Upgrading requires restarting the services.

3. Enter the SCP server IP address or hostname, username, and the path to the upgrade .zip file and password.

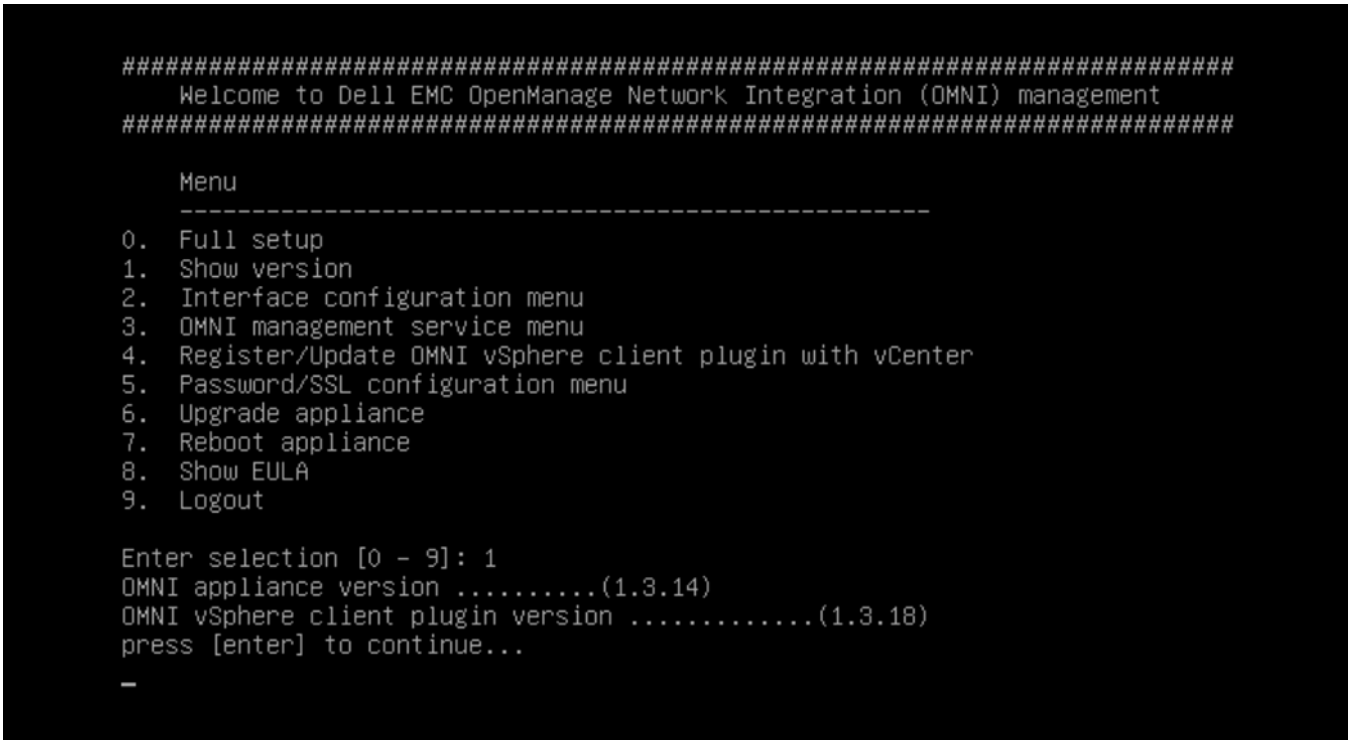
```
################################################################################
    Welcome to Dell EMC OpenManage Network Integration (OMNI) management
################################################################################

    Menu
    --------------------------------------------------
0.  Full setup
1.  Show version
2.  Interface configuration menu
3.  OMNI management service menu
4.  Register/Update OMNI vSphere client plugin with vCenter
5.  Password/SSL configuration menu
6.  Upgrade appliance
7.  Reboot appliance
8.  Show EULA
9.  Logout

Enter selection [0 - 9]: 6
2020-06-09 00:59:48 INFO  [setup.sh] Getting the upgrade file
Remote SCP server IP/hostname: 10.11.201.26
Username: admin
Path to the upgrade zip file: /tmp/OMNI-upgrade-1.3.18.zip
admin@10.11.201.26's password:
```

4. Verify all information, then enter **Y** to continue.

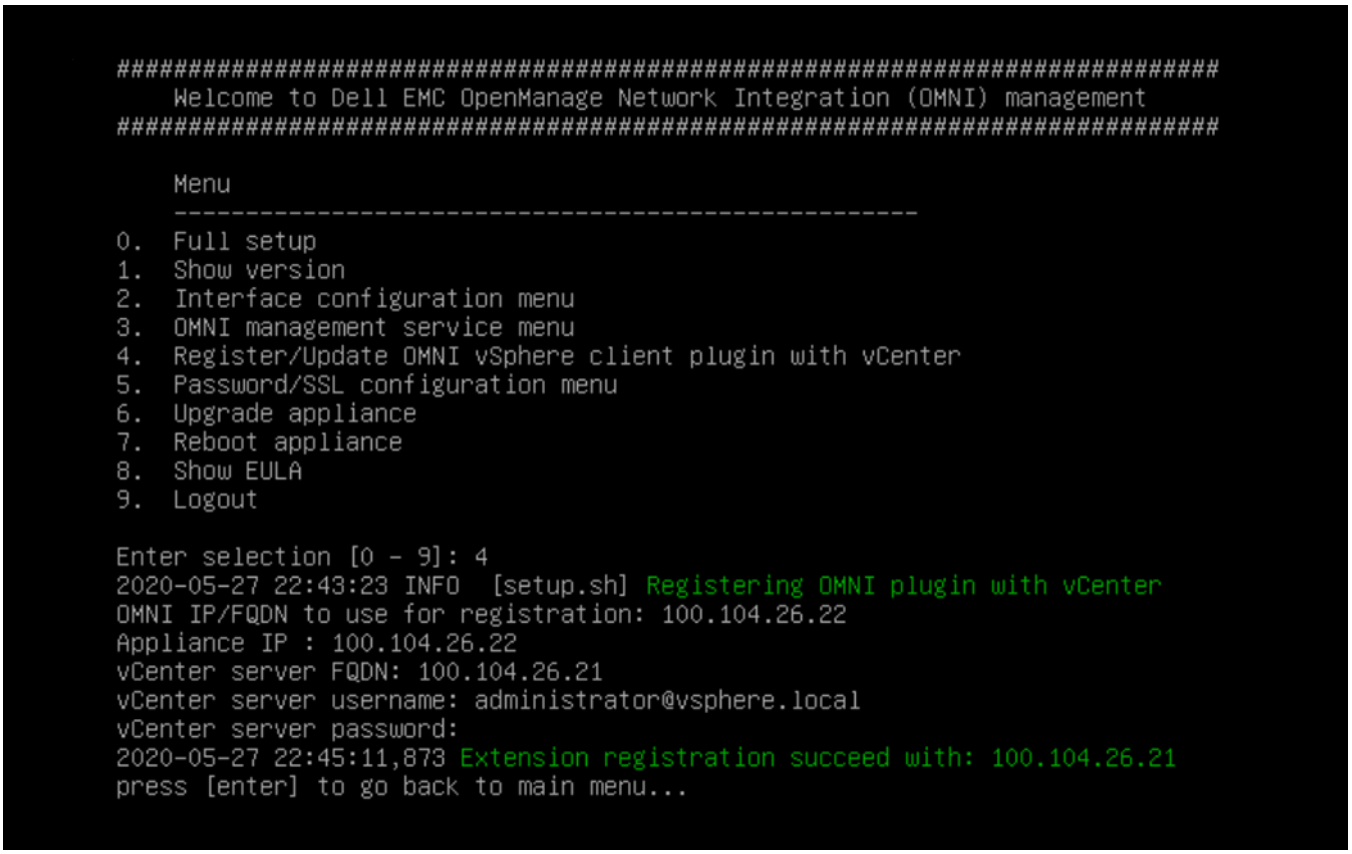
```
admin@10.11.201.26's password:
OMNI-upgrade-1.3.18.zip            100%  413MB 189.5MB/s   00:02
2020-06-09 01:02:23 INFO  [setup.sh] File successfully copied to
/home/isengard/upgrade/upgrade.zip
2020-06-09 01:02:23 INFO  [setup.sh] Verifying...
Archive:  /home/isengard/upgrade/upgrade.zip
  inflating: /home/isengard/upgrade/setup.sh
 extracting: /home/isengard/upgrade/version.txt
  inflating: /home/isengard/upgrade/passwd_mgr.py
 extracting: /home/isengard/upgrade/sslworkspace.zip
 extracting: /home/isengard/upgrade/rls.label
 extracting: /home/isengard/upgrade/vcenterapp.zip
2020-06-09 01:02:26 INFO  [setup.sh] OMNI applications will be upgraded
2020-06-09 01:02:26 INFO  [setup.sh] Setup file will be upgraded
2020-06-09 01:02:26 INFO  [setup.sh] Current OMNI appliance version : 1.3.14
2020-06-09 01:02:26 INFO  [setup.sh] Current OMNI plugin version : 1.3.16
2020-06-09 01:02:26 INFO  [setup.sh] New OMNI appliance version : 1.3.14
2020-06-09 01:02:26 INFO  [setup.sh] New OMNI plugin version : 1.3.18

Upgrade will restart the service if running. Proceed? [y]? y_
```

```
Deleted Images:
untagged: omni_api:1.3.16
deleted: sha256:b74a6bcaef6a0cb5bddbdfbcfe95a65b986bf16bd57baa7442be7f6bfde535db
deleted: sha256:b38a969d203cf912596a3315dee9d9c6b2a59ed28c3ea0df52760a873557046a
deleted: sha256:faf5a9a889563441d85fe9b9a6aa56e71c830a0428e501acefc52234da4204b9
deleted: sha256:e8c221ea7f6e27d7522b39c2f286e9c6c314501943c12eb720d66e0dcaa216cb
deleted: sha256:a93af37c97f86ddaf0142f4bbb26b7d37cc6f33d260dc1e84206bde3f3994686
deleted: sha256:eb837a36308d64855beb10d447128cad8e05a2a46b31721a66991da230c806ef
deleted: sha256:dfeccb855bbb49569ce74975cf1f0abf142146dedbe7faec58958e92c8660853
deleted: sha256:e6a4ef29eac986e9fdd62db2259029f86e972f7f35c59bc581ba28cb1430eaea
deleted: sha256:a4af04414a305e9ee614ba09a8611053f3aad9e657788c6d0d5b00f62e450e37
deleted: sha256:71e0704daed13a9f2ad9719a5bff2f88040a3e25bc92781e7608c44a85c8c08b
deleted: sha256:1530409102eb508e141789eda959e5f0d477c2d01eade3d04cc79b3474d5695e
deleted: sha256:e9439b40b20f9242279e9d7c7ee3a7ebb65bccfd8c80ad5b913323c38992da57
untagged: omni_db:1.3.16
deleted: sha256:12105165d7c98163621ef5690c3e0bc70f47363a78312738cd6de2edaf239af7
deleted: sha256:59e37a21240db89f411d4db2af49c7b38a38673c9f46b2e4d9a1888de86c5e00
untagged: omni_nginx:1.3.16
deleted: sha256:97405fdc4903348cd2ed3e97d5081aeef3afe0e9d6864769a817320739f26ffc
deleted: sha256:a042897f6913019143e8523b8515a8118ec981c636858b4eeed0d070b0f83f79
deleted: sha256:41941d8ddde4536258de137b984ccffaeeaaed8ecb3d3d3797cfde5bb794d4c9
deleted: sha256:bf7e2b14afa2e1d8a11af89e28ce0b429d477c70ebb8bfe57c2d1a174c1169e3
deleted: sha256:d7209c3b4a771e4890e391ee87cb14369128a352e942c5a7ab24dd9794ac420e
deleted: sha256:e087dbc984642a1a75477871343bd82daab105ae7bbb18a1a08999beb85abcee
deleted: sha256:490a28a6ff630009c3f279de6673e69fad50565f2c38b0f6a803e91d156b69dd
deleted: sha256:f96361a50e82dfc1c2ef6cee47b0f60e9f38c50e9926546829bdac4b7a80ec68
deleted: sha256:d74247f928c76f06384a245bc18a3156168c81fffeef09b5cd6d9b72dfc6fd39
deleted: sha256:55dbbfa3215fc6458b6f61a71b3c491dc3d8b549983618cd0fb328cc2ea1315d

Total reclaimed space: 99.6MB
2020-06-09 01:04:20 INFO [setup.sh] Removing upgrade files
2020-06-09 01:04:21 INFO [setup.sh] To get an updated plugin version in vCenter:
2020-06-09 01:04:21 INFO [setup.sh] plugin needs to be re-registered using
OMNI web client plugin menu (option 4 in main menu),


2020-06-09 01:04:21 INFO [setup.sh] Session will be closed now. Please log back in.
press [enter] to continue...
```

5. Verify the OMNI version.



6. Select **4. Register/Update OMNI vSphere client plugin with vCenter** to register the plug-in.
7. Enter the FQDN or IP address to use for registration, then repeat the steps to update the plug-in with the vCenter Server.



Upgrade SmartFabric OS in switch

You can upgrade SmartFabric OS from OMNI VM.

