Dell EMC SmartFabric Director

User Guide Release 2.0

November 2020
Rev. A03

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.

© 2019 - 2020 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

1

Revision history

This table provides an overview of the changes in this guide.

Table 1. Revision history

Release	Revision	Description
2.0.0	A03 (November 2020)	• Getting started — Added new section on supported and tested scale limits • Backup and restore — Added new section on how to create and restore backups • Upgrade SFD — Updated how to upgrade SFD • Notifications, events, alerts, and activities — Updated notifications, events, alerts, and activities • Fabric intent configuration — Updated L3 BGP leaf spine fabric and L3 BGP EVPN leaf spine fabric with VxLAN; added L3 BGP leaf spine with NSX-T overlay fabric • SwitchOS support matrix — Added new section on how to download new SmartFabric OS10 images and upload the images to SFD
1.2.0	A02 (May 2020)	• Installation using vCenter 6.7 — Updated information on service tag input • Specify system settings — Added new section to upload the service tag • Create user accounts — Updated screenshots for user management • Define fabric intent — Added BFD to Layer 3 configuration
1.1.1	A01 (March 2020)	• Define switch lifecycle job — Enter a user-specified OS10 image name • Upgrade SFD — Upgrade SFD software
1.1.0	A00 (January 2020)	Initial release

2

SmartFabric Director

Dell EMC SmartFabric Director (SFD) enables data center operators to build, operate, and monitor an open network underlay fabric. SFD works with Dell EMC PowerSwitch Series switches to ensure that their physical underlay networks are tuned for the specific overlay environment.

SFD enables the physical switch underlay infrastructure to keep pace with the changing demands of virtualized and software-defined networks, and provides customers a single view for operating, managing, and troubleshooting of physical and virtual networks.

Features

- Abstracted view of the fabric — no need to manage individual switches
- Define, build, and maintain a Layer 2 or Layer 3 leaf spine data center fabric (underlay and EVPN overlay)
- Intent template-based provisioning underlay
- Authoritative repository of intent and switch configuration and state
- Fabric health management and monitoring including events, logs, alarms, states, and metrics (counters)
- Operator-driven remediation
- Full life-cycle management of switches including grouping of switches and scheduling of jobs
- Uses OpenConfig (gNMI, gNOI) for provisioning and streaming telemetry of switches

Inputs

- Provisioning using REST or gRPC/gNOI
- ONIE and gNOI life-cycle management
- Streaming telemetry using gRPC
- Agentless or Agent interface to switches
- L2 or L3 fabric topology

Streaming telemetry

Model-driven telemetry is a new approach for network monitoring. Data is streamed from network switches continuously, using a push model which provides near real-time access to operational statistics. Applications can subscribe to specific data items they need, by using standard-based YANG data models.

Streaming telemetry enables users to push data off the switch to an external collector at a higher frequency, more efficiently, and data on-change streaming.

Models

- *destination-group* tells the switch where to send telemetry data and how
- *sensor-group* identifies a list of YANG models that the switch should stream
- *subscription-profile* ties together the destination-group and the sensor-group

3

Getting started

This information describes the component and configuration requirements.

Dell EMC SmartFabric Director

- Dell EMC SmartFabric Director release 2.0.0

SmartFabric OS10

All PowerSwitches must be running these versions of Dell EMC SmartFabric OS10:

Release 2.0.0	10.5.2.0P1
Release 1.2.0	10.5.1.2
Release 1.1.2	10.5.0.4 or 10.5.0.5
Release 1.1.1	10.5.0.4 or 10.5.0.5
Release 1.1.0	10.5.0.4

Dell EMC PowerSwitches

- S4048-ON, S4048T-ON
- S4112F-ON, S4112T-ON
- S4128F-ON, S4128T-ON
- S4148F-ON, S4148FE-ON, S4148T-ON
- S4248FB-ON, S4248FBL-ON
- S5212F-ON
- S5224F-ON
- S5232F-ON
- S5248F-ON
- S5296F-ON
- S6010-ON
- Z9100-ON
- Z9264F-ON
- Z9332F-ON

Platforms supported for BGP EVPN intent

Table 2. Supported platforms for BGP EVPN intent

Spine	Z9100-ON, Z9264F-ON, Z9332F-ON, S5232F-ON
Leaf	S5212F-ON, S5224F-ON, S5248F-ON, S5296F-ON, S4112F-ON, S4112T-ON, S4128T-ON, S4128F-ON, S4148T-ON, S4148FE-ON, S4148F-ON

VMware requirements

VMware ESXI

- Virtualization-ready x86 server
- VMware ESXi 7.0b U1, U2 (recommended); ESXi 6.5, U1, U2, U3
- VMware vSphere Enterprise Plus license
- Virtual appliance (OVA)
- 4vCPU
- 16G memory
- 100G available disk space (higher disk sizes may be required depending on fabric size and data retention requirements)

VMware NSX-T

See docs.vmware.com/VMware NSX-T Data Center for complete NSX-T requirements.

More requirements

- Web browser — Chrome (version 72.0.3626.121 and later) and Firefox (version 68.0 and later) recommended
- vSphere web client 6.5 U1, U2, U3 — supported for Flash client; not supported for HTML5 client
- vSphere web client 7.0 (all versions) — nonsupported for Flash client; supported for HTML5 client
- Text or JSON editor to modify the JSON wiring diagram if required

Supported and tested scale limits

- Maximum number of switches in a fabric — 64
- Maximum number of spines in a fabric — 8
- Maximum number of leaf switches in a fabric — 60
- Maximum number of edge leaf switches — 2
- Maximum number of host-facing physical links — 3000
- Maximum number of VLANs — 512
- Maximum number of VNIs — 512
- Maximum number of tenants/VRFs — 1
- Maximum number of vCenter Servers — 1
- Maximum number of NSX-T Managers — 1
- Maximum number of DVS per vCenter — 3

4

Software installation

This information describes how to install SFD in your SmartFabric OS10 network. If your switch came preinstalled with Dell EMC SmartFabric OS10, see Log in to SmartFabric OS10.

NOTE: For detailed hardware installation steps, see the product-specific *Installation Guide* at www.dell.com/support/.

Topics:

Download SFD image

This information explains show to download the SmartFabric Director software image.

1. Sign into DDL using your account credentials.
2. Locate your entitlement ID and order number, then select the product name.
3. Select the **Products** tab and view your service tag that is located under Associated Hardware of Software ID; write the service tag down. The service tag is needed during first-time setup. The service tag is also visible in the license key.
4. Select the **Available Downloads** tab, select the wanted files to download, then click **Download**.
5. Read the Dell End-User License Agreement. Scroll to the end of the agreement, then click **Yes, I agree**.
6. Select how to download the software files, then click **Download Now**.
7. After you download the image, unpack the .tar file on a Linux or Windows server, then open the README file for instructions on how to validate the OVA file.

NOTE: The available downloads include the software image, release notes, user guide, and JSON wiring diagram template (see Fabric wiring diagram definition for complete information).

Log in to SmartFabric OS10

To log in to SmartFabric OS10, turn on the device and wait for the system to perform a power-on self-test (POST). Enter `admin` for both the default username and user password.

For better security, change the default `admin` password during the first SmartFabric OS10 login. The system saves the new password for future logins. After you change the password through the CLI, enter the `write memory` command to save the configuration.

```
OS10 login: admin
Password: admin
Last login: Sat Oct  6 00:25:33 UTC 2018 on ttyS0
Linux OS10 4.9.110 #1 SMP Debian 4.9.110-3+deb9u4 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.


-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
-*          Dell EMC  Network Operating System (OS10)            *-
-*                                                               *-
-* Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.     *-
-*                                                               *-
-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
```

```
This product is protected by U.S. and international copyright and
intellectual property laws. Dell EMC and the Dell EMC logo are
trademarks of Dell Inc. in the United States and/or other
jurisdictions. All other marks and names mentioned herein may be
trademarks of their respective companies.

OS10# configure terminal
OS10(config)# username admin password alpha404! role sysadmin
OS10(config)# exit
OS10# write memory
```

Check SmartFabric OS10 version

1. View the SmartFabric OS10 version in EXEC mode.

```
OS10# show version
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2020 by Dell Inc. All Rights Reserved.
OS Version: 10.5.2.0
Build Version: 10.5.2.0.228
Build Time: 2020-09-19T04:16:06+0000
System Type: MX9116N-ON
Architecture: x86_64
Up Time: 01:28:47
```

2. (Optional) If your switch is not preloaded with SmartFabric OS10 10.5.2.0, you must upgrade the operating system (see Upgrade SmartFabric OS10 in the *Dell EMC SmartFabric OS10 User Guide* at www.dell.com/support/).

5

Switch configuration

This information explains how to configure SmartFabric OS10 for SFD. For complete configuration information, see the *Dell EMC SmartFabric OS10 User Guide* at www.dell.com/support/.

Checklist

Gather these items before starting switch configuration from SmartFabric OS10 for SFD:

- Management interface IP address
- Host names to correspond with names used in the wiring diagram (JSON)
- JSON file (optionally exported from FDC)
- Interface breakouts
- Switch-port profile and port-group modes
- NTP server address
- Crypto security certificate

Topics:

Management interface

This information explains how to configure Management interface access to network devices. You can configure the Management interface, but the configuration options on this interface are limited. You cannot configure gateway addresses and IP addresses if it appears in the main routing table. Proxy ARP is not supported on this interface.

1. Configure the Management interface.

```
OS10(config)# interface mgmt 1/1/1
```

2. By default, DHCP client is enabled on the Management interface. Disable DHCP client operations.

```
OS10(conf-if-ma-1/1/1)# no ip address dhcp
```

3. Configure an IP address and mask on the Management interface.

```
OS10(conf-if-ma-1/1/1)# ip address A.B.C.D/prefix-length
```

4. Enable the Management interface.

```
OS10(conf-if-ma-1/1/1)# no shutdown
```

5. Exit CONFIGURATION mode.

```
OS10(conf-if-ma-1/1/1)# exit
```

6. Configure the default route for the Management interface.

```
OS10(config)# management route 0.0.0.0/0 gateway_ip_address
```

Configure Management interface

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# no ip address dhcp
OS10(conf-if-ma-1/1/1)# ip address 10.1.1.10/24
```

```
OS10(conf-if-ma-1/1/1)# no shutdown
OS10(conf-if-ma-1/1/1)# exit
OS10(config)# management route 10.10.20.0/24 10.1.1.1
```

For complete information about configuring Management interfaces, see the *Dell EMC SmartFabric OS10 User Guide* at www.dell.com/support/.

Crypto security

This information explains how to prepare your switch for SmartFabric Director from the OS10 side to install the crypto security profile and license.

The gNMI agent, available with SmartFabric OS10 release 10.5.2.0 and later, provides a new interface to configure OS10 devices. It uses gNMI protocol and OpenConfig YANG models to support create, read, update, and delete (CRUD) operations, life cycle management through gNOI and configuration of streaming telemetry.

The gNMI agent listens to SFD to receive remote configuration-change requests or upgrade and downgrade instructions. As a part of these remote configuration changes, the gNMI agent enables the telemetry agent to transmit preconfigured sensor group data in the OpenConfig format to SFD.

Setup crypto security

1. Log in to SmartFabric OS10, then verify that the installed software version meets the requirements.

```
OS10# show version
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2020 by Dell Inc. All Rights Reserved.
OS Version: 10.5.2.0
Build Version: 10.5.2.0.228
Build Time: 2020-09-19T04:16:06+0000
System Type: MX9116N-ON
Architecture: x86_64
Up Time: 01:28:47
```

2. Verify your switch operating mode in EXEC mode.

```
OS10# show switch-operating-mode

Switch-Operating-Mode : Full Switch Mode
```

3. Set up the crypto security profile and certificate, then replace `gnmi-os10-0` with a security-profile name of your choice. Format is `gnmi-xxx-0` where `xxx` is any string.

```
OS10# config t
OS10(config)# crypto security-profile gnmi-os10-0
OS10(conf-sec-profile)# certificate gnmi-os10-0
OS10(conf-sec-profile)# exit
```

4. Start `restconf` and set HTTPS session timeout value.

```
OS10(config)# rest api restconf
OS10(config)# rest https session timeout 60
```

5. Set up the `gnmi-security-profile`.

```
OS10(config)# gnmi-security-profile gnmi-os10-0
OS10(config)# exit
```

6. Create crypto certificate.

```
OS10# crypto cert generate self-signed cert-file home://gnmi-os10-0.crt key-file
home://gnmi-os10-0.key cname os10
Processing certificate ...
Successfully created certificate file and key
```

NOTE: The creation of the crypto certificate only needs to be done once. If the startup configuration is deleted, this step does not need to be repeated as certificates are retained.

7. Install the certificate.

```
OS10# crypto cert install cert-file home://gnmi-os10-0.crt key-file home://gnmi-
os10-0.key
Processing certificate ...
Certificate and keys were successfully installed as "gnmi-os10-0.crt" that may be
used in a security profile. CN = os10
```

8. Set the switch operating mode to SFD, then verify the mode.

```
OS10# switch-operating-mode sfd
OS10# show switch-operating-mode
Switch-Operating-Mode : SmartFabric Director Mode
OS10# show sfd status
Controller IP                           Port            Status
------------------------------------------------------------------------------
::ffff:100.94.25.246                    8443            active
```

9. Save the configuration.

```
OS10# write memory
```

10. SFD displays an informational message to reload the device for SFD mode to take effect; reload the switch.

```
OS10# reload
```

For complete information about crypto security profiles, see the *Dell EMC SmartFabric OS10 User Guide* at www.dell.com/support/.

Switch-port profiles

This information explains switch-port profiles. A port profile determines the enabled front-panel ports and supported breakout modes on Ethernet and unified ports. Change the port profile on a switch to customize uplink and unified port operation, and the availability of front-panel data ports.

NOTE: Port profiles are only applicable for the S4148-ON and S4148U-ON switches. You can skip to the next section if using these switches.

To change the port profile at the next reboot, use the `switch-port-profile` command with the wanted profile, save it to the startup configuration, then use the `reload` command to apply the changes.

1. Configure a platform-specific port profile. For a stand-alone switch, enter `1/1` for `node/unit`.

   NOTE: Switch-port profiles are platform-specific. If `switch-port-profile` is not available, the configuration is not available for your specific platform.

```
OS10(config)# switch-port-profile node/unit profile
```

2. Exit CONFIGURATION mode, then save the port profile change to the startup configuration.

```
OS10(config)# exit
OS10# write memory
```

3. Reload the switch.

```
OS10# reload
```

The switch reboots with the new port configuration and resets the system defaults, except for the switch-port profile and these configured settings:

- Management interface 1/1/1 configuration
- Management IPv4/IPv6 static routes
- System hostname
- Unified forwarding table (UFT) mode
- ECMP maximum paths

You must manually reconfigure other settings on the switch after you apply a new port profile and reload the switch.

NOTE: After you change the switch-port profile, do not immediately back up and restore the startup file. You must use the `write memory` command and reloading the switch using the `reload` command or the new profile does not take effect.

Configure port profile

```
OS10(config)# switch-port-profile 1/1 profile-6
OS10(config)# exit
OS10# write memory
OS10# reload
```

Verify port profile

```
OS10(config)# show switch-port-profile 1/1

|  Node/Unit   |  Current     |  Next-boot   | Default    |
|--------------+--------------------+--------------------|
|     1/1      |  profile-2   |  profile-2   | profile-1  |

Supported Profiles:
profile-1
profile-2
profile-3
profile-4
profile-5
profile-6
```

For complete information about configuring specific ON-Series switch-port profiles, see the *Dell EMC SmartFabric OS10 User Guide* at www.dell.com/support/.

NTP server configuration

This information explains how to set up network time protocol (NTP) to synchronize timekeeping among a set of distributed time servers and clients. The protocol coordinates time distribution in a large, diverse network. NTP clients synchronize with NTP servers that provide accurate time measurement. NTP clients choose from several NTP servers to determine which offers the best available source of time and the most reliable transmission of information.

NOTE: The NTP server configured on SFD should be on premise (located in the same data center as SFD), and reachable by SFD. Using NTP servers (such as time.google.com) that are not on premise or need Internet access for SFD to interface with is not recommended. The NTP server and the switch must have the same time.

To maintain accurate time, OS10 synchronizes with a time-serving host. For the current time, you can set the system to poll specific NTP time-serving hosts. From those time-serving hosts, the system chooses one NTP host to synchronize with and acts as a client to the NTP host. After the host-client relationship establishes, the networking device propagates the time information throughout its local network.

For complete information about NTP, see the *Dell EMC SmartFabric OS10 User Guide* at www.dell.com/support/.

Enable NTP

NTP is disabled by default. To enable NTP, configure an NTP server where the system synchronizes. To configure multiple servers, enter the command multiple times. Multiple servers may impact CPU resources.

Enter the IP address of the NTP server where the system synchronizes.

```
OS10(config)# ntp server ip-address
```

View system clock state

```
OS10(config)# do show ntp status
system peer:          0.0.0.0
system peer mode:     unspec
leap indicator:       11
stratum:              16
precision:            -22
```

```
root distance:          0.00000 s
root dispersion:        1.28647 s
reference ID:           [73.78.73.84]
reference time:         00000000.00000000  Mon, Jan  1 1900  0:00:00.000
system flags:           monitor ntp kernel stats
jitter:                 0.000000 s
stability:              0.000 ppm
broadcastdelay:         0.000000 s
authdelay:              0.000000 s
```

View calculated NTP synchronization variables

```
OS10(config)# do show ntp associations
     remote           local    st poll reach  delay   offset    disp
==============================================================================
 10.16.150.185   10.16.151.123 16 1024    0 0.00000  0.000000 3.99217

OS10# show ntp associations
     remote           local    st poll reach  delay   offset    disp
==============================================================================
 10.16.150.185   10.16.151.123 16 1024    0 0.00000  0.000000 3.99217
```

Authentication lockout

This information explains how to prepare your switch for SmartFabric Director from the OS10 side in case of authentication lockout.

In OS10 10.5.2.0P1, the default lockout period after three invalid login attempts is five minutes. Within the five minutes, if additional login attempts are made irrespective of valid or invalid credentials, the lockout period is reset to five minutes after each attempt. This may lead to a denial of service from OS10. To avoid this issue, you need to configure the default lockout-period to zero minutes. Authentication lockout is applicable for all NBIs or applications connecting to a switch.

1. Configure the password attributes to zero seconds.

   ```
   OS10(config)# password-attributes lockout-period 0
   ```

2. Exit CONFIGURATION mode.

   ```
   OS10(config)# exit
   ```

3. Display the running configuration to verify the change.

   ```
   OS10# show running-configuration password-attributes
   !
   password-attributes lockout-period 0
   ```

4. Write memory to save the configuration.

   ```
   OS10# write memory
   ```

Configure lockout period