You can upload an OS10 image to upgrade the fabric. For more information about changing the SmartFabric password, see Configure fabric management actions.

You can upgrade OS using the following steps:

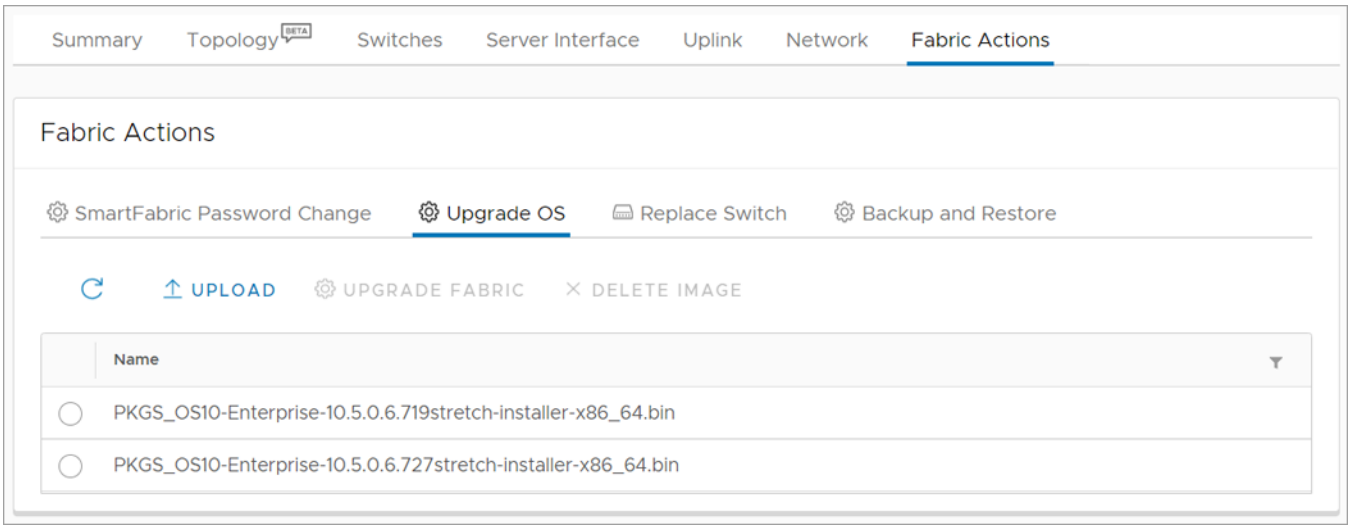
- Upload the latest image in the OMNI VM.
- Upgrade fabric using the uploaded image.
- (Optional) Delete the image from the OMNI VM.

NOTE: Dell Technologies recommends stopping the fabric automation service that is running before starting fabric upgrade. The system displays the notification before you start SmartFabric OS10 upgrade.

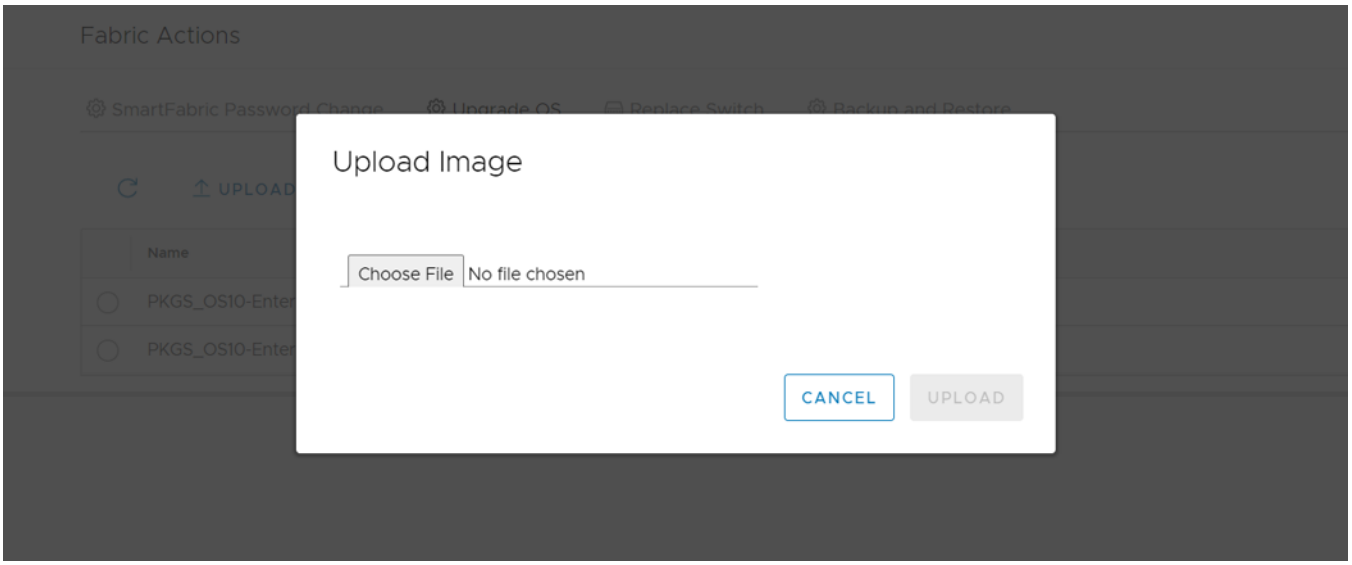
Upload image

Upload an OS10 image to the OMNI VM:

1. Select **Service Instance** > **Fabric Actions** > **Upgrade OS**.



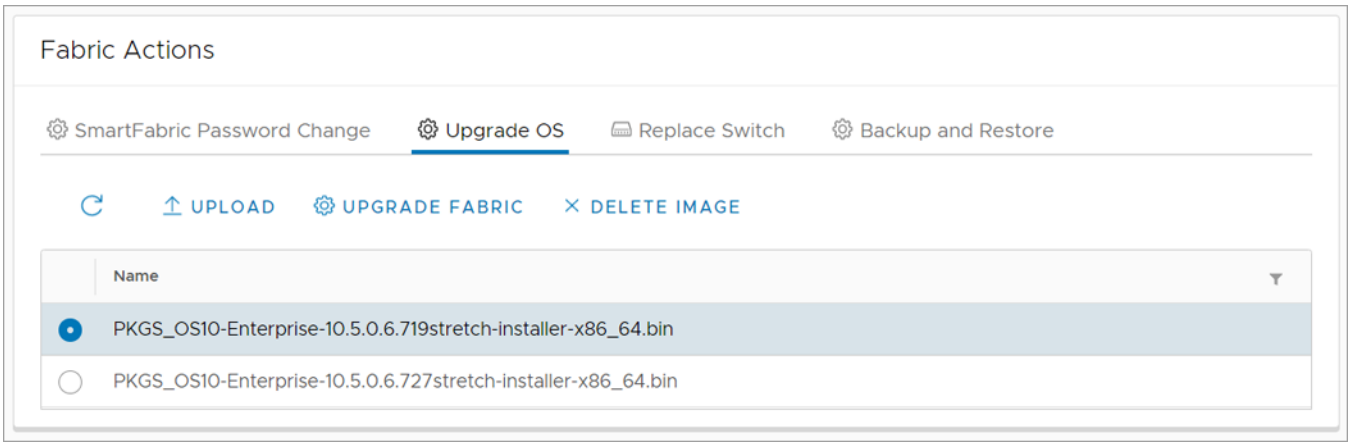
2. Click **Upload** to upload the .bin file.



Upgrade fabric

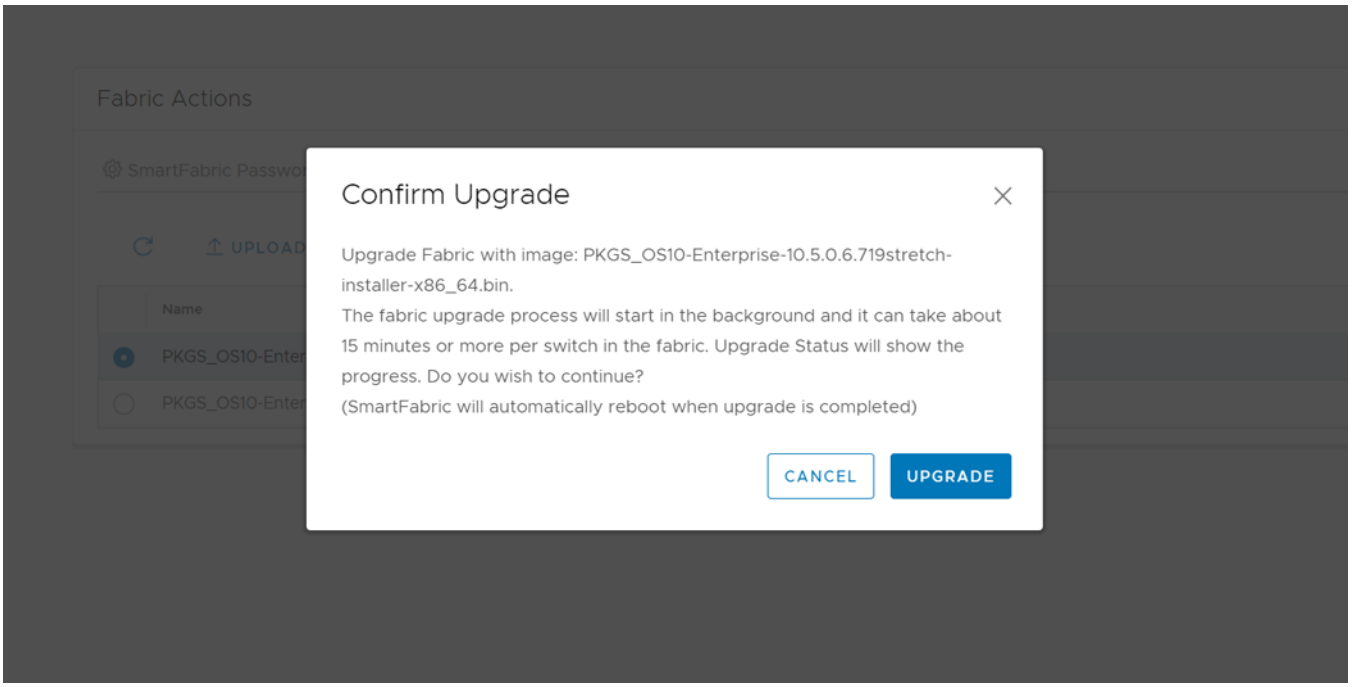
Upgrade the switches in a fabric with an OS10 image:

1. Select the .bin image, and click **Upgrade Fabric**.



NOTE: **Upgrade Fabric** option upgrades all the switches in a network fabric. You cannot stop the upgrade after it is triggered.

2. Click **Upgrade** to confirm.



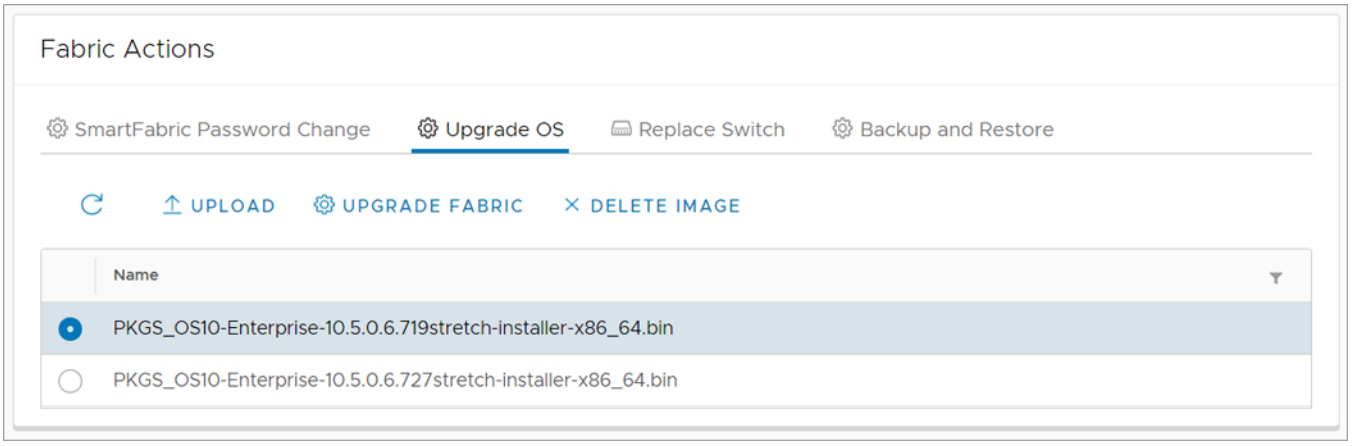
3. The system displays fabric upgrade success message.

   SmartFabric automatically reboots when the upgrade is complete.