```
OS10(config)# password-attributes lockout-period 0
OS10(config)# exit
OS10# show running-configuration password-attributes
!
password-attributes lockout-period 0
OS10# write memory
```

6

First-time setup

This information explains what you must do if setting up SmartFabric Director for the first time.

NOTE: SFD cannot be installed on a single ESXi embedded host client, and must be installed through a vCenter server.

Topics:

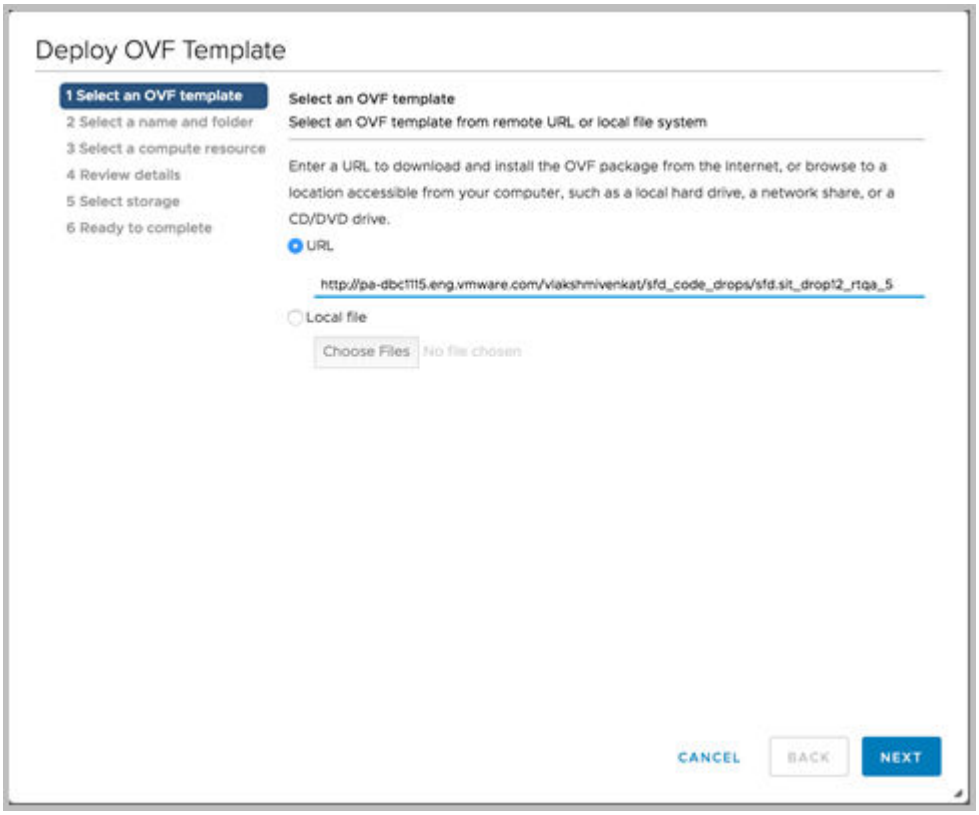
Installation using vCenter 6.7

This information describes how to import the SmartFabric Director OVA file into the content library, then create a virtual machine (VM). It is recommended that SFD is installed on a server which is part of your infrastructure rack, and is different from workload servers.

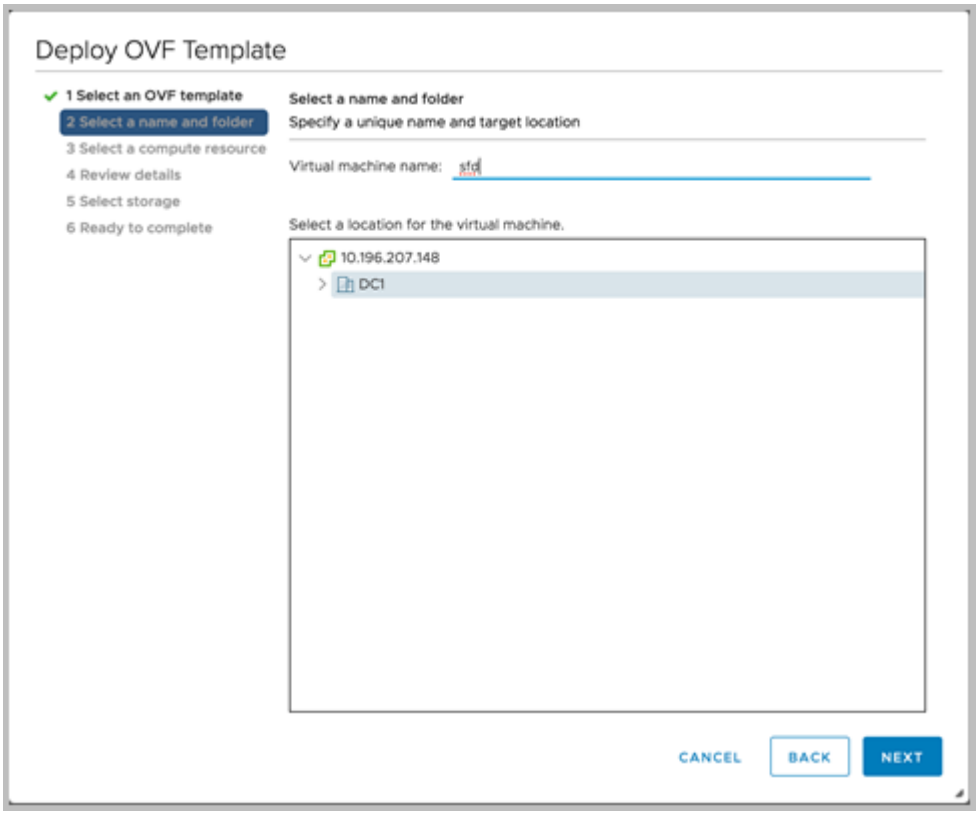
Download and install OVA

You can add items to a content library by importing files from your local system. You can import an OVA package to use as a template for deploying virtual machines.

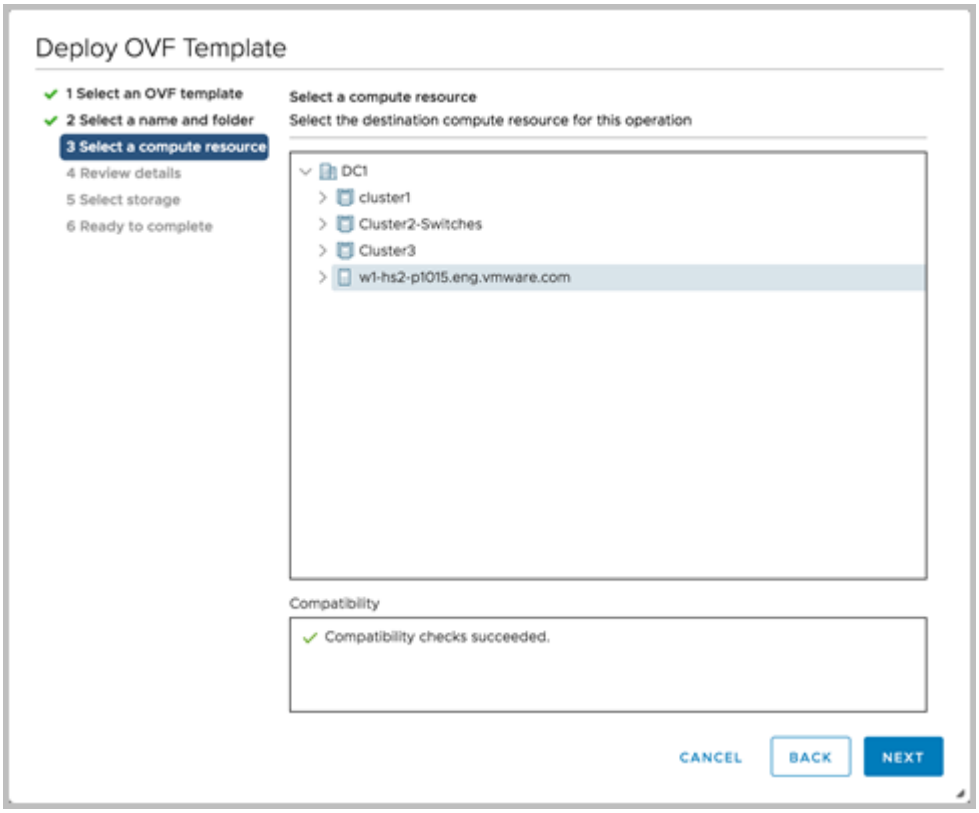
1. Download the OVA from DDL or the VMware Solution Exchange, then store the OVA image locally or on a server.
2. Select **Hosts and Domains**, select the domain that the plug-in must manage, then select **Action** > **Deploy OVF Template**.