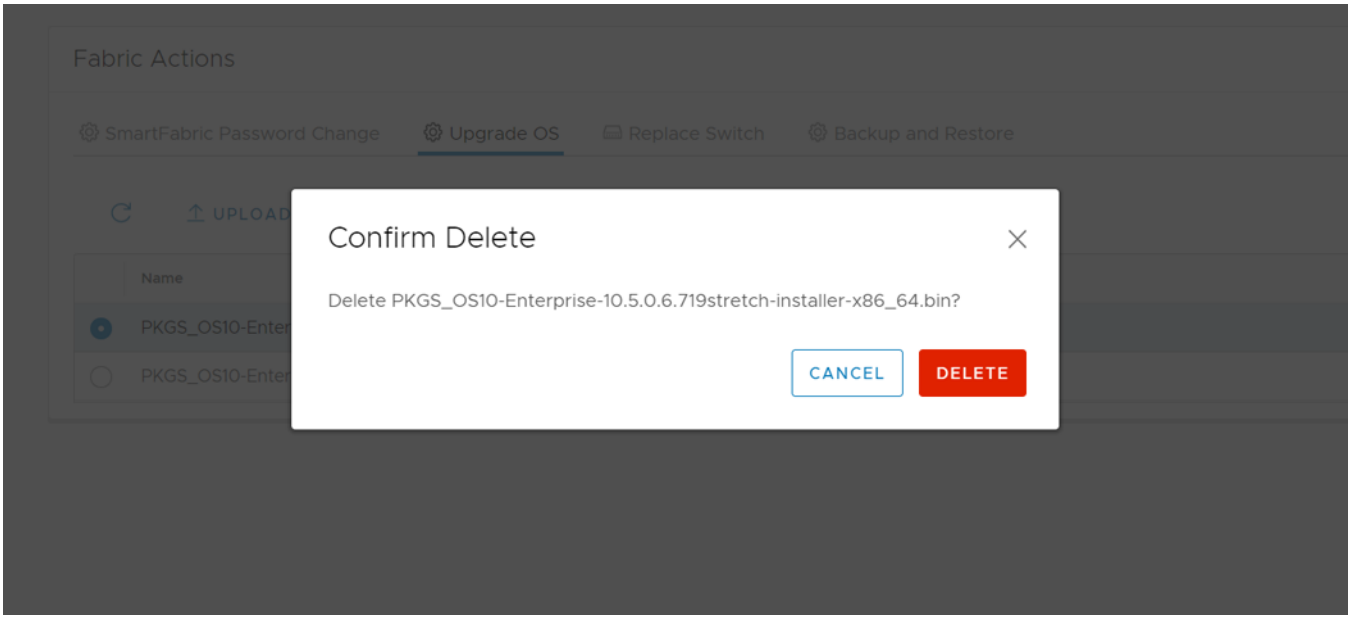
Delete image

Delete the OS10 image uploaded in the OMNI VM:

1. Select the .bin image to delete.



2. Click **Delete Image**.



3. Click **Delete** to confirm.
4. The system displays delete image is success.

Replace switch in a fabric

You can replace the faulty OS10 switch in a fabric. To replace:

1. Identify the OS10 switch to be replaced and label each of the cables with the port numbers before disconnecting the cables.
2. Back up the following configurations from the faulty switch to configure the new switch with the same details:
   - Hostname
   - Management IP address
   - DNS and NTP IP addresses if configured
   - Spanning-tree mode

     NOTE: In SmartFabric Services mode, RPVST+ is enabled by default on the uplink interfaces.
   - Other nonfabric commands
3. Ensure that the new switch has the same OS version as the faulty switch. You can check the version using the following command:

```
OS10# show version
```

4. Power off the existing switch to prevent data traffic loss in the cluster.
5. Remove the ICL and uplink connections from the existing switch, and connect to the new switch.

NOTE: Do not remove connections to VxRail nodes until the new switch is in SmartFabric Services mode.

NOTE: Ensure that the ICL ports are connected to the other leaf switch which is already in SmartFabric Service mode.

6. Enable SmartFabric Services on the new switch and define the ICL ports.
   - For **L2 personality**—Enable SmartFabric Services on the new switch, and define the breakouts, uplinks, interlink ports, plus any other parameters such as management VLAN, LACP, VLAN tagging, and so on.

     For example, if the uplink port is 1/1/4 and the interlink ports are 1/1/29,1/1/30, no VLAN tagging, LACP auto, management VLAN 1 as default.

     ```
     :~$ sfs_enable_vxrail_personality.py -i 1/1/6,1/1/8 -u 1/1/4 -l
     ```

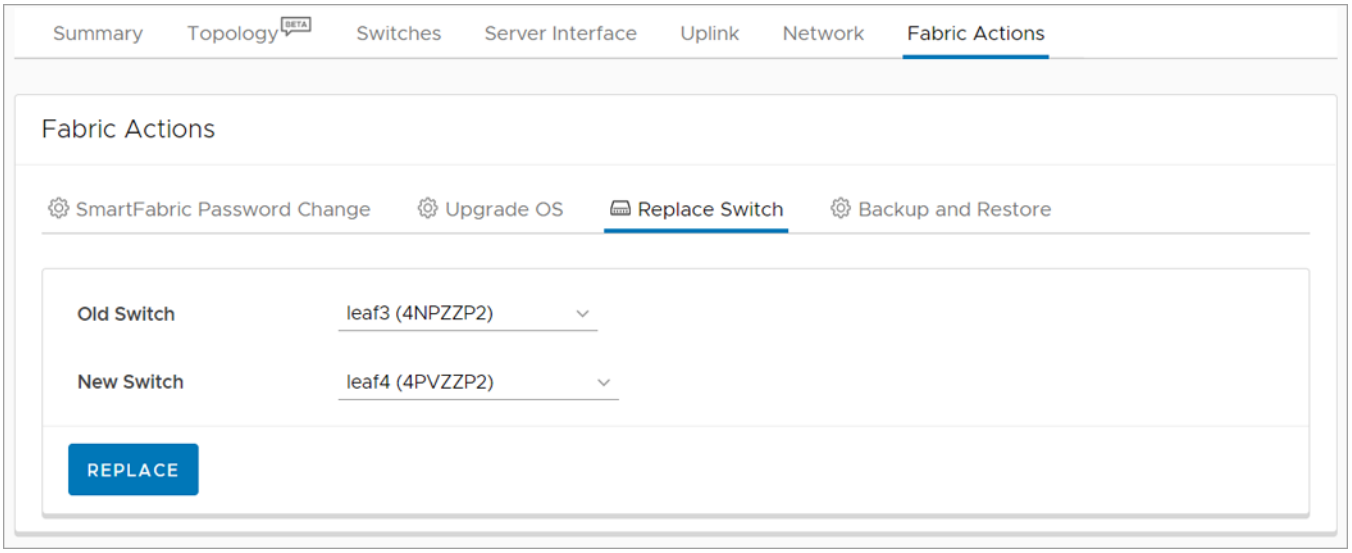
   - For **L3 personality**—Enable SmartFabric Services on the new switch using the `smartfabric l3fabric enable role` command. Example:

     ```
     OS10# smartfabric l3fabric enable role LEAF vlti ethernet 1/1/29-1/1/30
     ```

     For more information about enabling SmartFabric Services, see *Dell EMC SmartFabric OS10 User Guide Release 10.5.0*.
7. The new switch reboots and is placed in SmartFabric Services mode.

   NOTE: During reboot, the configurations are synchronized in the new switch and it takes several minutes.
8. Connect VxRail server ports to the new switch one-by-one to bring up the switch ports and advertise LLDP.
9. Review the command outputs on both switches for same configurations. Use the following commands to validate the configurations:
   - `OS10# show vlan`

     NOTE: The command displays if the switch is a primary or secondary peer.
   - `OS10# show vlt 255`
   - `OS10# show lldp neighbor`
10. After ensuring all the configurations are up and running, go to **OMNI** > **Service Instance** > **Fabric Actions** > **Replace Switch** to complete the switch replacement workflow.



11. Select the switch that you want to replace from the list, select the new switch, and click **Replace**. The system displays switch replace success message.

Back up and restore the fabric configuration

You can save the current fabric configuration in a repository, and restore the data using a backup file when an error or failure occurs.

Using the **Fabric backup and restore** tab, you can:

- Set a local or remote repository.
- Back up the configuration of a select fabric in the OMNI VM.
- Download the backup files to the local system.
- Delete the downloaded backup from the OMNI VM.
- Upload or import the fabric backup file from the local or remote repository to the OMNI VM.
- Restore the fabric from a backup file.

NOTE: The fabric backup and restore features are supported from the OS10.5.0.7 version. If the OS10 software version is less than 10.5.0.7, the system displays a message that backup is not supported for the software version and disables all the backup and restore functions.

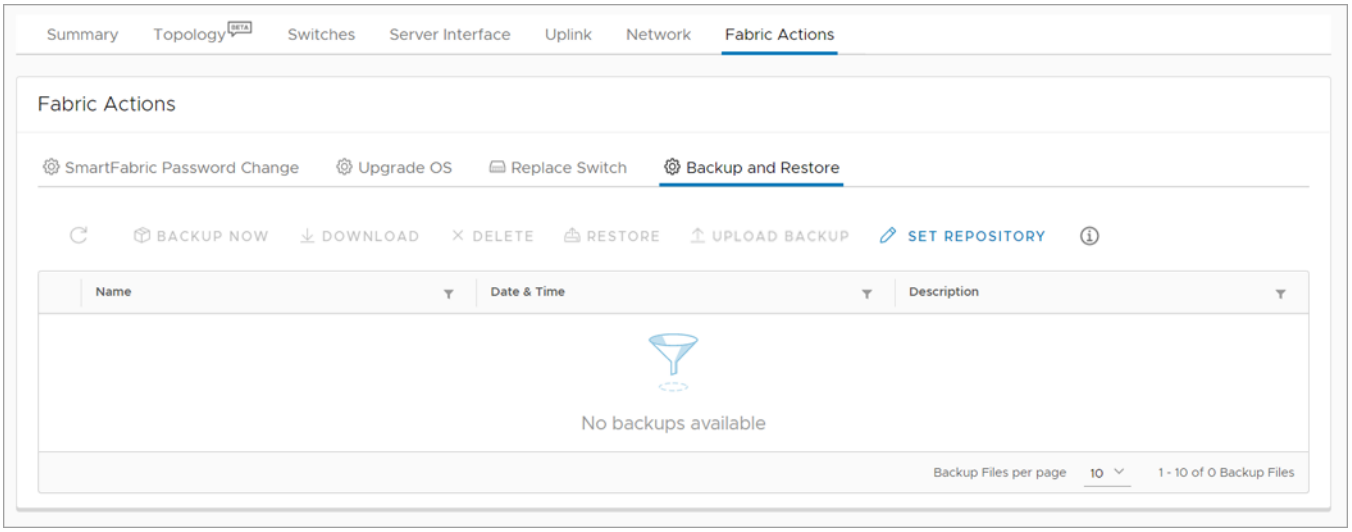
Set Repository

To backup the configuration, set up a local repository on the OMNI VM or a remote repository to store the backup files. OMNI supports File Transfer Protocol (FTP) and Secure Copy protocol (SCP) to transfer the backup files to a remote repository.

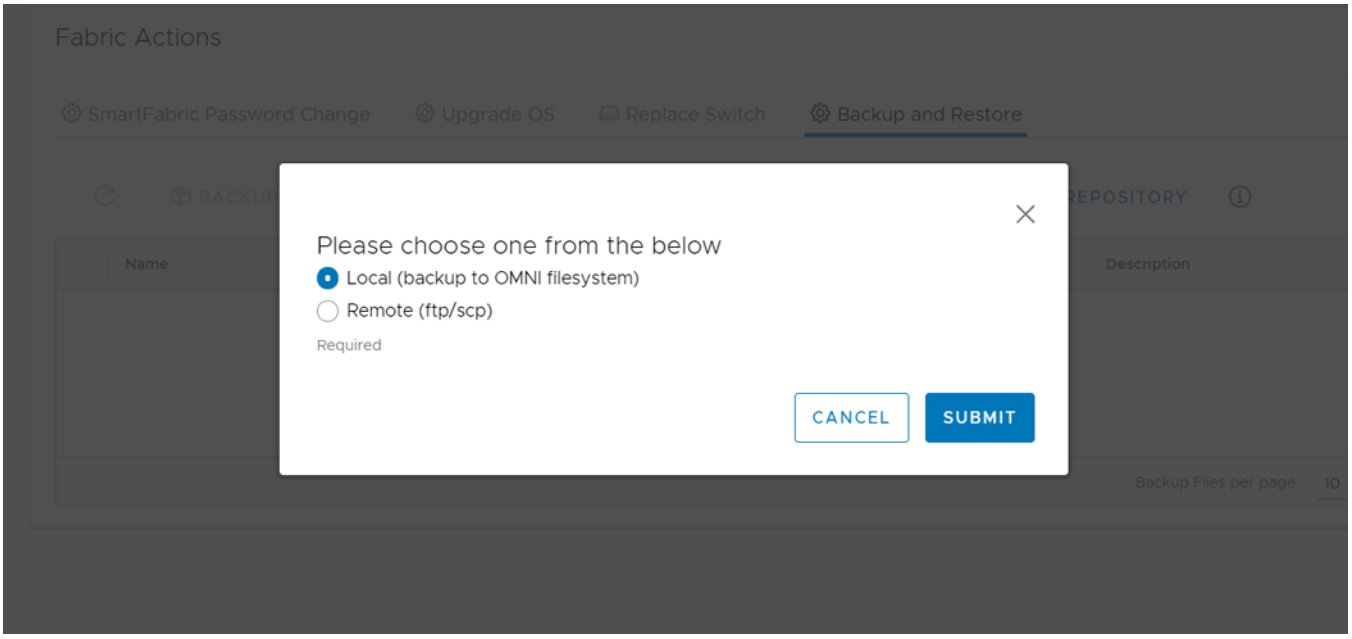
NOTE: You can either set a local or a remote repository at a time. To change the backup repository, edit the repository setting accordingly.

Set a local repository

1. Select the **Service Instance** > **Fabric Actions** > **Backup and Restore**.
2. From **Backup and Restore** tab, click **Set Repository**.



3. Select **Local**, and click **Submit**.

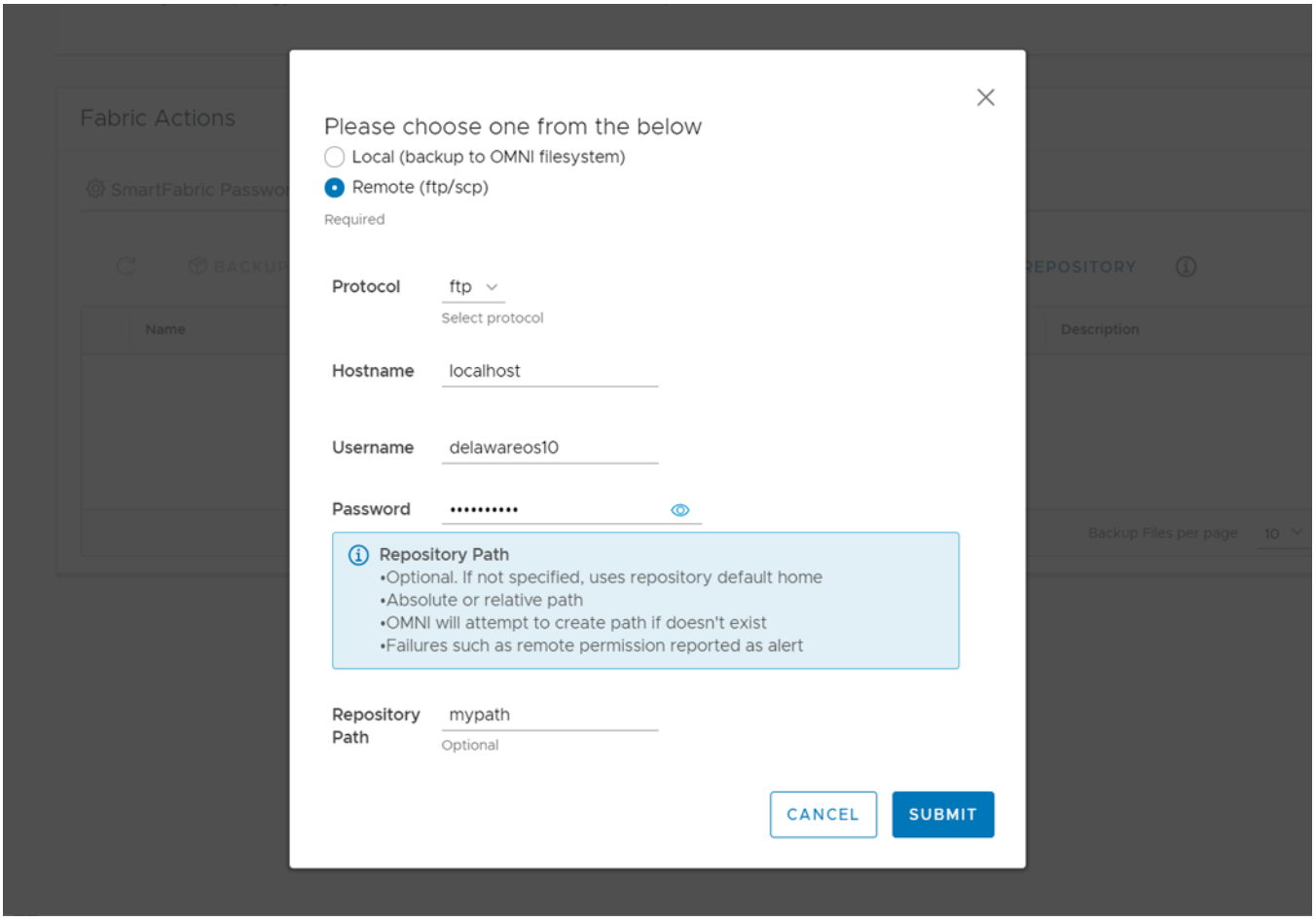


4. The system displays local repository configuration success message.

Set a remote repository

1. From **Backup and Restore** tab, click **Set Repository**.
2. Select **Remote**.
3. Select the protocol (SCP or FTP) from the list. Enter the **Hostname**, **Username**, and **Password** details.

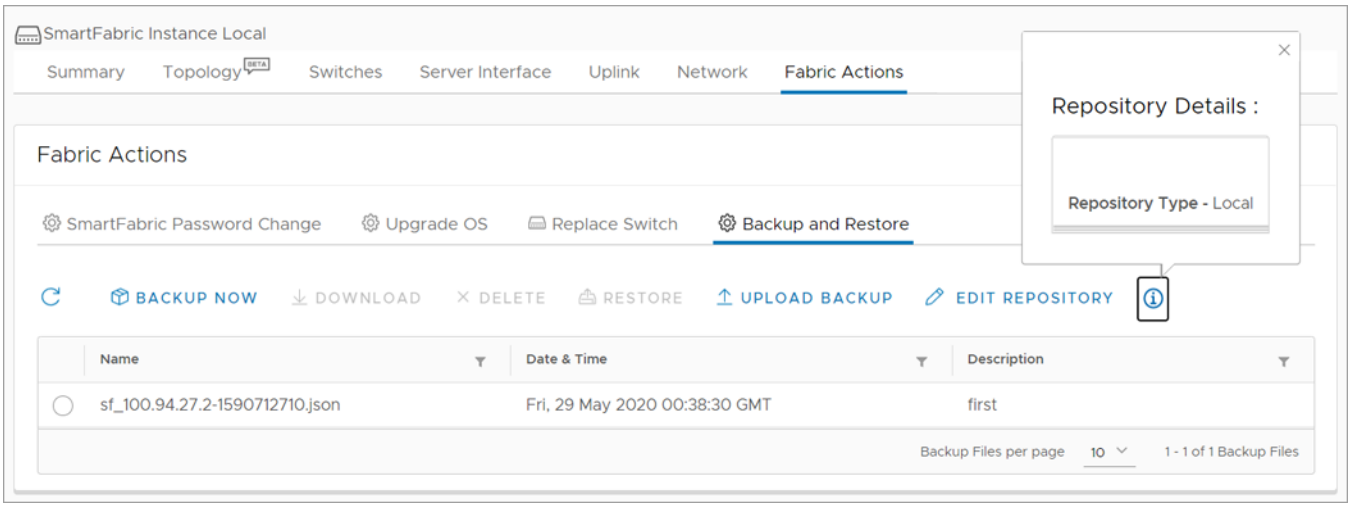
   (Optional) Enter the **Repository Path** details, and click **Submit**.



4. The system displays remote repository configuration success message.

View repository

View the repository details by clicking the information icon.



Edit repository

You can edit the repository type that is already set. To do so:

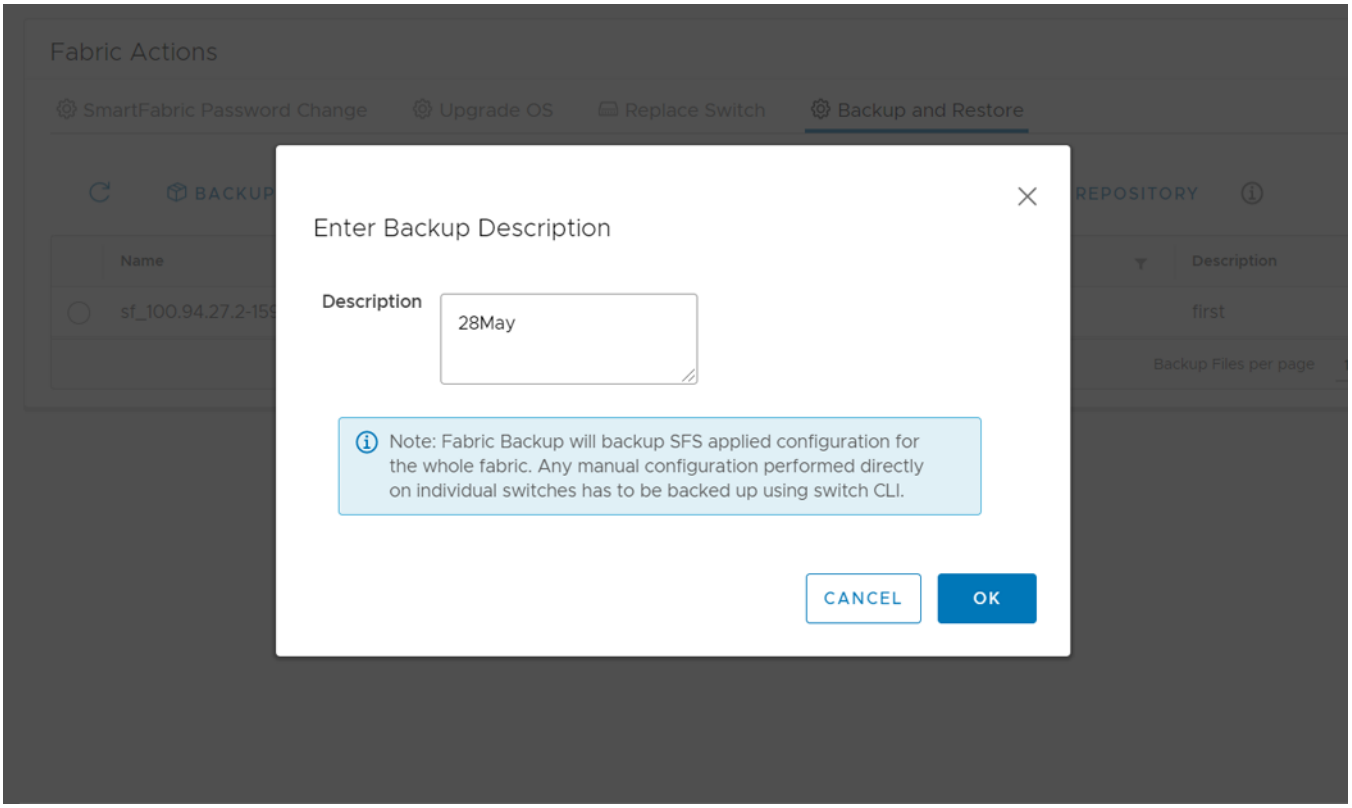
1. From **Backup and Restore** tab, click **Edit Repository**.
2. Edit the repository type, enter the required details if prompted, and click **Edit**.

   NOTE: When you edit the repository from local to remote, the backup files from the local OMNI VM are transferred to the remote repository. If you change the repository from remote to local, they backup files are not transferred to local OMNI VM.

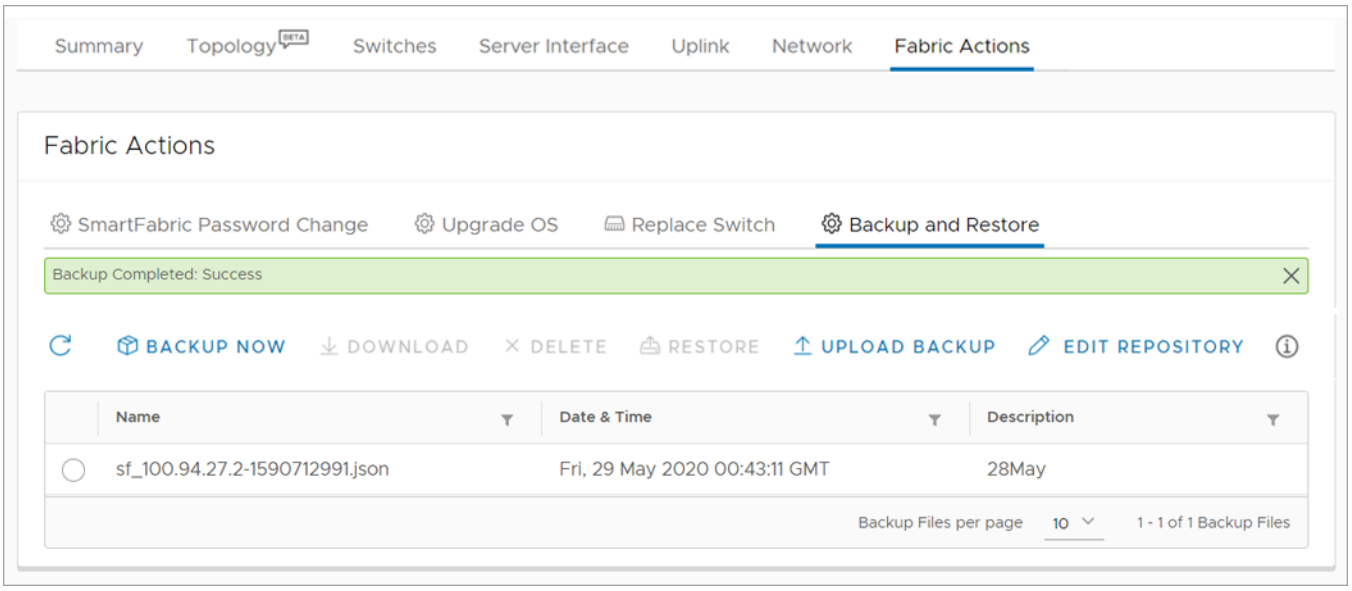
Backup fabric configuration

To backup the fabric configuration:

1. Select **Fabric Actions** > **Backup and Restore**, and click **Backup Now**.



2. Enter the description for the backup file and click **Ok**.



The backup file is stored as a JSON file with the date and time with the GMT timestamp.