3. Select **Local file**, click **Choose Files** and select `SmartFabric_Director_2.0.0.ova` from a local source, then click **Next**. You can use either a URL or a local file.



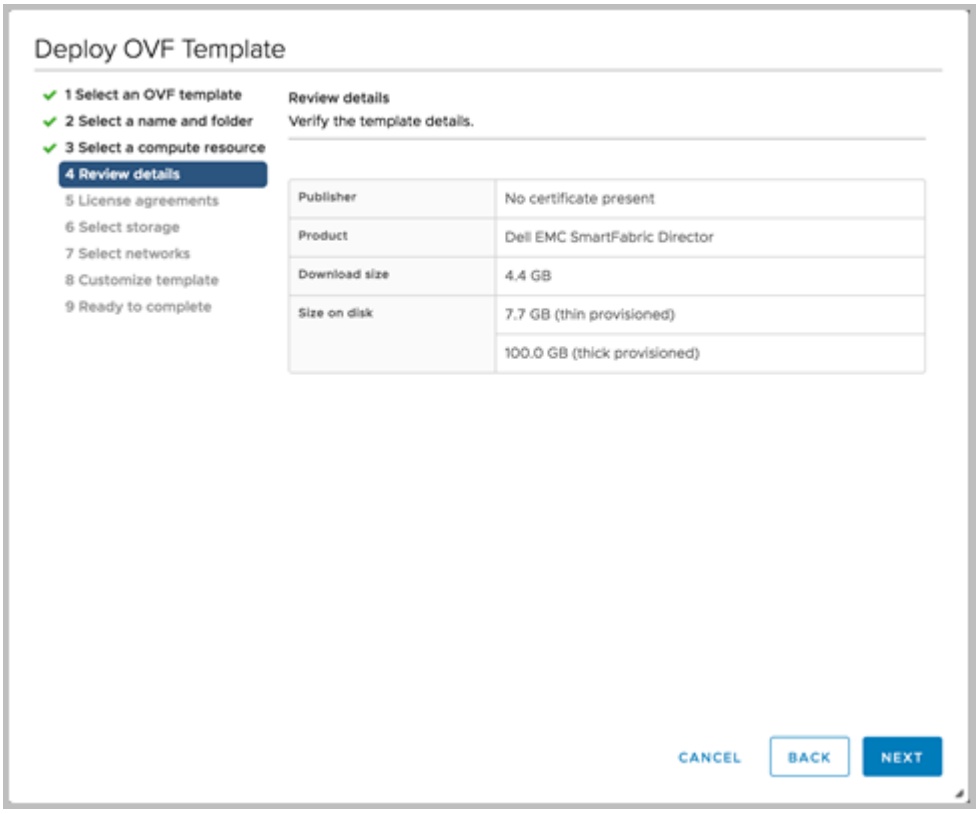
4. Select a name and folder for the VM, then click **Next**.



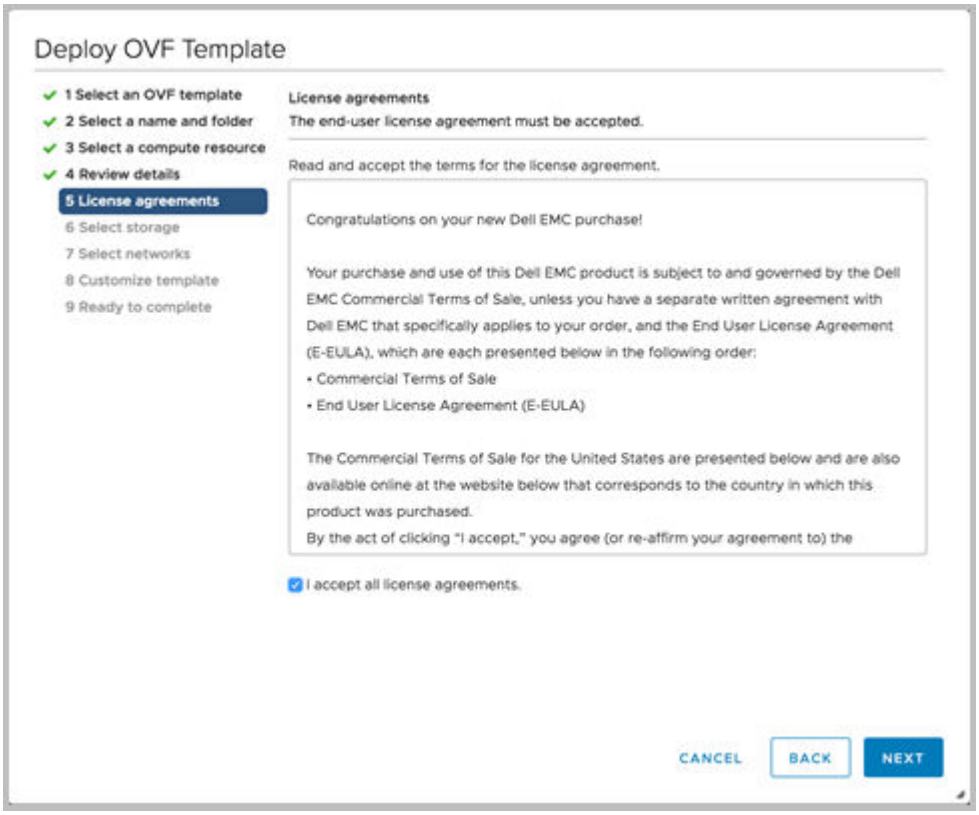
5. Select the destination compute resource, then click **Next**.



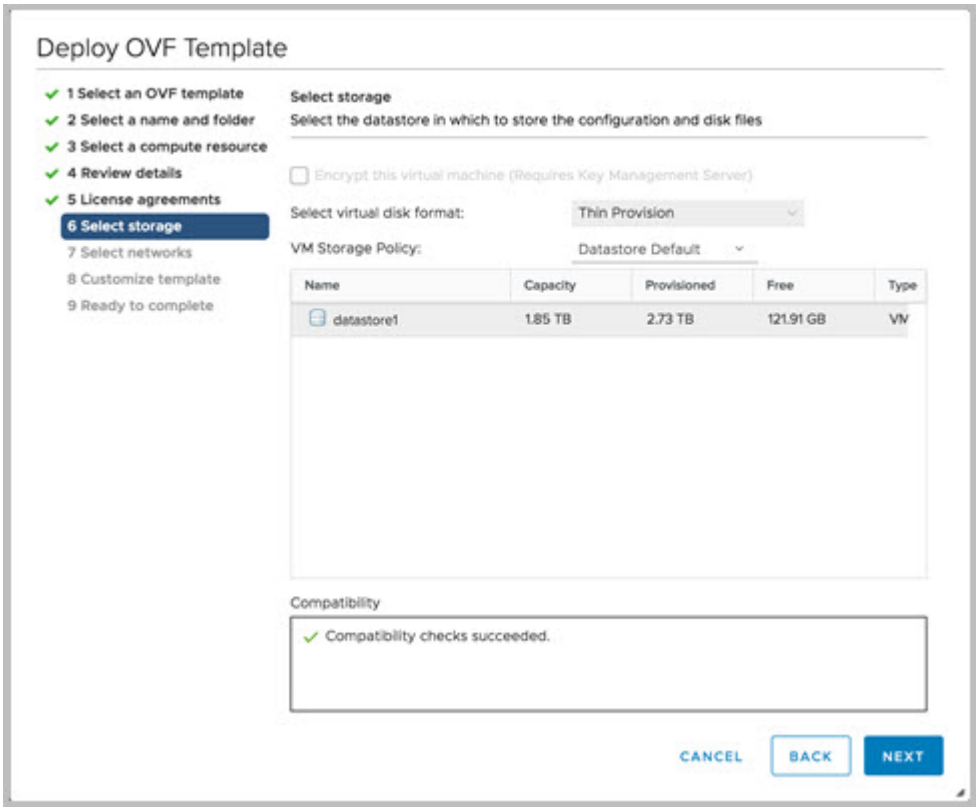
6. Review and verify the template details, then click **Next**.



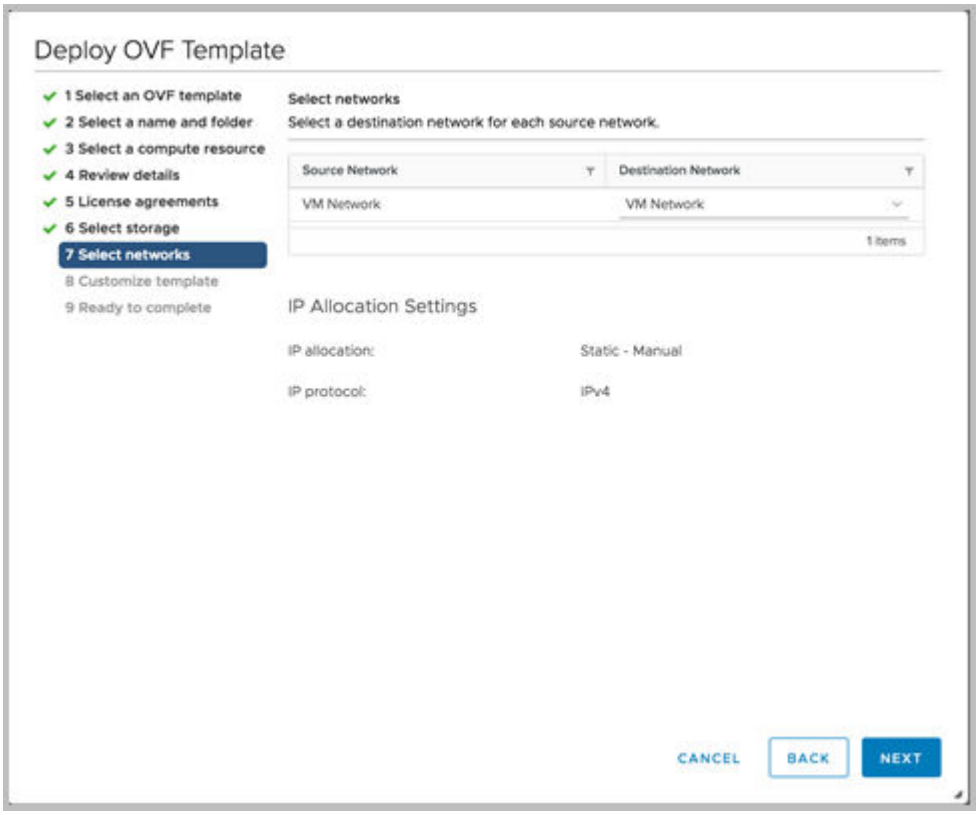
7. Accept the user license agreement (EULA), then click **Next**.



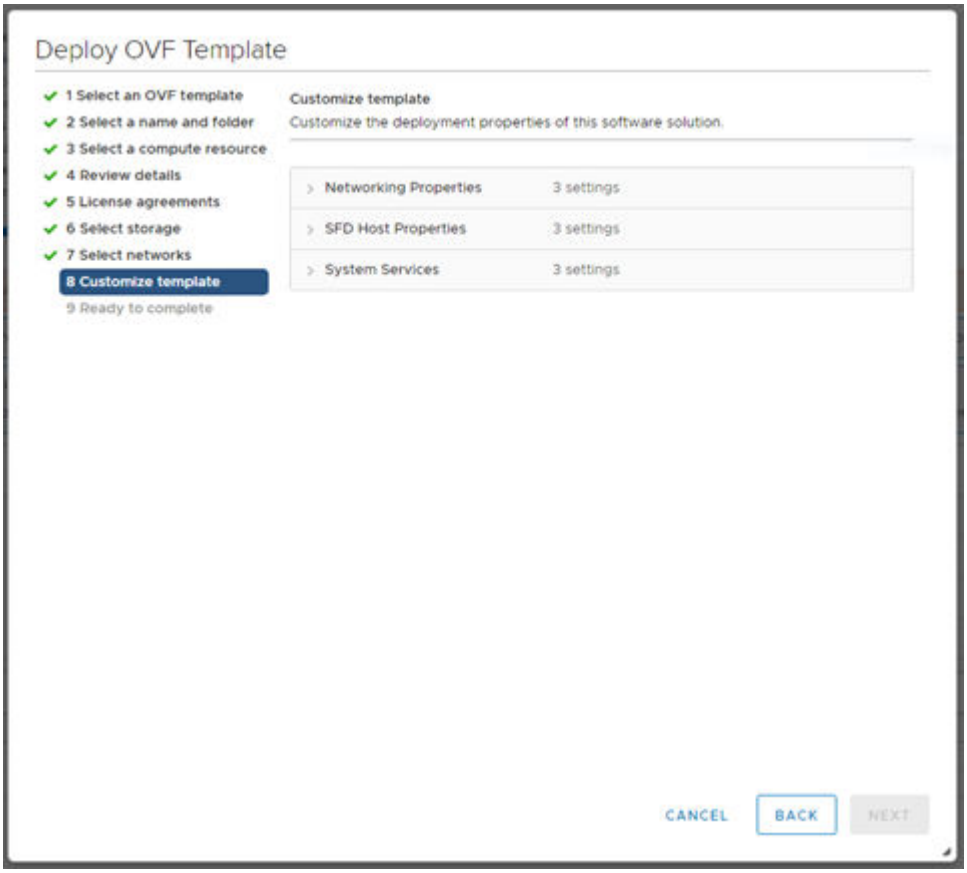
8. Select the data store to store the configuration and datafile, then click **Next**.



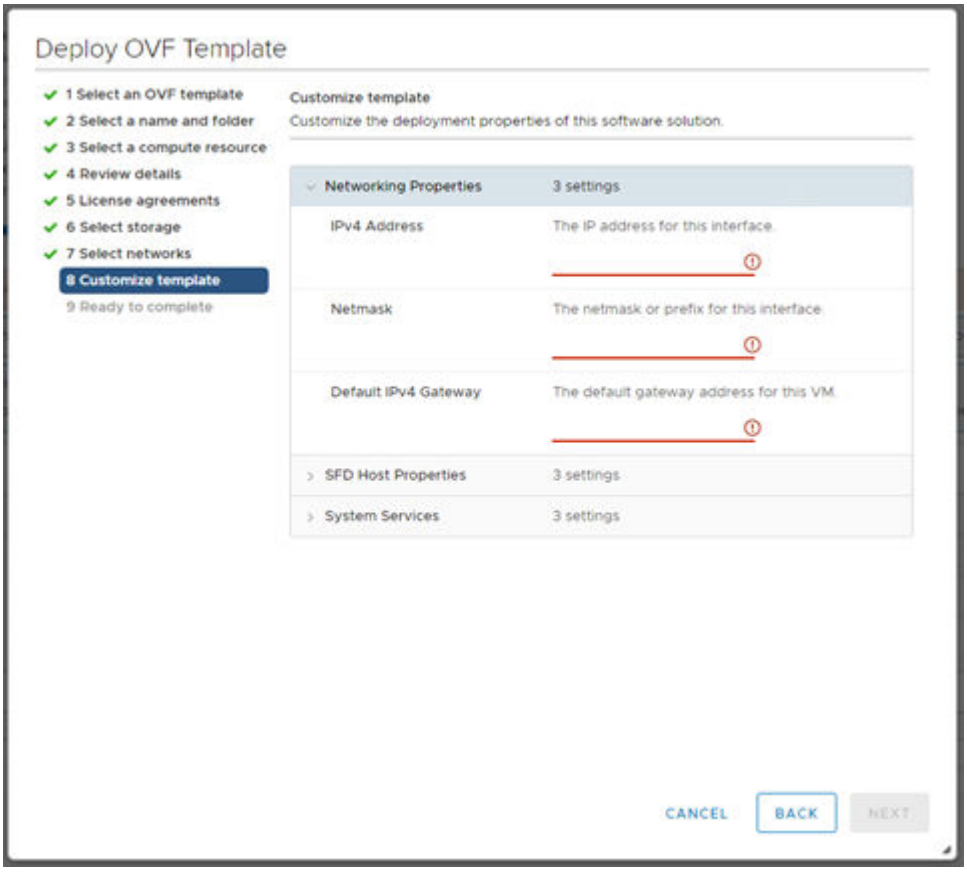
9. Select a destination network for each network source, then click **Next**. The default VLAN ID for this network is 3939. The vCenter Server network must be connected to the port group where the vCenter is reachable for plug-in deployment of the VM.



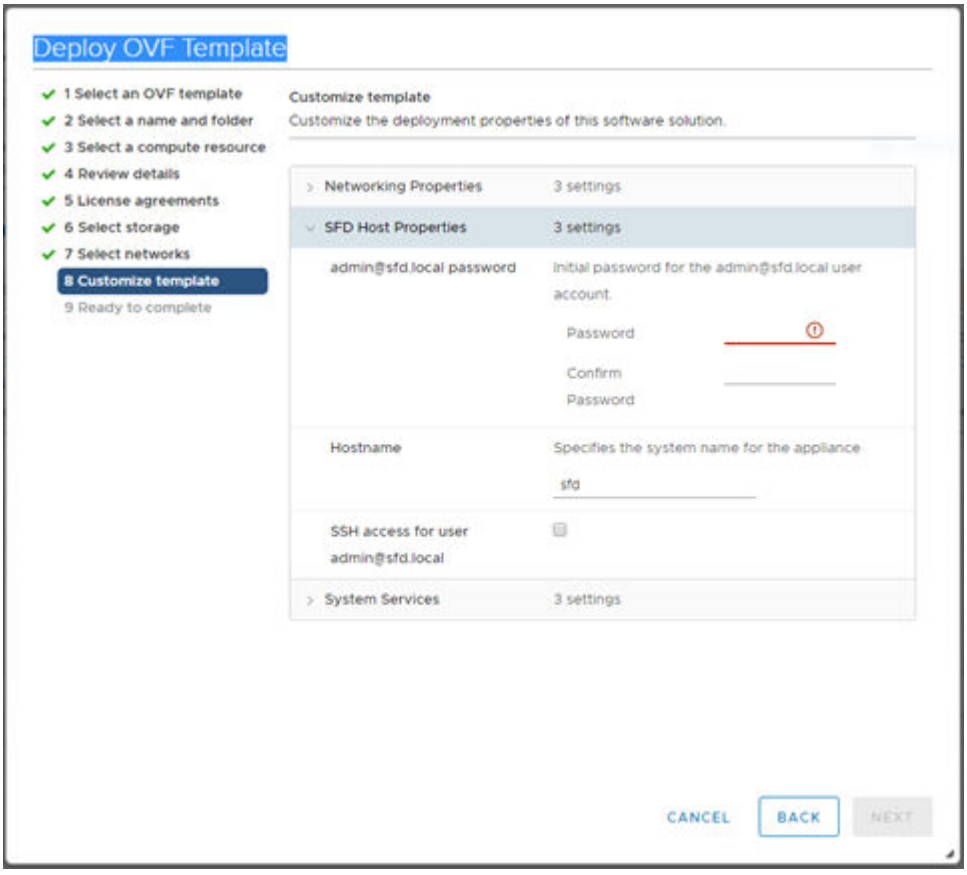
10. Enter the system name for the appliance, select the checkbox if SSH access is enabled, list the NTP servers (space separated), enter the Domain Name Server, then click **Next**. The Service Tag can be added later as part of the system settings after logging into SFD.