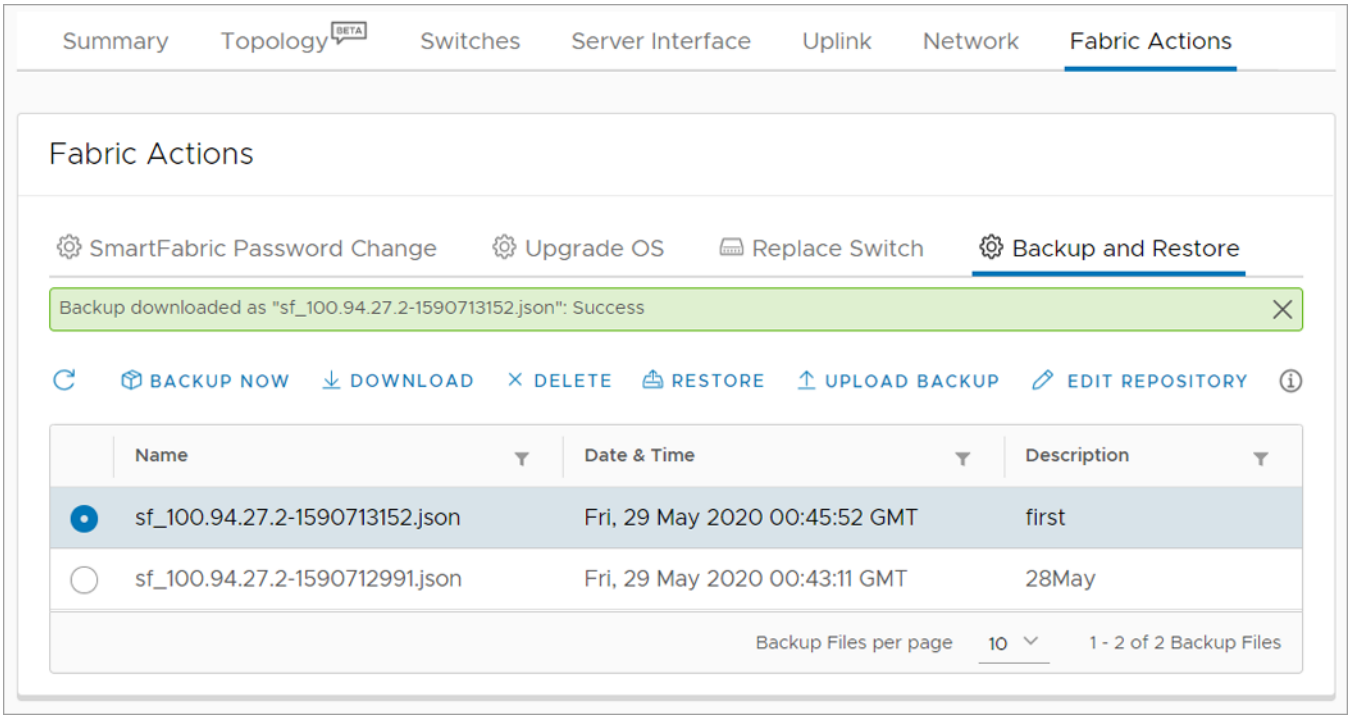
NOTE: The backup action stores SFS-applied configuration for the whole fabric. Any OS10 system configuration that is done on the individual switches directly has to be backed up using the OS10 CLI. For more information about how to backup the configuration, see *Dell EMC SmartFabric OS10 User Guide*.

3. The system displays backup completed success message.

Download backup

You can download a backup file from the OMNI VM to the local system.

1. Select **Backup and Restore** tab, and select the backup JSON file that you wanted to download from the list.
2. Click **Download**.

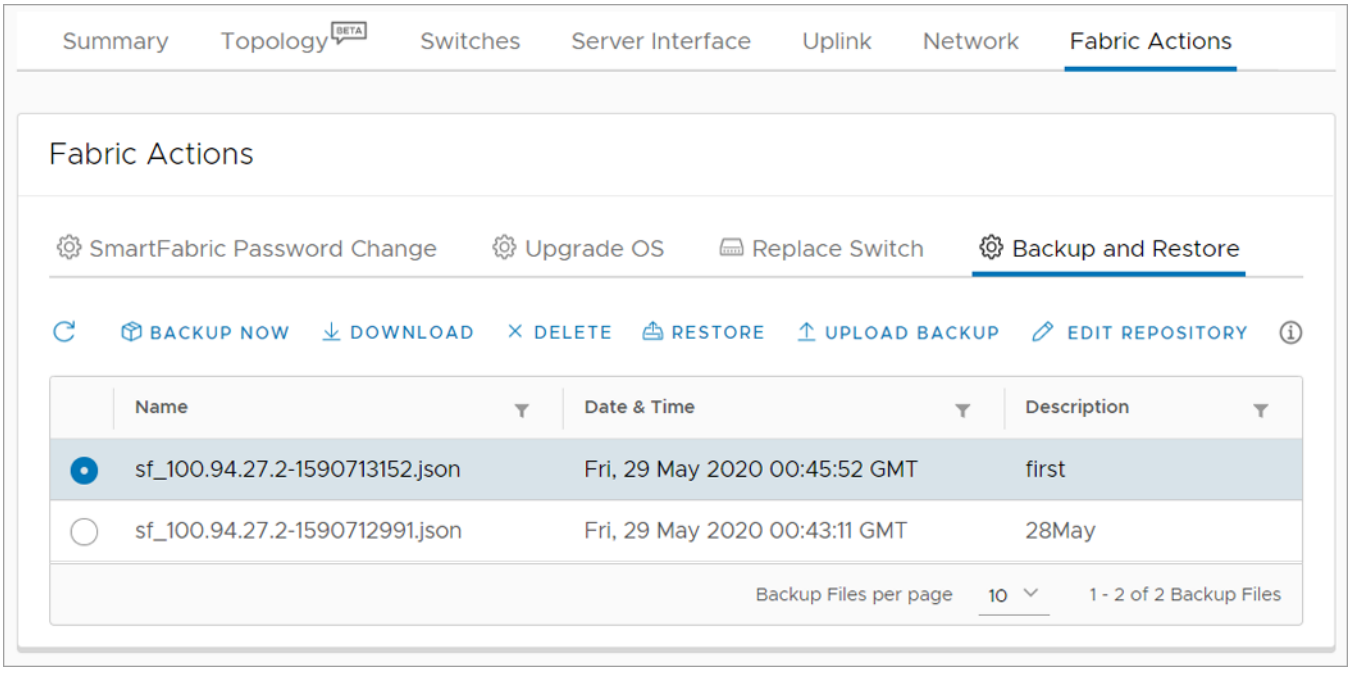


The file is downloaded locally with the backup download success message.

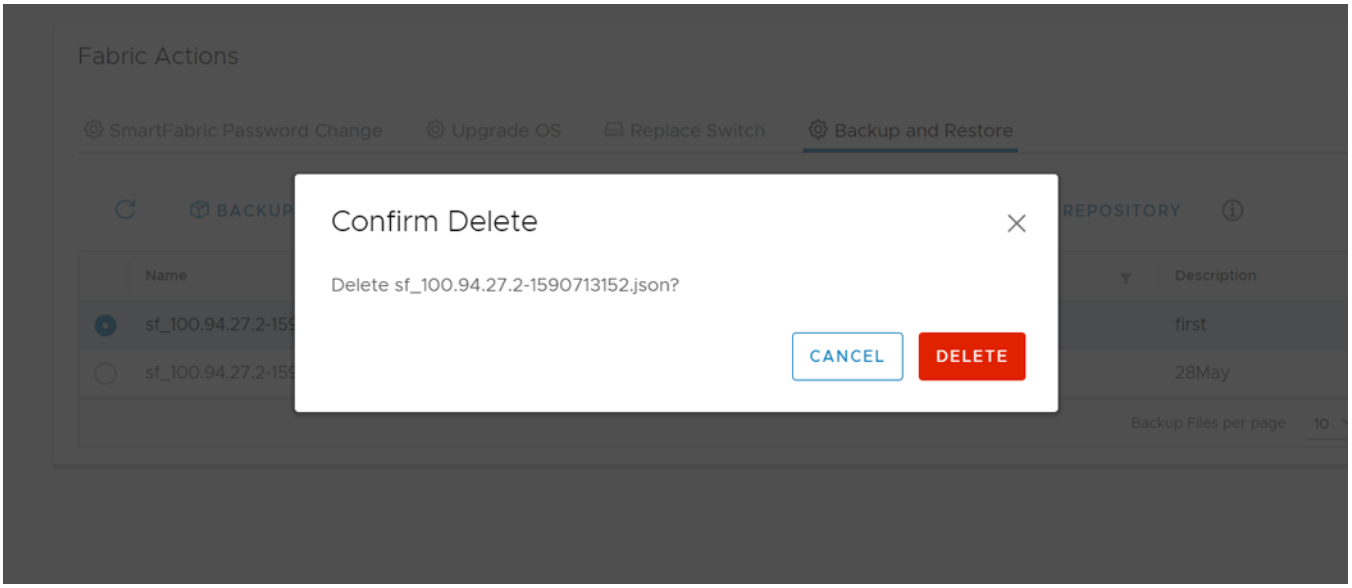
Delete backup

You can delete a backup file from the OMNI VM.

1. Select **Backup and Restore** tab.
2. Select the backup file that you want to delete from the displayed list, and click **Delete**.



3. Click **Delete** to confirm.

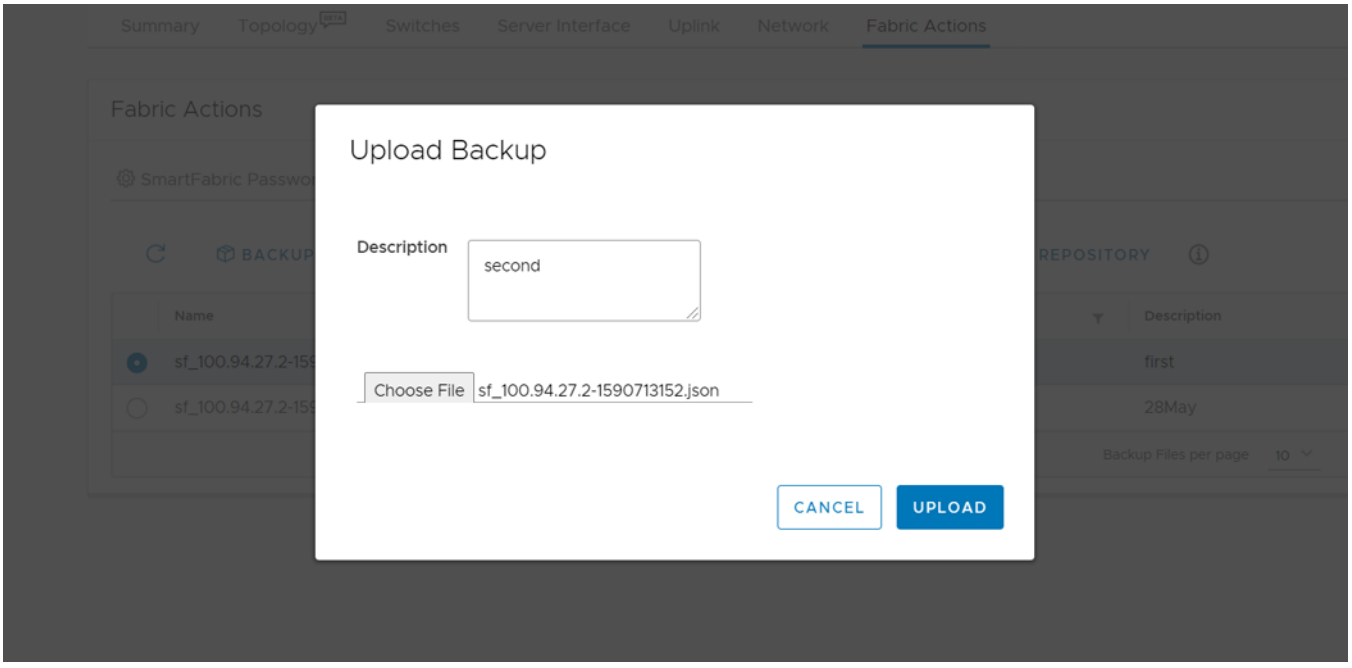


4. The system displays backup deleted success message.

Upload backup

You can upload a backup file from the local system to the OMNI VM.

1. From **Backup and Restore** tab, click **Upload Backup**.
2. Enter the description and choose the file that you want to upload, and click **Upload**.