11. Select **Networking Properties** to customize the template.



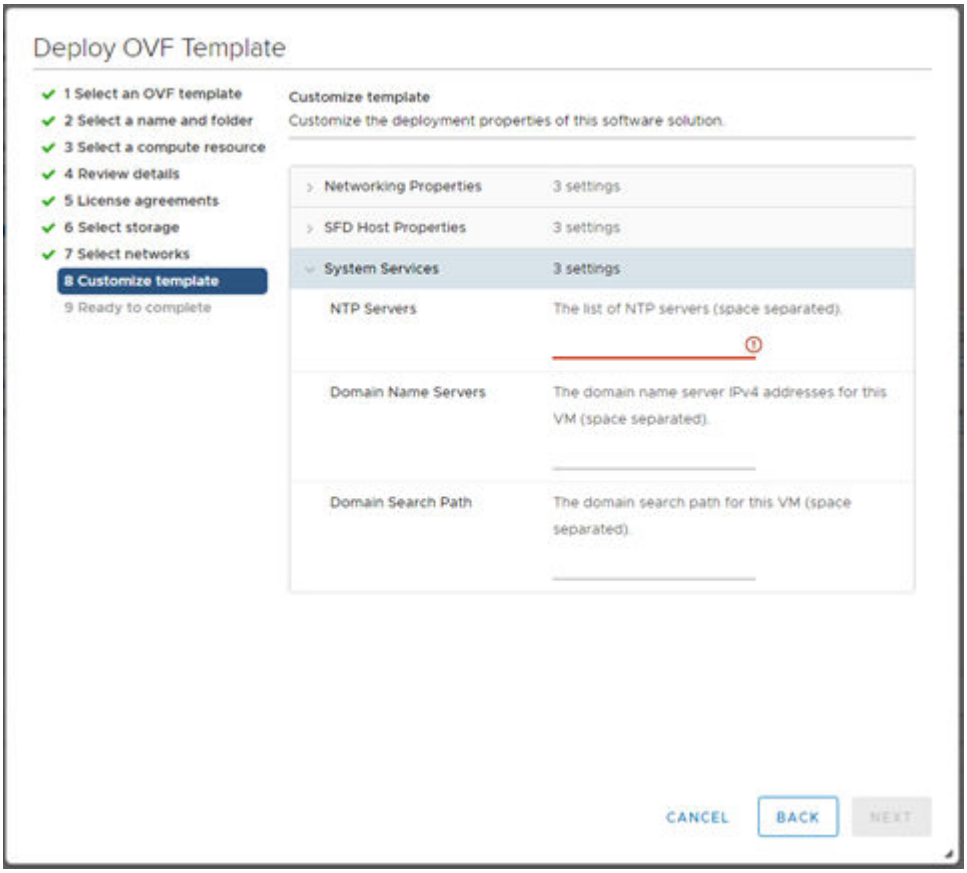
12. Enter the IPv4 address for this interface, the netmask, and the default IPv4 gateway address for this VM.



13. Select **SFD Host Properties**, then enter the password for the SFD host.



14. Select **System Services**, enter the list of NTP servers separated by a space, then click **Next**.



15. Click **Finish** to start creation of the VM, then power on the VM.

NOTE: Once installation finishes, it may take 7 to 12 minutes for the SFD VM to be fully operational.

Installation using vCenter 6.5

This information describes how to modify the .vmx file for a successful SmartFabric Director installation on vSphere 6.5. You must edit the .vmx file and comment out the nvram location setting.

NOTE: If you are using vSphere 6.7, go to the next section. If you are using vSphere 6.5, you must modify the nvram setting before creating a VM.

1. Shut down the SFD virtual machine.
2. Download the .vmx configuration file from the VM folder, then open the file in a text editor.
3. Comment out the nvram setting.