3. The system displays upload file success message.

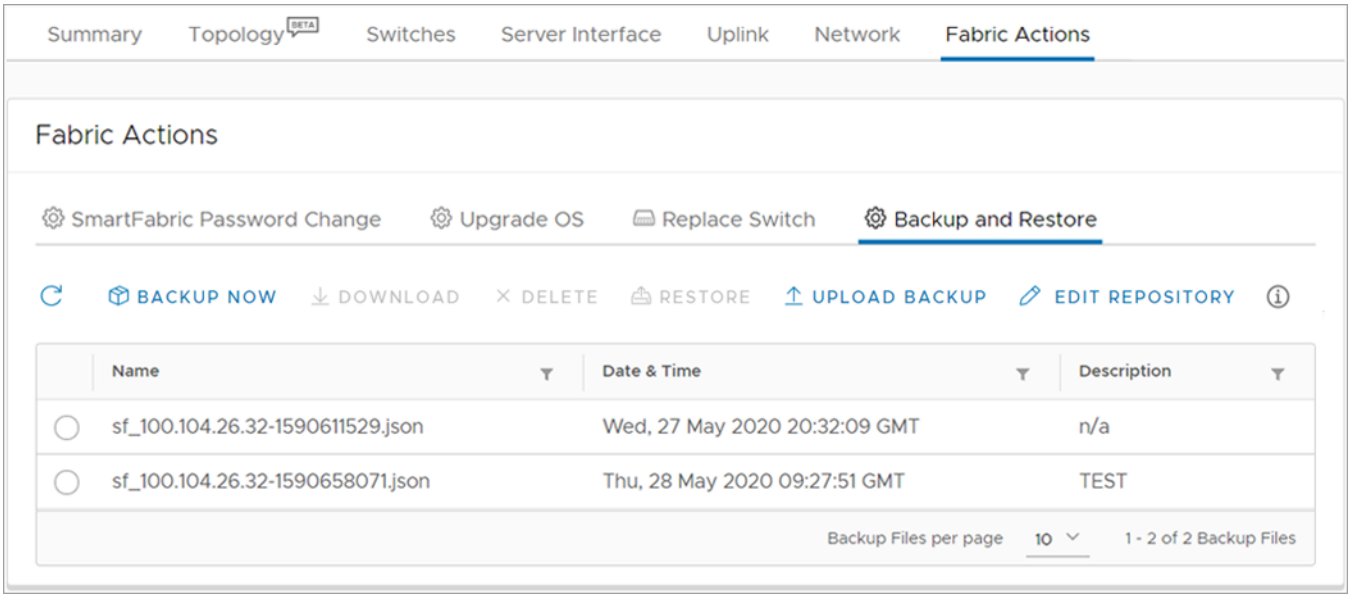
NOTE: OMNI displays error if the uploaded file is not in the JSON format.

Restore from a backup file

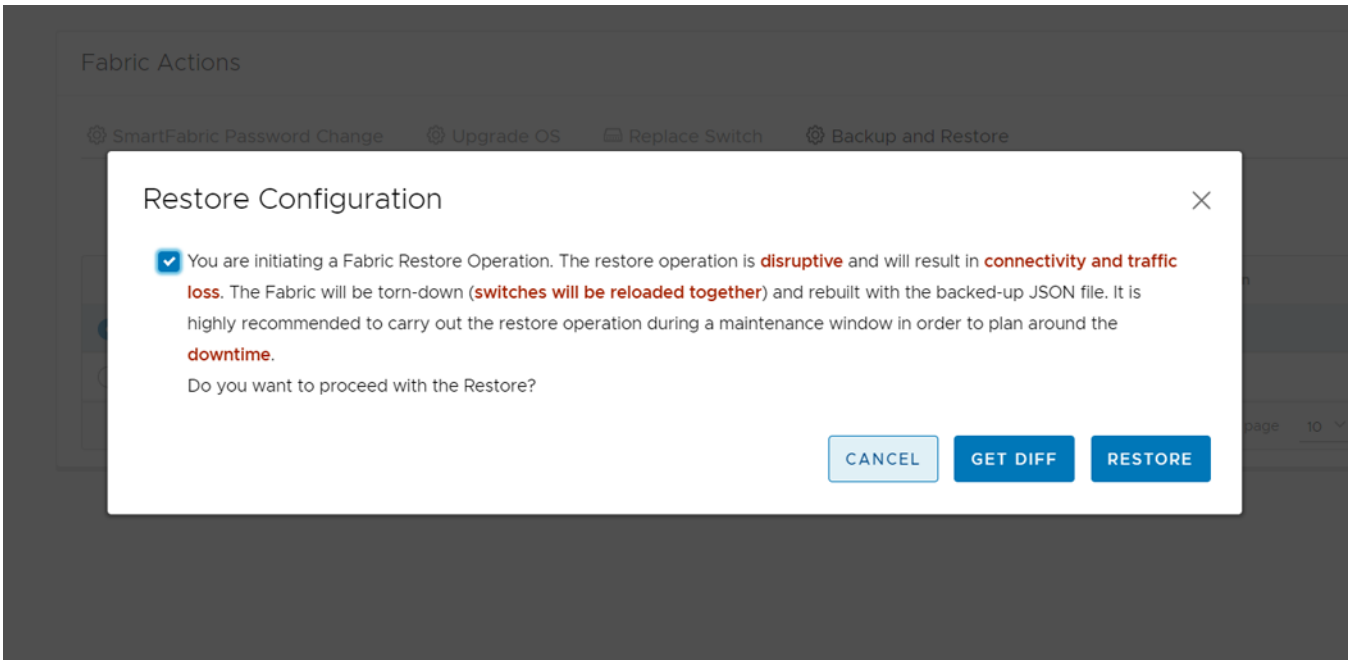
You can restore the configuration running on the SmartFabric using a backup file during unexpected error situation or disaster.

CAUTION: Restore action is disruptive and cause connection downtime and traffic loss. The restore action erases all fabric configuration and restarts the entire fabric with the configuration in the backup file. It is highly recommended to use the restore action during a maintenance window.

1. Select **Fabric Actions** > **Backup and Restore**.

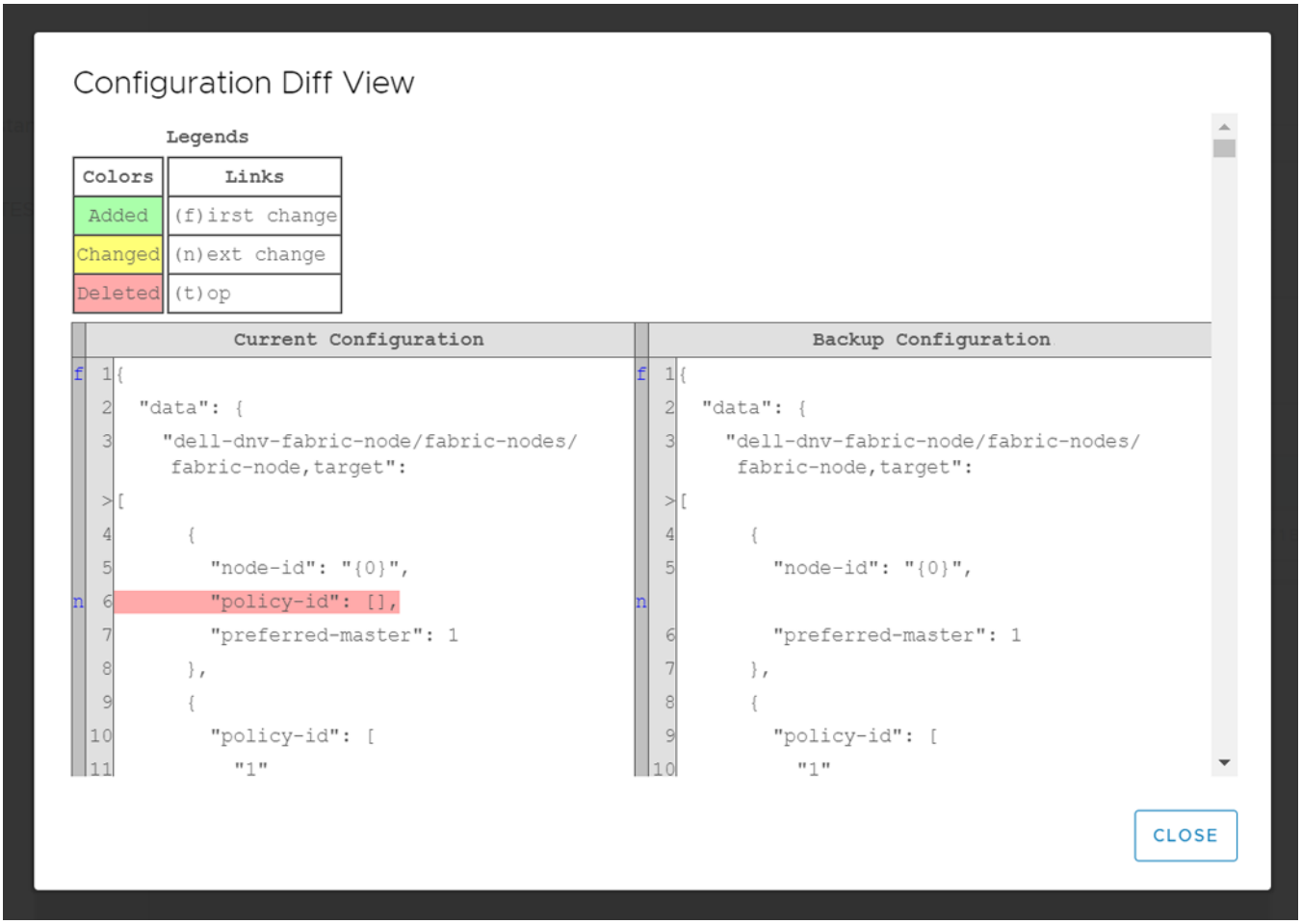


2. Select the backup file from which you want to restore the configuration, and click **Restore**.



NOTE: The restore action reboots all the switches with the applied fabric settings. Any manual configuration that are performed directly on individual switches has to be restored manually using the OS10 CLI. For more information about how to restore the configuration, see *Dell EMC SmartFabric OS10 User Guide*.

3. (Optional) Click **Get Diff** to compare the current configuration with the configuration in the backup file. **Configuration Diff View** displays the detailed comparison between the current and backup configuration.



4. To proceed with the restore action, select the checkbox to confirm, and click **Restore**.

   Once you initiate the restore process, OMNI appliance changes the service instance state to Maintenance mode automatically, which stops all the fabric automation services specific to the service instance.

5. The system displays the restore success message.

   When the fabric restore is complete, change the Maintenance mode of the service instance to **In Service**. For more information about Maintenance mode, see OMNI Maintenance mode. Start the automation services of the specific service instance manually from the OMNI Appliance Management UI. For more information about the OMNI Appliance Management UI, see OMNI Appliance Management User Interface.

6. For internal vCenter environment, restart the vCenter manually from the Platform Service Controller page. For more information about restarting the vCenter, see *VMware vSphere Documentation*.

9

Troubleshooting

Use the following information to troubleshoot the SmartFabric vCenter OMNI appliance connectivity, SmartFabric errors, and UI population errors.

OMNI appliance connectivity

Verify the IP address, DNS settings, and connection status.

1. From the OMNI management menu, select **2. Interface Configuration Menu**.

```
################################################################################
    Welcome to Dell EMC OpenManage Network Integration (OMNI) management
################################################################################

    Menu
    --------------------------------------------------
0.  Full setup
1.  Show version
2.  Interface configuration menu
3.  OMNI management service menu
4.  Register/Update OMNI vSphere client plugin with vCenter
5.  Password/SSL configuration menu
6.  Upgrade appliance
7.  Reboot appliance
8.  Show EULA
9.  Logout

Enter selection [0 - 9]: 2
```

2. Enter the selection as **1. Show Interfaces** and press **Enter**.

```
    --------------------------------------------------
    OMNI interface configuration menu
    --------------------------------------------------
1.  Show interfaces
2.  Show connection status
3.  Configure interfaces
4.  Show NTP status
5.  Configure NTP server
6.  Unconfigure NTP Server
7.  Start NTP Server
8.  Stop NTP Server
9.  Exit

Enter selection [1 - 9]: 1
```

```
Enter selection [1 - 9]: 1
sudo: unable to resolve host OMNI-1.3.14: Name or service not known
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:05:1a:45:da  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 100.104.26.22  netmask 255.255.255.0  broadcast 100.104.26.255
        inet6 fe80::250:56ff:fe85:abb7  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:85:ab:b7  txqueuelen 1000  (Ethernet)
        RX packets 695002  bytes 159086623 (151.7 MiB)
        RX errors 0  dropped 54  overruns 0  frame 0
        TX packets 157180  bytes 144654105 (137.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:50:56:85:93:cd  txqueuelen 1000  (Ethernet)
        RX packets 463229  bytes 46227842 (44.0 MiB)
        RX errors 0  dropped 52  overruns 0  frame 0
        TX packets 65686  bytes 11664357 (11.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 624296  bytes 90090468 (85.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 624296  bytes 90090468 (85.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(END)
```

3. Select **2. Show Connection Status**.

```
                ------------------------------------------------
                OMNI interface configuration menu
                ------------------------------------------------
            1.  Show interfaces
            2.  Show connection status
            3.  Configure interfaces
            4.  Show NTP status
            5.  Configure NTP server
            6.  Unconfigure NTP Server
            7.  Start NTP Server
            8.  Stop NTP Server
            9.  Exit

            Enter selection [1 - 9]: 2
            DEVICE   TYPE      STATE      CONNECTION
            ens160   ethernet  connected  Vcenter server network
            docker0  bridge    connected  docker0
            ens192   ethernet  connected  Vxrail Mgmt network
            lo       loopback  unmanaged  --
            press [enter] to continue...
```

Unable to register service instance in OMNI

Unable to register the service instances in OMNI, when:

1. SmartFabric is not reachable. To check the SFS connectivity:
   a. Log in as root user through the OMNI appliance console.
   b. Check the connectivity of the service instance using the `ping` command. Use IPv4, hostname, or IPv6 address of the service instance.