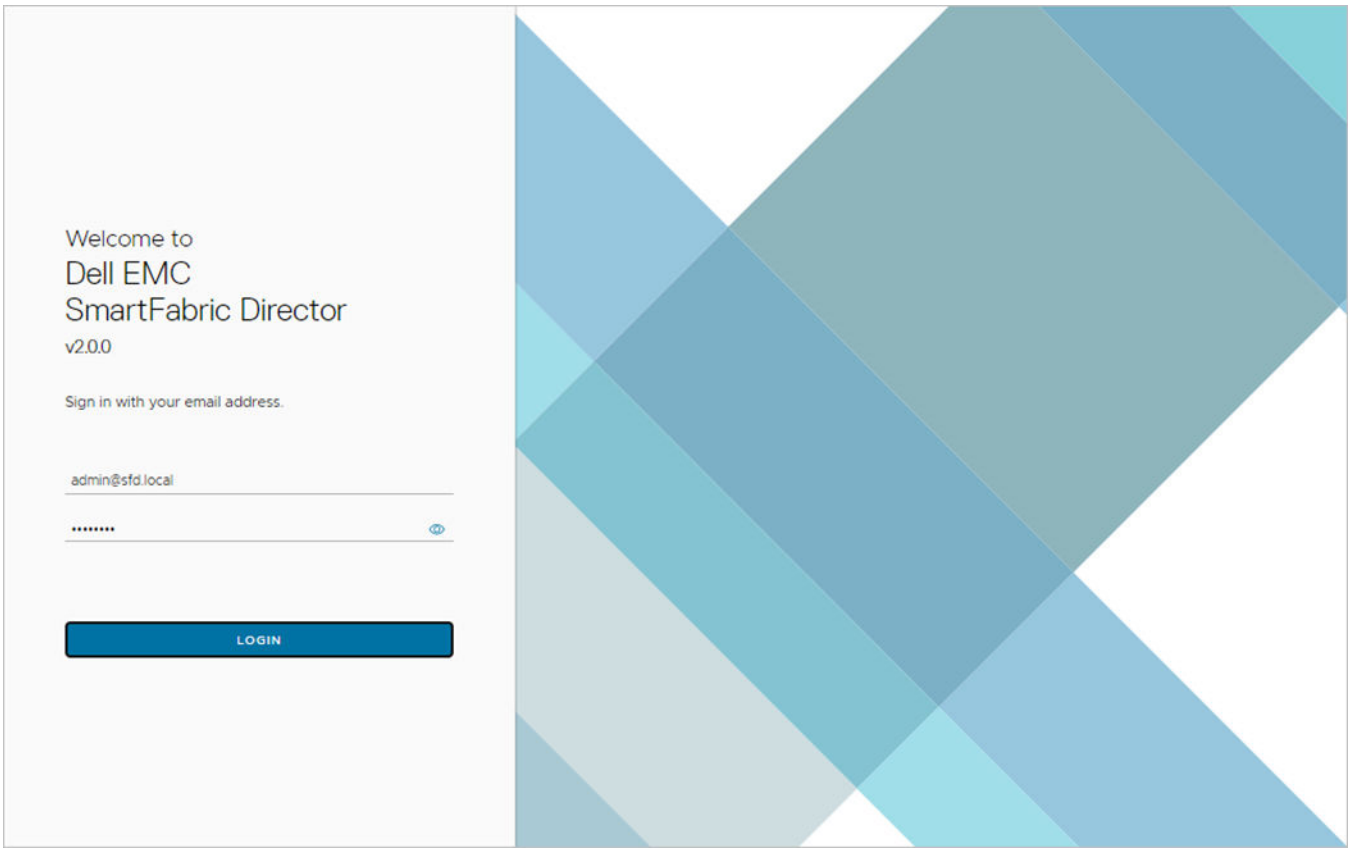
```
.encoding = "UTF-8"
config.version = "8"
virtualHW.version = "10"
pciBridge0.present = "TRUE"
svga.present = "TRUE"
pciBridge4.present = "TRUE"
pciBridge4.virtualDev = "pcieRootPort"
pciBridge4.functions = "8"
pciBridge5.present = "TRUE"
pciBridge5.virtualDev = "pcieRootPort"
<snip>
#nvram = "ovf:/file/file2" <- The 'nvram' entry must be commented out
```

4. Save the changes, replace the file on the VM folder, then exit the text editor.
5. Start the VM.

NOTE: If SmartFabric Director is restarted and if any changes have been made to the switches (such as switches reloaded) during this time, it is recommended to reload the switch again after SFD is up. This ensures that the complete configuration is redownloaded to the switches.

Log in to SmartFabric Director

1. Open a browser window, then enter the IP address that is specified during installation of the SFD VM in vCenter.
2. Enter **admin@sfd.local** for the username and the password that is configured during VM deployment, then click **Login**.



Navigating SmartFabric Director

The navigation menu is automatically collapsed at log in. Click **>>** to expand the menu.

Specify system settings

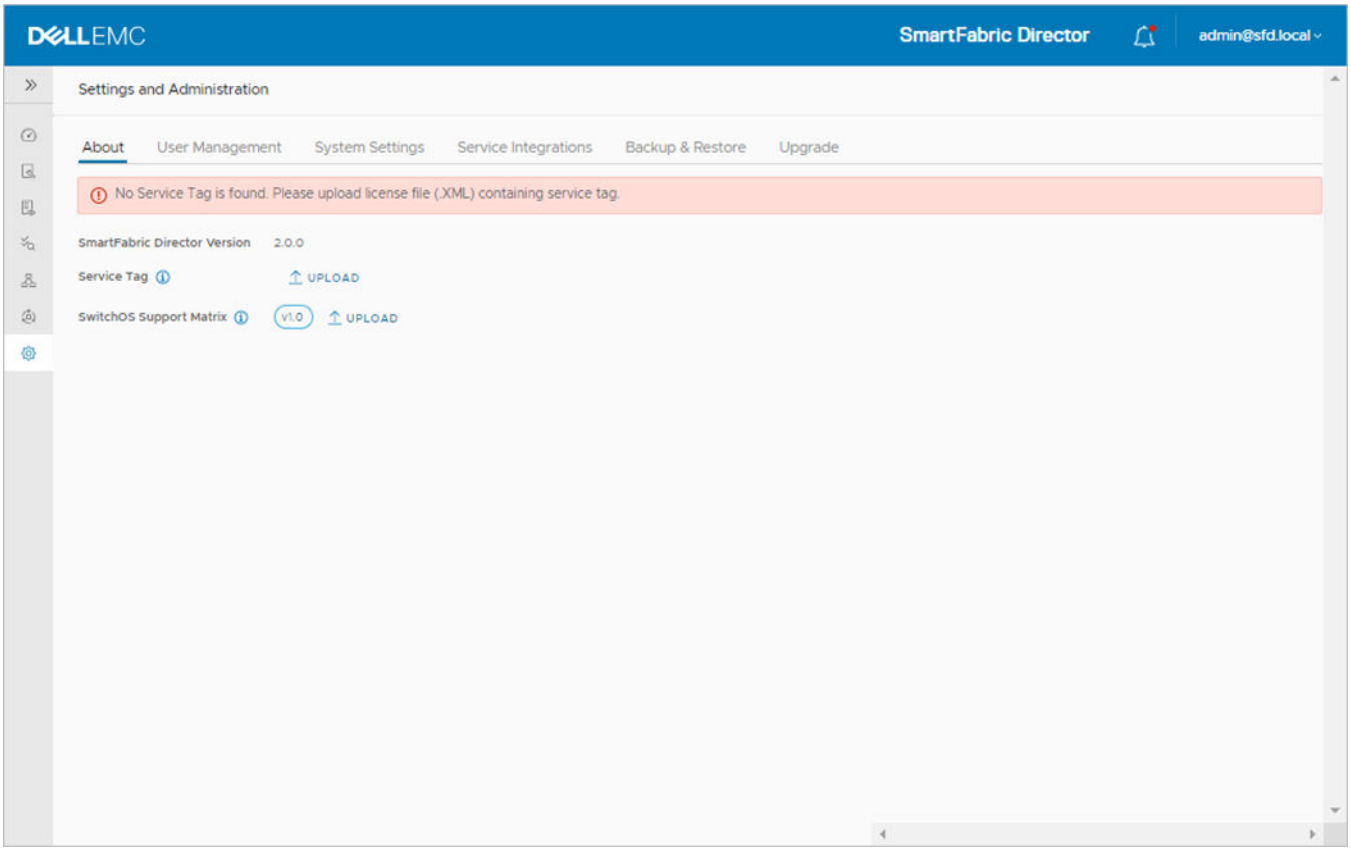
This information describes how to specify system settings for SmartFabric Director for first-time use.

1. Upload service tag to About.
2. Upload SwitchOS support matrix to About.
3. Add vCenter server or NSX-T Manager to VMware Managers.
4. (Optional) Add additional DNS servers System Settings.
5. (Optional) Add additional NTP servers to System Settings.
6. (Optional) Add Active Directory server to Service Integrations.
7. Add switch image server to Service Integrations.
8. Add backup location to Backup Locations.

Upload service tag and Switch OS support matrix

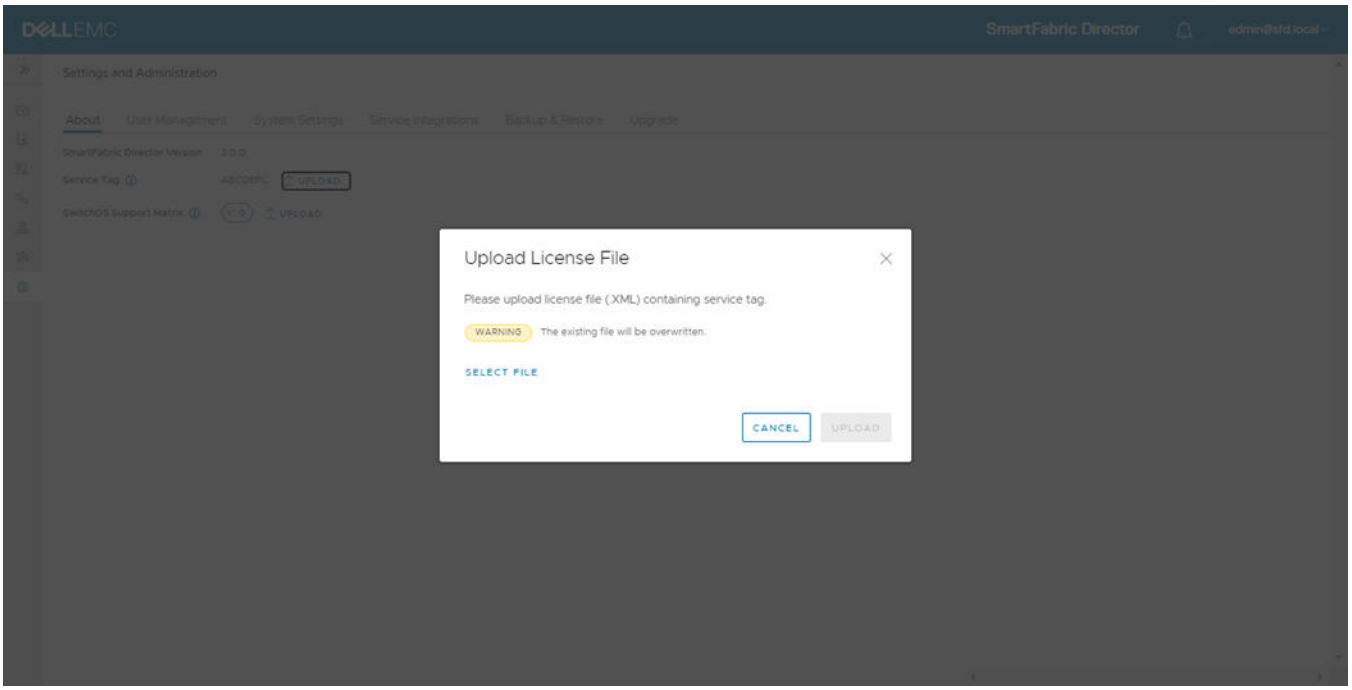
The About tab displays the SmartFabric Director software version, service tag, and switchOS support.

NOTE: This example shows a new installation.



Upload service tag

1. Sign into DDL using your account credentials (see Download SFD image).
2. Download the SFD license file (XML) to your local file system.
3. Click **Upload** to the right of Service Tag.

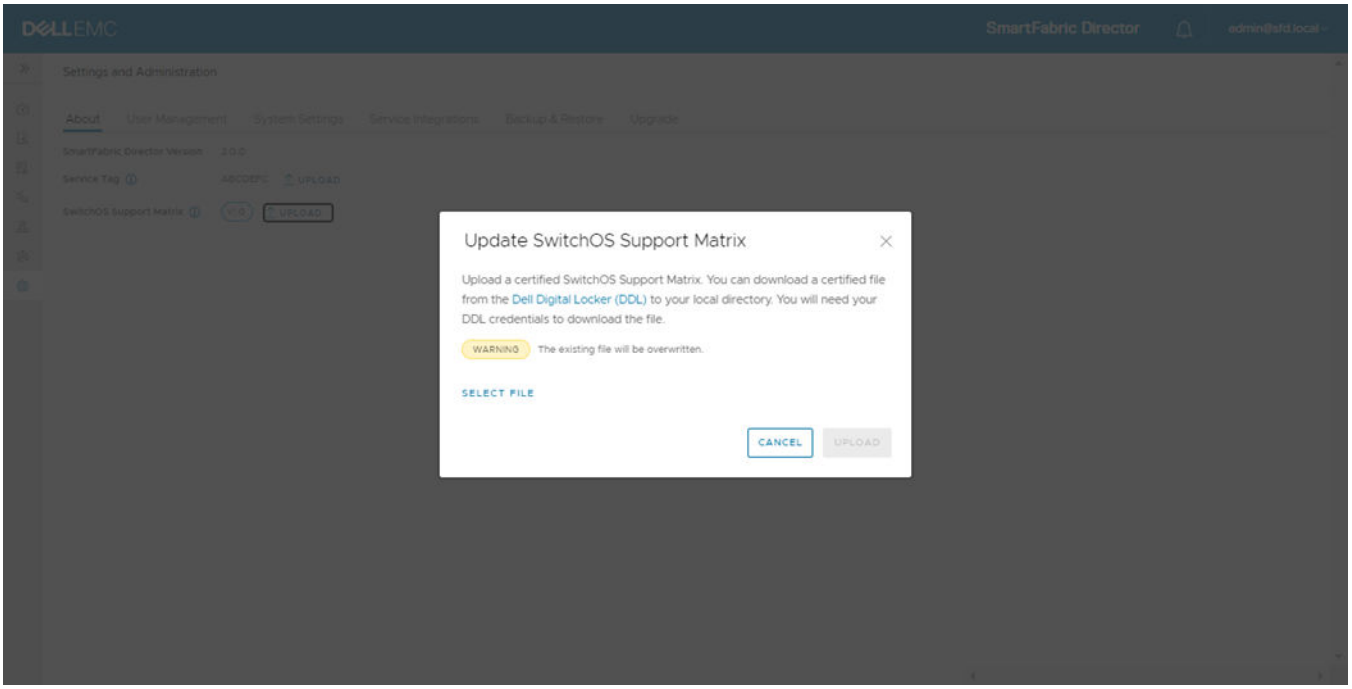


4. Click **Select file**, navigate to where you saved the file, then click **Upload**.

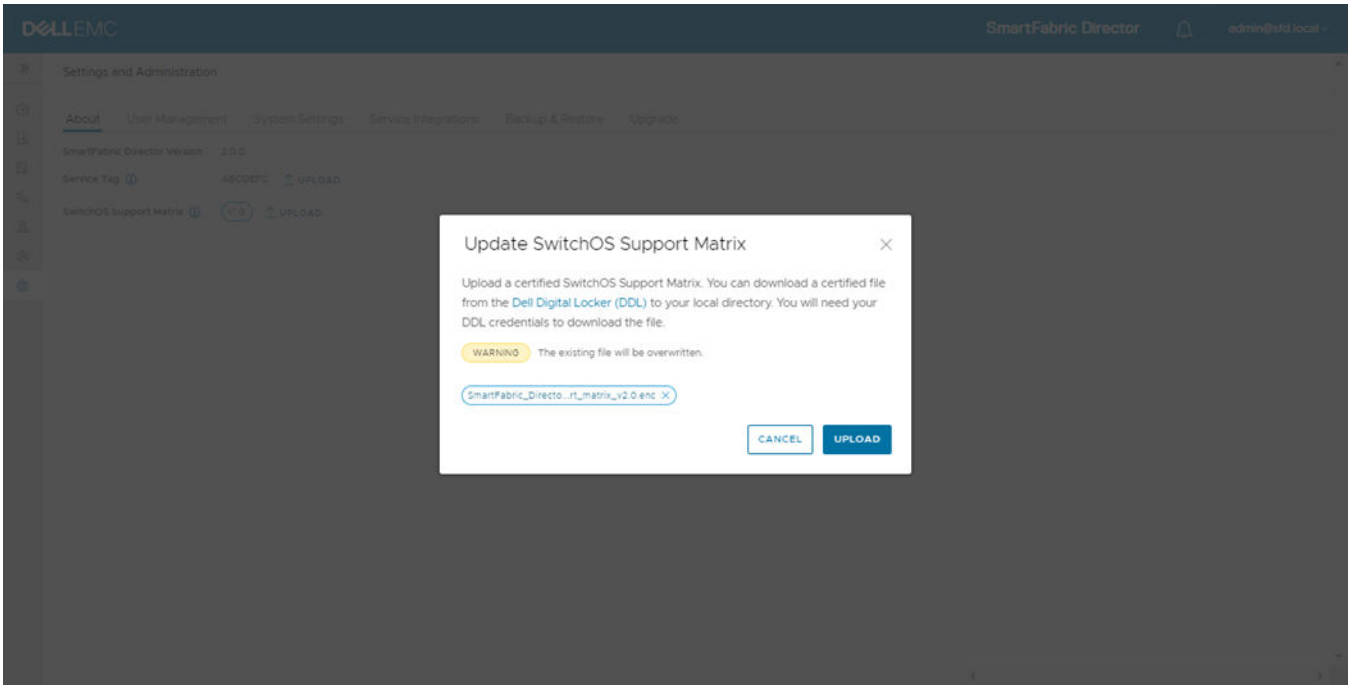
Upload switchOS support matrix

1. Sign into DDL using your account credentials (see Download SFD image).

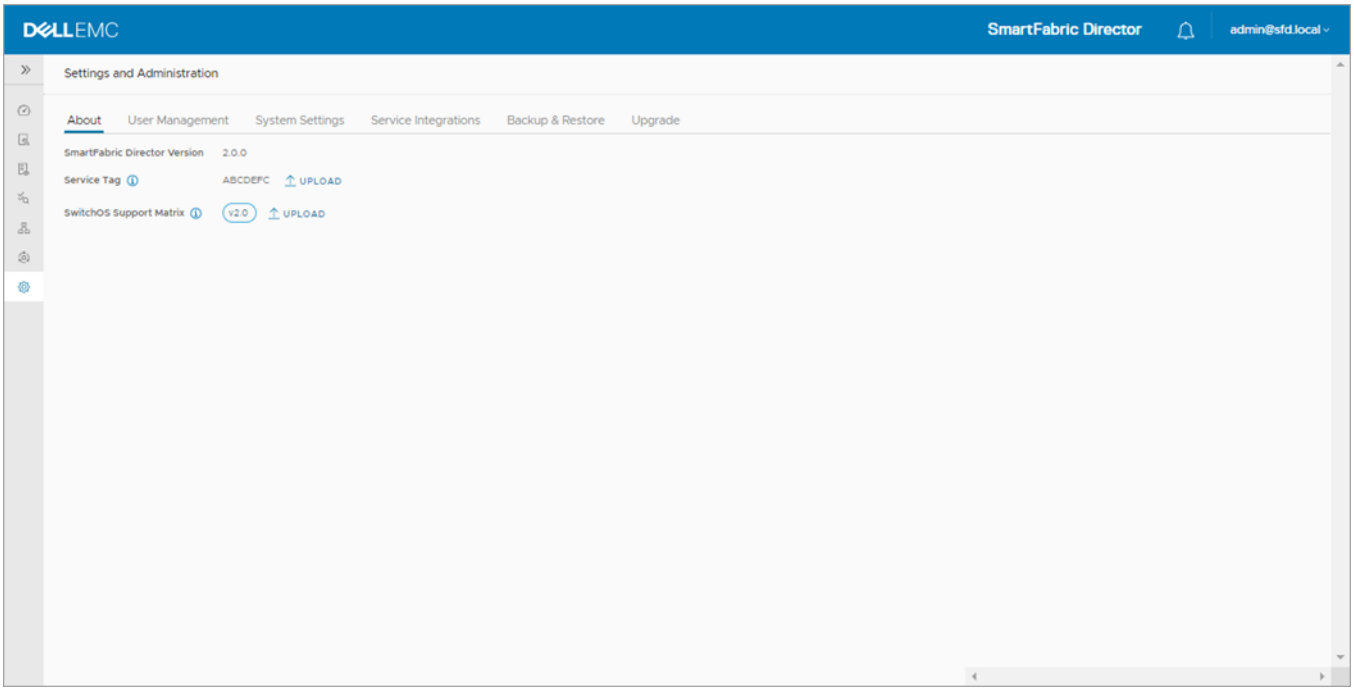