      ```
      :~$ ping 100.104.22.22
      :~$ping6 <fully qualified domain name>
      ```

   c. If ping fails, check if the OMNI interfaces are configured properly. If OMNI is internal, ensure that the VxRail Management network is configured.
   d. If OMNI is external, ensure that OMNI appliance is configured with the correct port-group that provides connectivity to SFS.
2. If SFS is reachable, but not able to register service instance.
   a. If the master node of the SFS has changed, the IP address of the SFS can also change.

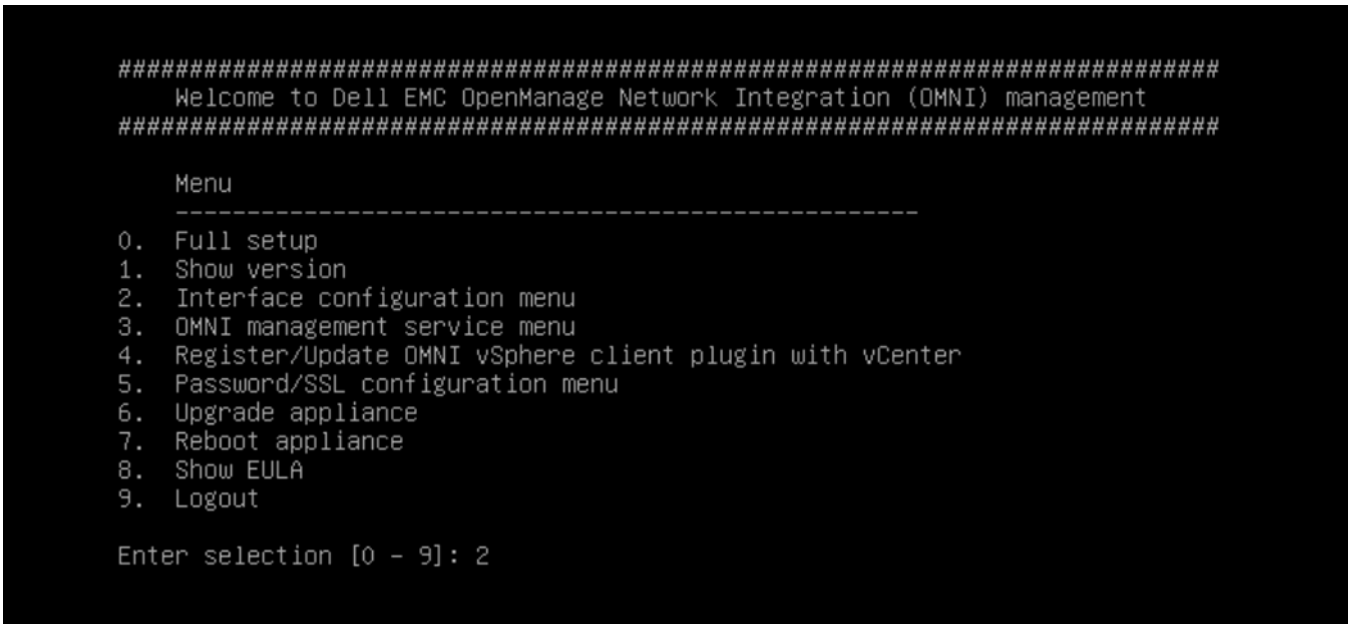
      NOTE: This scenario is not applicable if the OMNI appliance is inbound.
   b. Identify the master node using the OS10 CLI command. For more information about the command, see Add service instance.
   c. Register with the identified IP address.

OMNI appliance is not synchronized

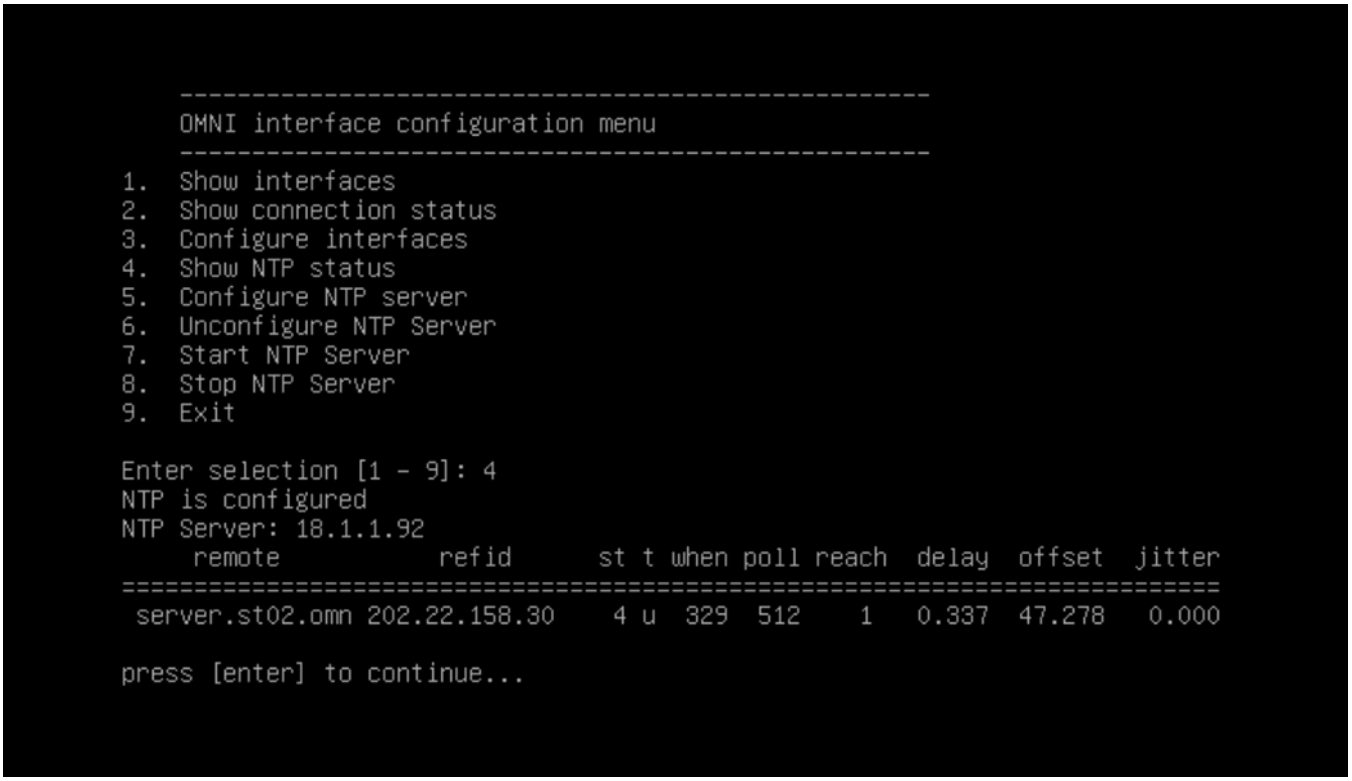
If the NTP server is not configured, the OMNI appliance VM does not synchronize with the data center.

Check the NTP server status in the OMNI appliance.

1. From the OMNI management menu, select **2. Interface Configuration Menu**.



2. Select **4. Show NTP Status**.



3. If the NTP server is not configured, select **5. Configure NTP Server**, and enter the valid NTP Server IP address or hostname.

UI is not populated

NOTE: Any IP address or SSL certificate changes on the VM, OMNI automation services can be restarted by changing the status of the service instance to Maintenance mode and then In Service mode. For more information about Maintenance mode, see OMNI Maintenance mode.

Check the service status on the plug-in VM.

1. From the OMNI management menu, enter the selection as **3. OMNI management service menu**.
2. Select **4. Restart OMNI management service** to restart all the database and web essential services.
   NOTE: To restart the automation services, go to OMNI Appliance Management UI and restart the services.
3. Select **2. View OMNI management service status** to view the list of registered vCenter managed by the OMNI VM. Confirm that all services are active.

```
    ------------------------------------------------
    OMNI management service menu
    ------------------------------------------------
1.  Start OMNI management service
2.  View OMNI management service status
3.  Stop OMNI management service
4.  Restart OMNI management service
5.  Create support bundle
6.  Change application log-level
7.  Exit

Enter selection [1 - 7]: 2
    Name                  Command               State   Ports
------------------------------------------------------------
omni_api        /usr/local/bin/gunicorn -w ...   Up
omni_db         docker-entrypoint.sh postgres    Up
omni_nginx      nginx -g daemon off;             Up
omni_services   /usr/local/bin/gunicorn -w ...   Up
2020-05-27 06:10:56,998 OMNI is registered with 100.104.26.21 vCenter host
2020-05-27 06:10:57,002 OMNI is registered with 100.104.26.32 controller
press [enter] to continue...
-
```

NOTE: **View OMNI management service status** is recommended for status validation and debugging purpose. Hence, the output does not show the port numbers.

4. If the problem still persists, try to unregister and register OMNI appliance with vCenter again.

Create support bundle

Download the support bundle from the OMNI Appliance Management UI. If you cannot access the UI, use to OMNI console to download the support bundle.

1. From the OMNI management menu, enter the selection as **3. OMNI Management Service Menu**.
2. Select **5. Create Support Bundle** to create a support bundle at /tmp/support-bundle.tar.gz on the OMNI VM.

```
    ------------------------------------------------
    OMNI management service menu
    ------------------------------------------------
1.  Start OMNI management service
2.  View OMNI management service status
3.  Stop OMNI management service
4.  Restart OMNI management service
5.  Create support bundle
6.  Change application log-level
7.  Exit

Enter selection [1 - 7]: 5
2020-05-27 06:00:20 INFO  [setup.sh] Creating support bundle..
2020-05-27 06:00:20 INFO  [setup.sh] OMNI appliance version ..........(1.3.14)
2020-05-27 06:00:20 INFO  [setup.sh] OMNI vSphere client plugin
version ............(1.3.14)
sudo: unable to resolve host OMNI-1.3.14: Name or service not known
sudo: unable to resolve host OMNI-1.3.14: Name or service not known
2020-05-27 06:00:20 INFO  [setup.sh] Support bundle creation successful
2020-05-27 06:00:20 INFO  [setup.sh] Support bundle available for SCP at
/tmp/support-bundle.tar.gz
press [enter] to continue...
-
```

NOTE: The recommendation is to set the log level to DEBUG before creating the support bundle.

3. From an external host, scp using `admin` credentials to transfer the support bundle file out. SCP credentials for the OMNI appliance are the same as the OMNI appliance console password. By default, `admin` is used for the username and password.

Change log level

NOTE: Use OMNI Appliance Management UI to change the log level of each service. For more information about changing log-level using UI, see OMNI Appliance Management UI.

1. From the OMNI management menu, enter the selection as **3. OMNI Management Service Menu**.
2. Select **6. Change Application Log Level** to display the current log-level and switch accordingly.

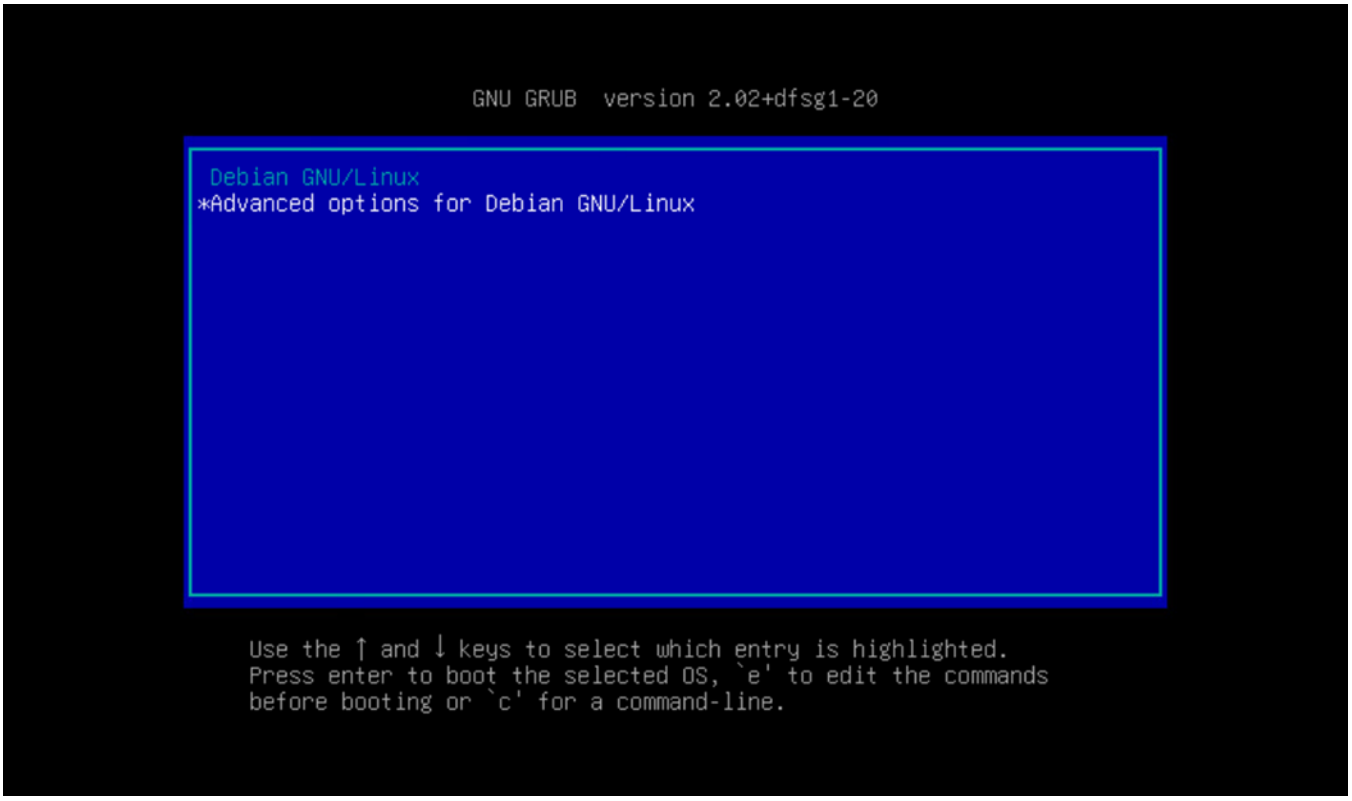
```
    ------------------------------------------------
    OMNI management service menu
    ------------------------------------------------
1.  Start OMNI management service
2.  View OMNI management service status
3.  Stop OMNI management service
4.  Restart OMNI management service
5.  Create support bundle
6.  Change application log-level
7.  Exit

Enter selection [1 - 7]: 6
2020-05-27 05:51:43 INFO  [vc-extension.sh] omni_api Log Level.
2020-05-27 05:51:46,945 Current application log-level: ERROR
2020-05-27 05:51:47 INFO  [vc-extension.sh] omni_services Log Level.
2020-05-27 05:51:48,293 Current application log-level: ERROR

Existing log-level will be toggled from (DEBUG<->ERROR), do you want to Proceed? [y]? y
2020-05-27 05:52:01 INFO  [vc-extension.sh] omni_api Log Level toggle.
2020-05-27 05:52:02,428 Changing application log-level to: DEBUG
2020-05-27 05:52:02 INFO  [vc-extension.sh] omni_services Log Level toggel.
2020-05-27 05:52:03,983 Changing application log-level to: DEBUG
2020-05-27 05:52:04 INFO  [setup.sh] log-level change successful
press [enter] to continue...
_
```

NOTE: By default, the log-level in OMNI appliance is set to ERROR. The appliance log can be swapped between ERROR to DEBUG.

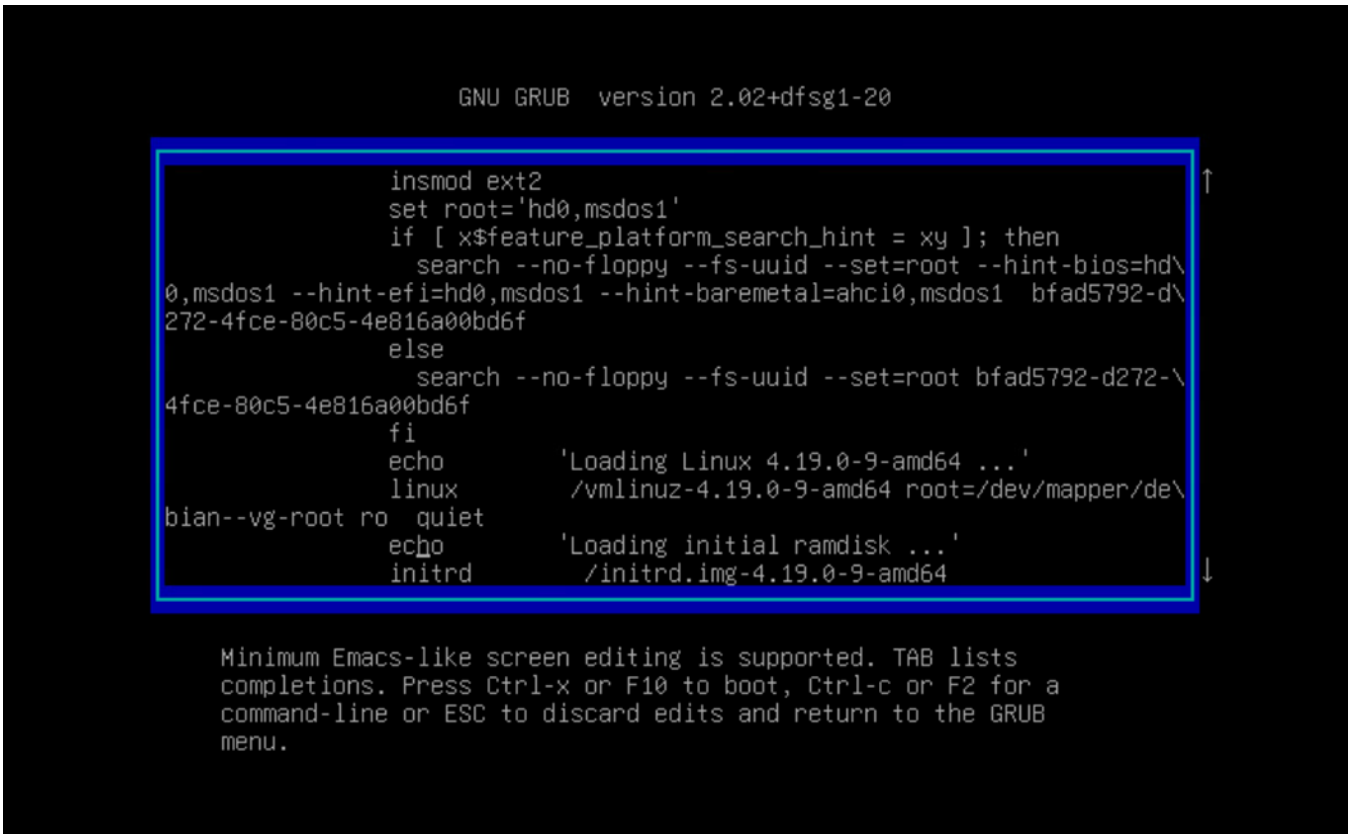
3. Stop if the log level is already on the wanted log level.

Reset OMNI VM password

1. Reboot the VM from vCenter, then select **Advanced Options for Debian GNU/Linux**.

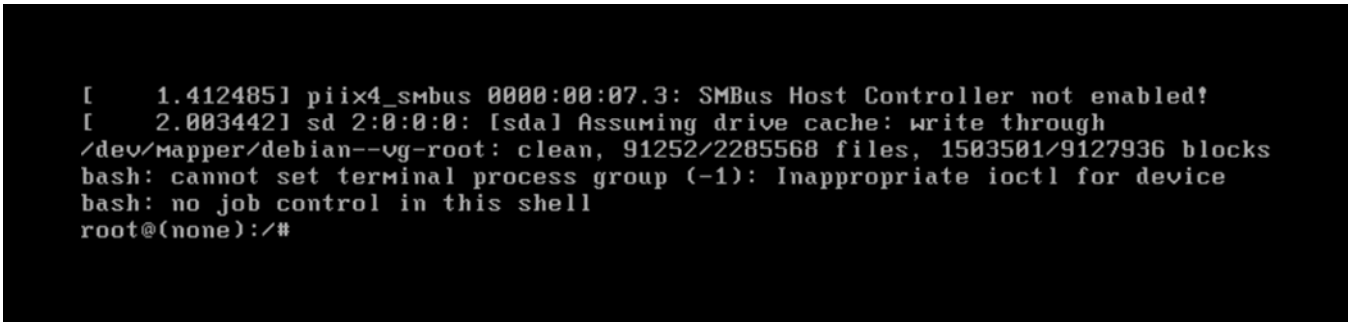


2. Use the arrow keys to go to the line starting with `linux` and ending with `ro quiet`.



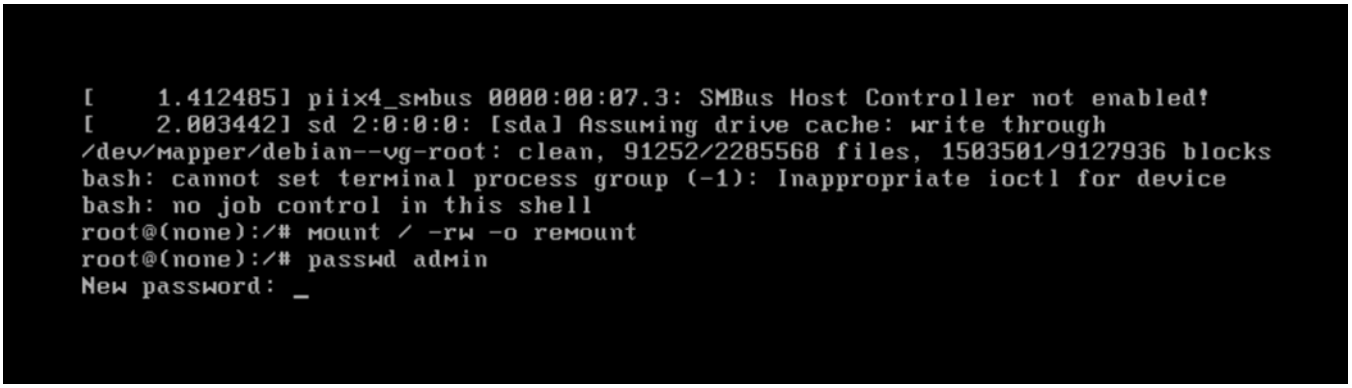
3. Append `init=bin/bash` after `ro quiet`.

4. Press **Ctrl-X** to boot into the shell with root access.

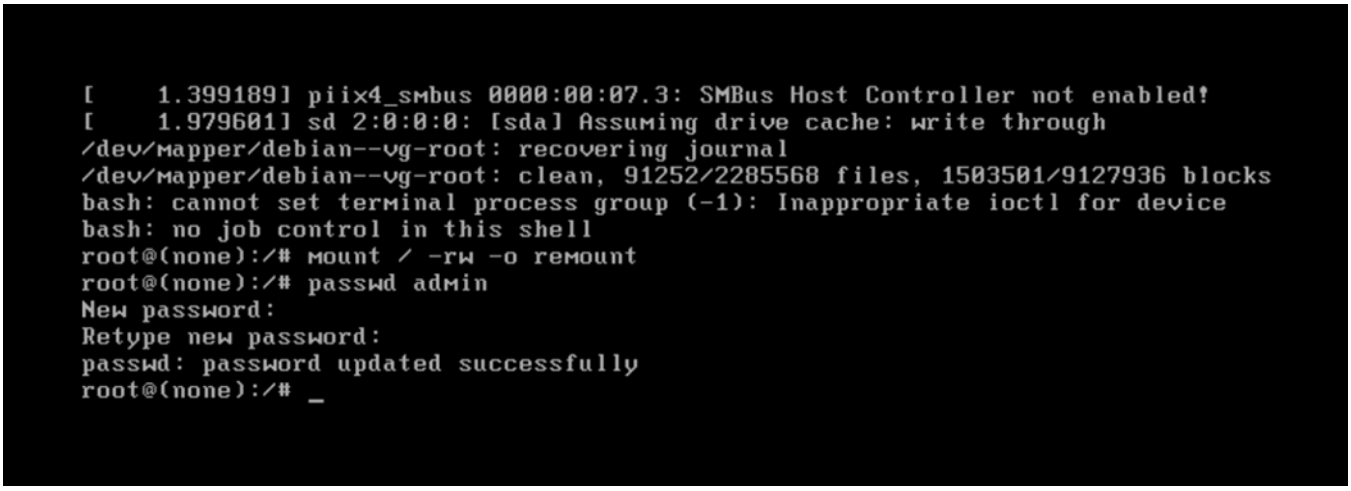


5. Remount the directory.

```
# mount / -rw -o remount
```



6. Change the password for admin using `passwd admin`. Enter the new password and confirm the password.



7. Reset the VM from vCenter and log in through the new password for the OMNI VM.

Missing networks on server interfaces

If OMNI fails to create and associate the appropriate network on a server interface during automation, OMNI automation services can be restarted so that OMNI reconfigures the networks. OMNI automation services can be restarted by changing the status of the service instance to Maintenance mode, then changing the instance to In Service mode. For more information about Maintenance mode, see OMNI Maintenance mode.

OMNI unable to resolve vCenter FQDN

A change in the DNS can cause an issue during FQDN resolution. If there is any change in DNS, set the proper DNS for the interface through option **2. Interface configuration Menu**. For complete information, see *Network interface profile configuration* in OpenManage Network Integration.

Certificate not trusted error

If OMNI is having issues communicating with the vCenter due to SSL certificate errors, new SSL certificates must be installed.

1. To install new SSL certificates, see Generate and Install SSL certificates.
2. OMNI automation services can be restarted by changing the status of the service instance to Maintenance mode, then changing the instance to In Service mode. For more information about Maintenance mode, see OMNI Maintenance mode.