2. Download the SFD SwitchOS support matrix file to your local file system.
3. Click **Upload** to the right of SwitchOS support matrix.



4. Click **Select file**, navigate to where you saved the file, then click **Upload**.



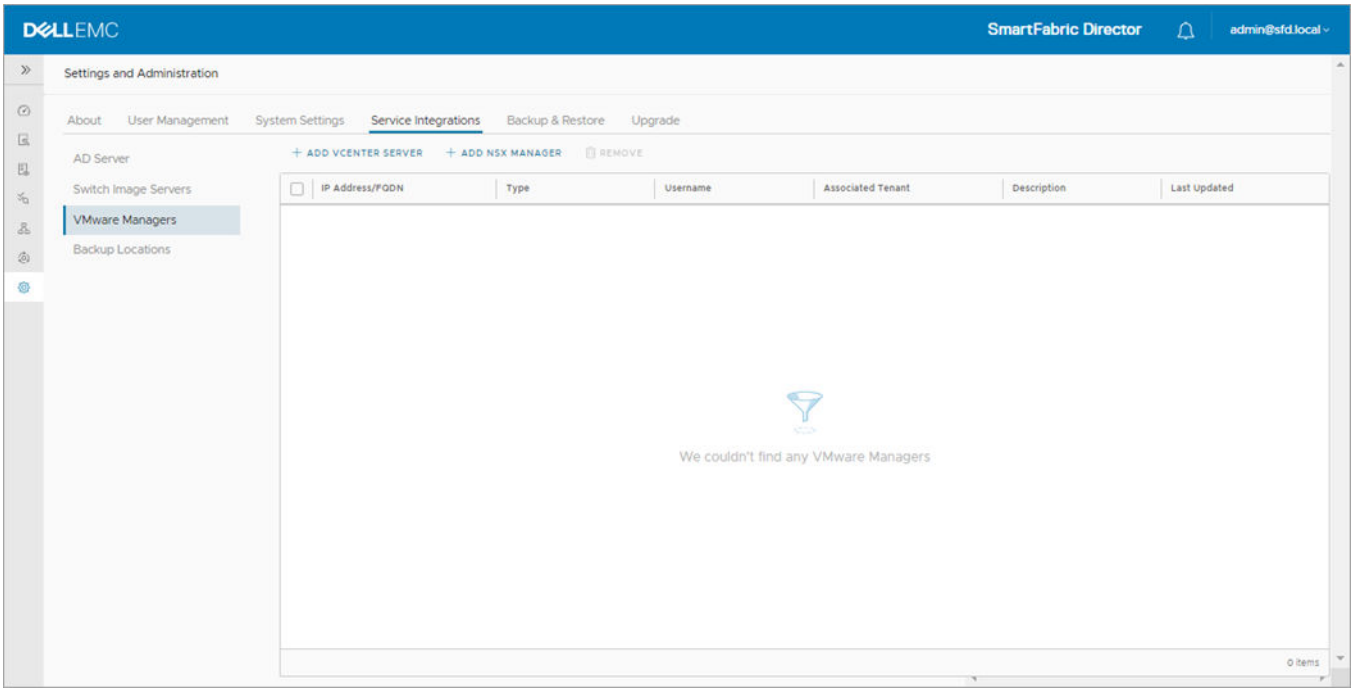
Both the license and SwitchOS support matrix are now uploaded successfully.



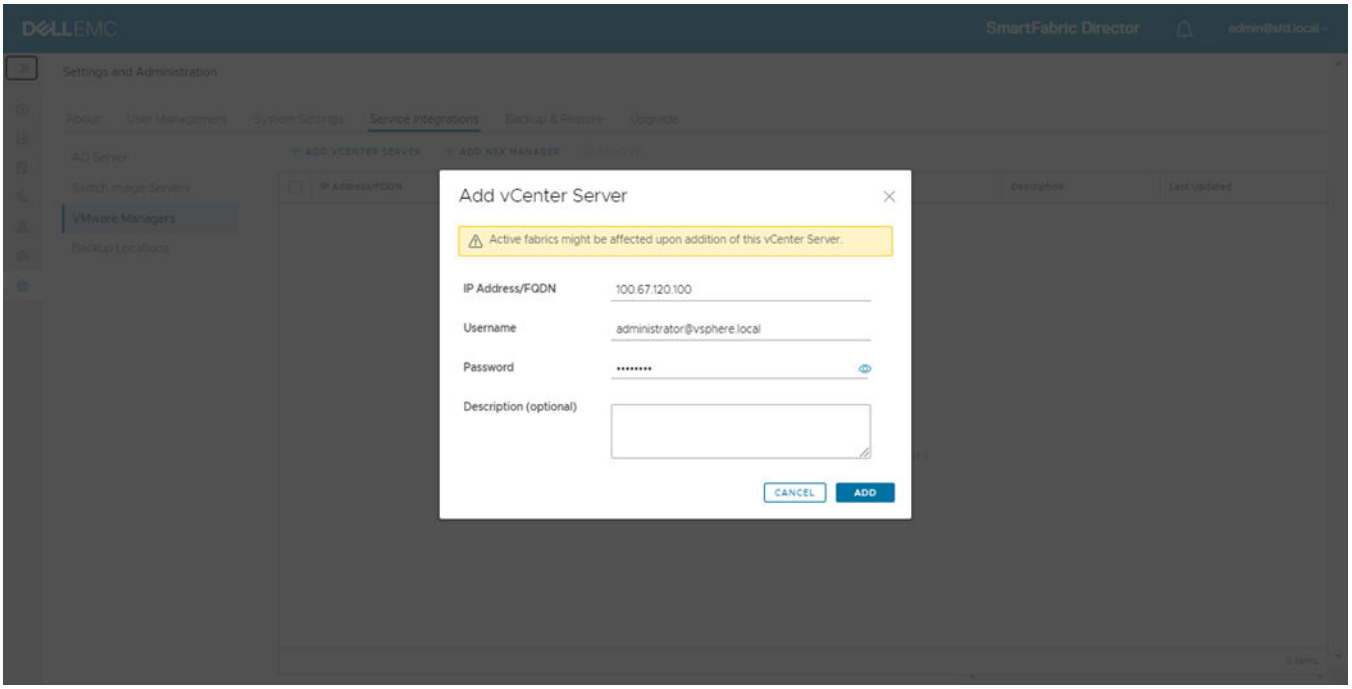
VMware Manager integrations

NOTE: You can only have one active VMware Manager integration with SmartFabric Director.

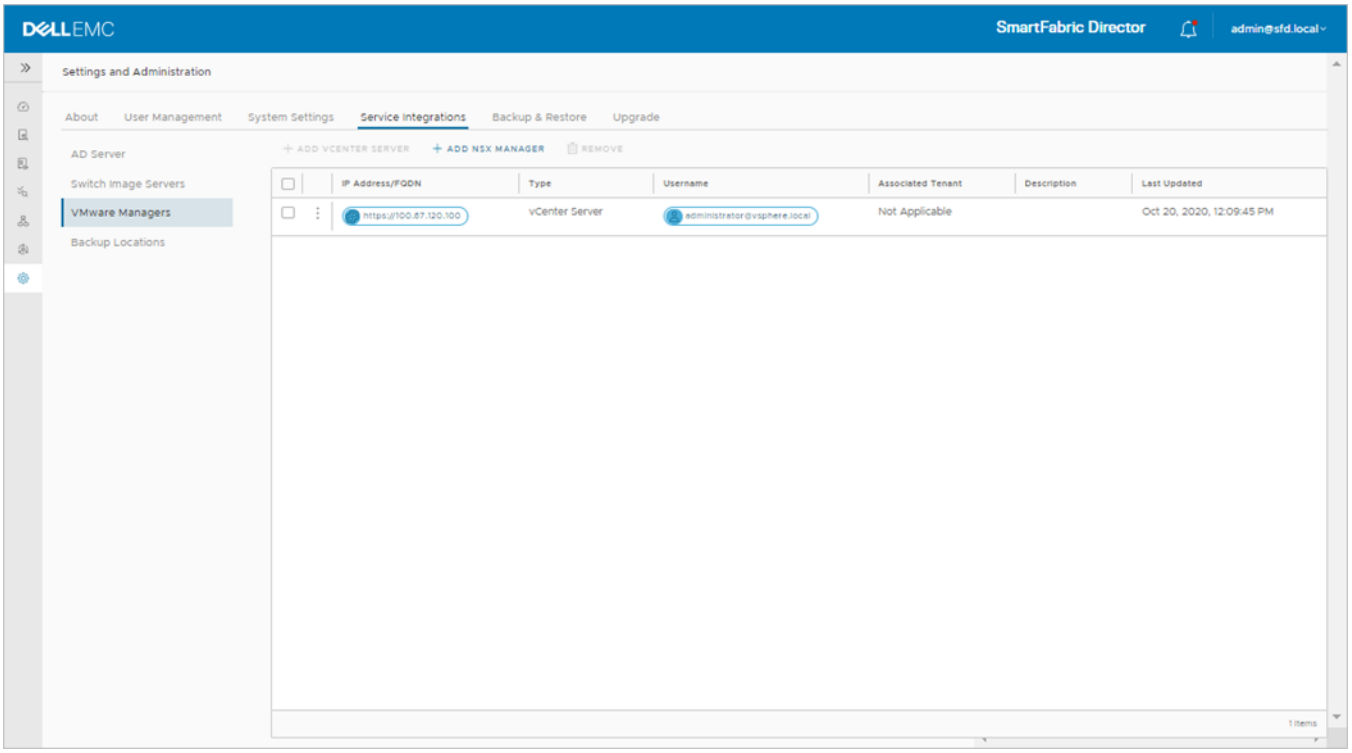
1. Select **Settings and Administration > Service Integrations**, then select **VMware Managers**.



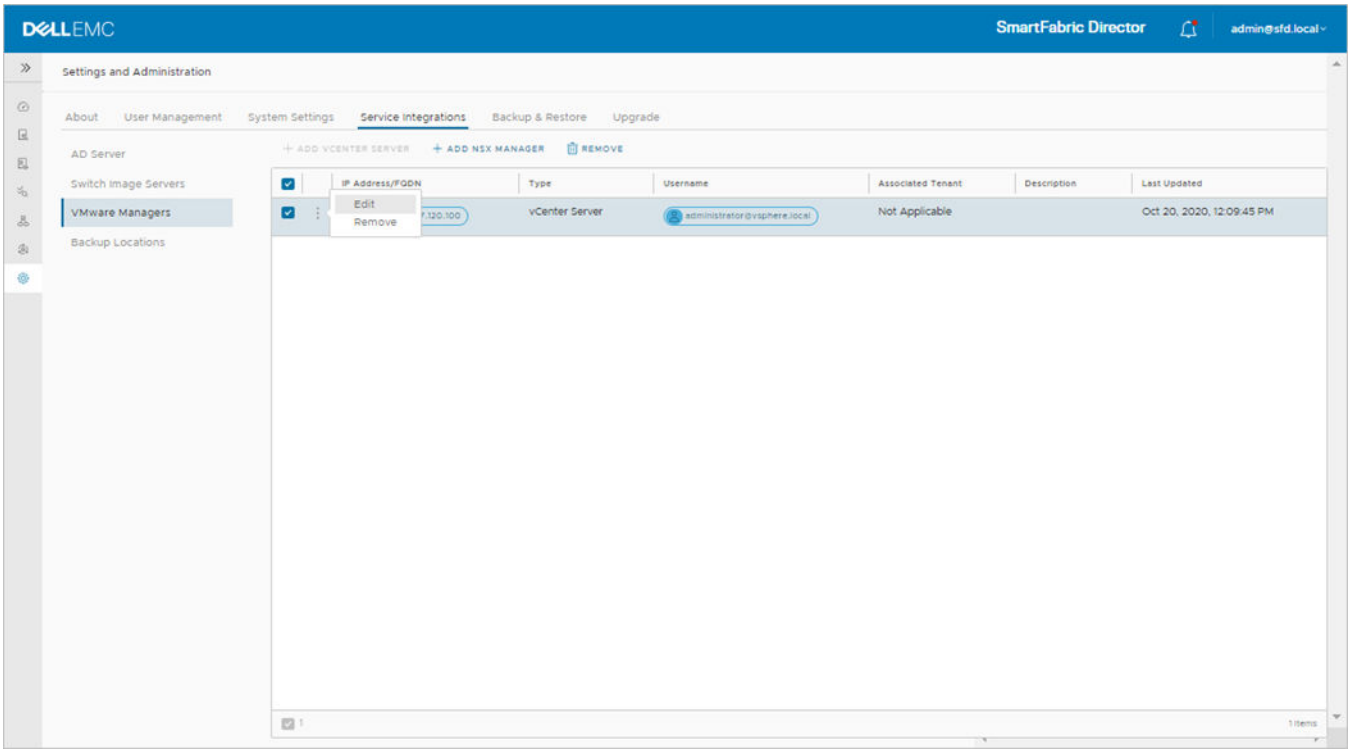
2. Click **Add vCenter server** to configure integration with a vCenter. See **NSX Manager** if you are not using a vCenter Server.



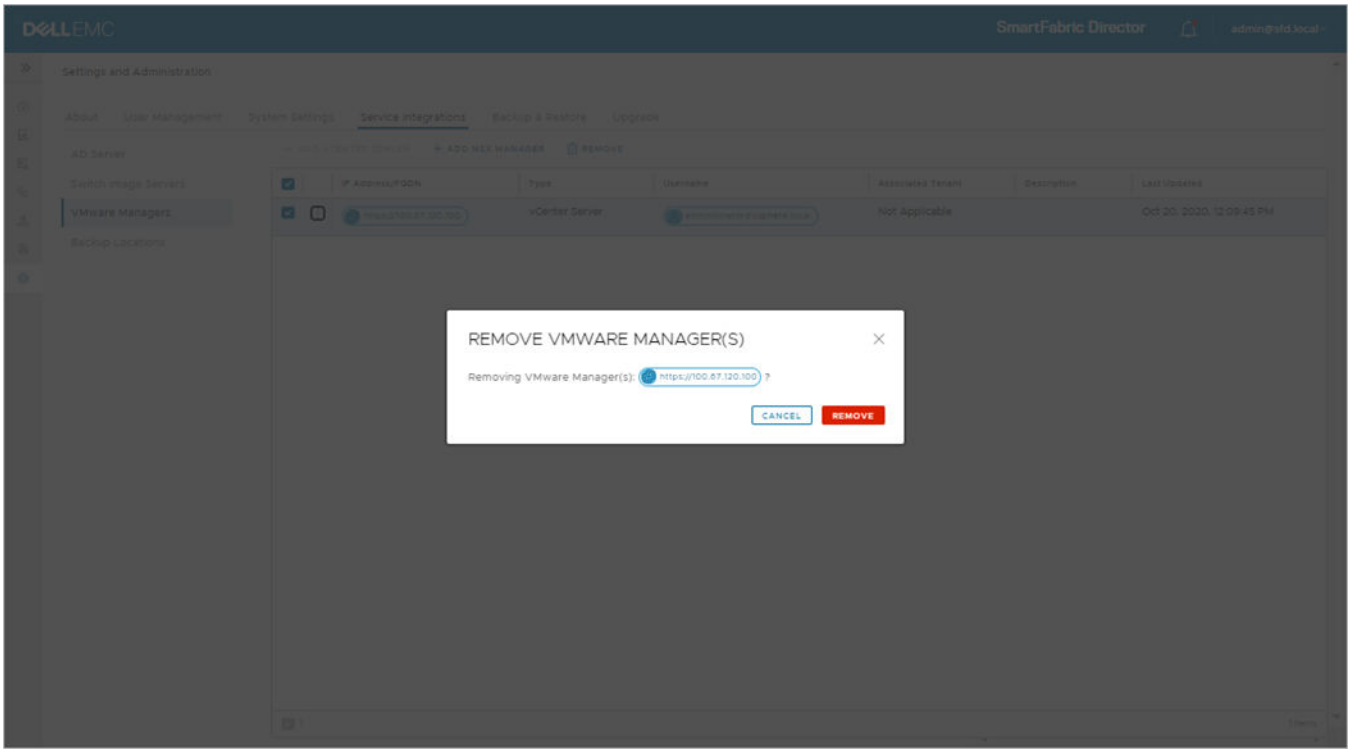
3. Enter the IP address/FQDN, username, password, optional description, then click **Add**.



4. (Optional) Select the vCenter server, click on the three dots, select **Remove** and follow the steps. You can also select **Edit** to modify the settings for the vCenter server.



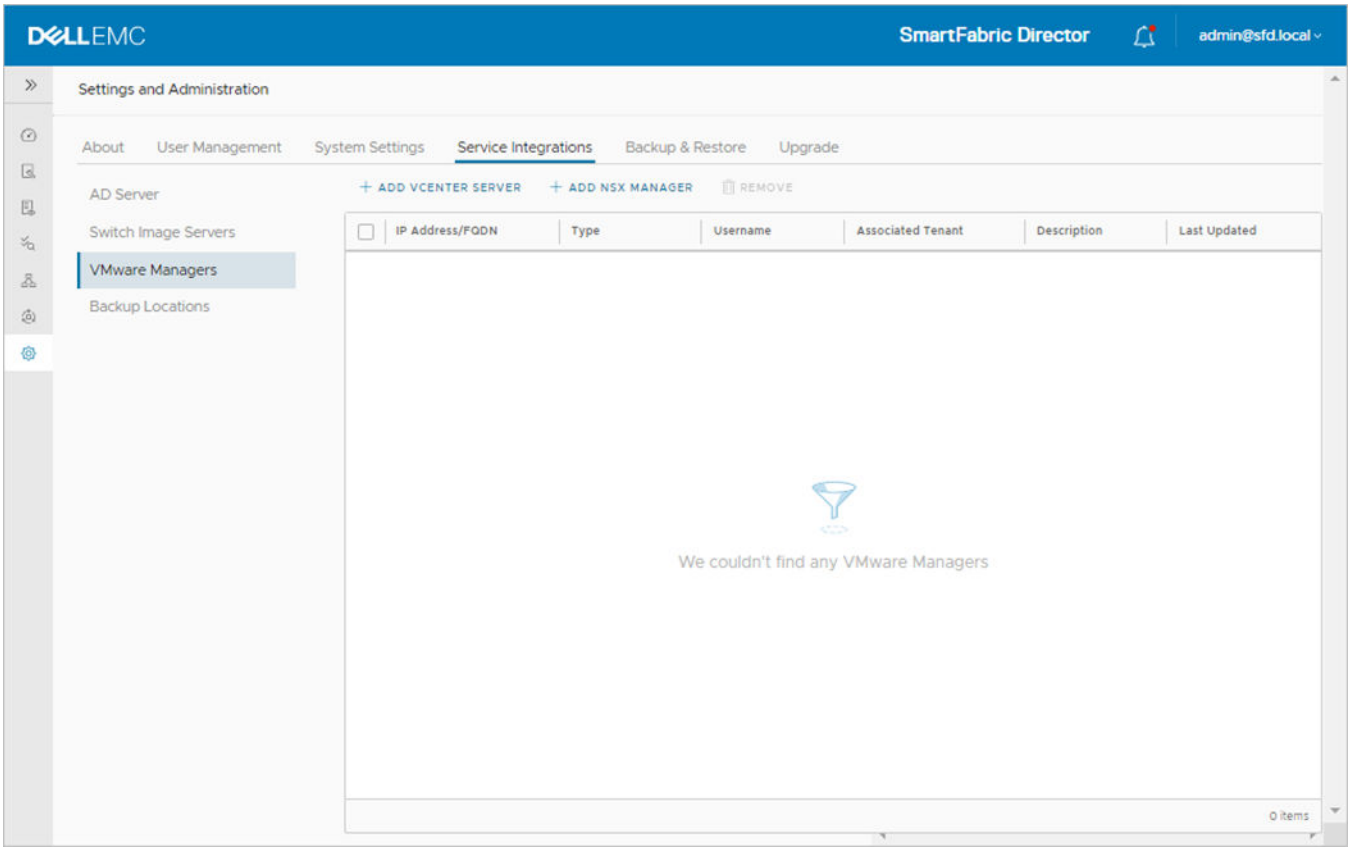
Click **Remove** to delete the vCenter server.



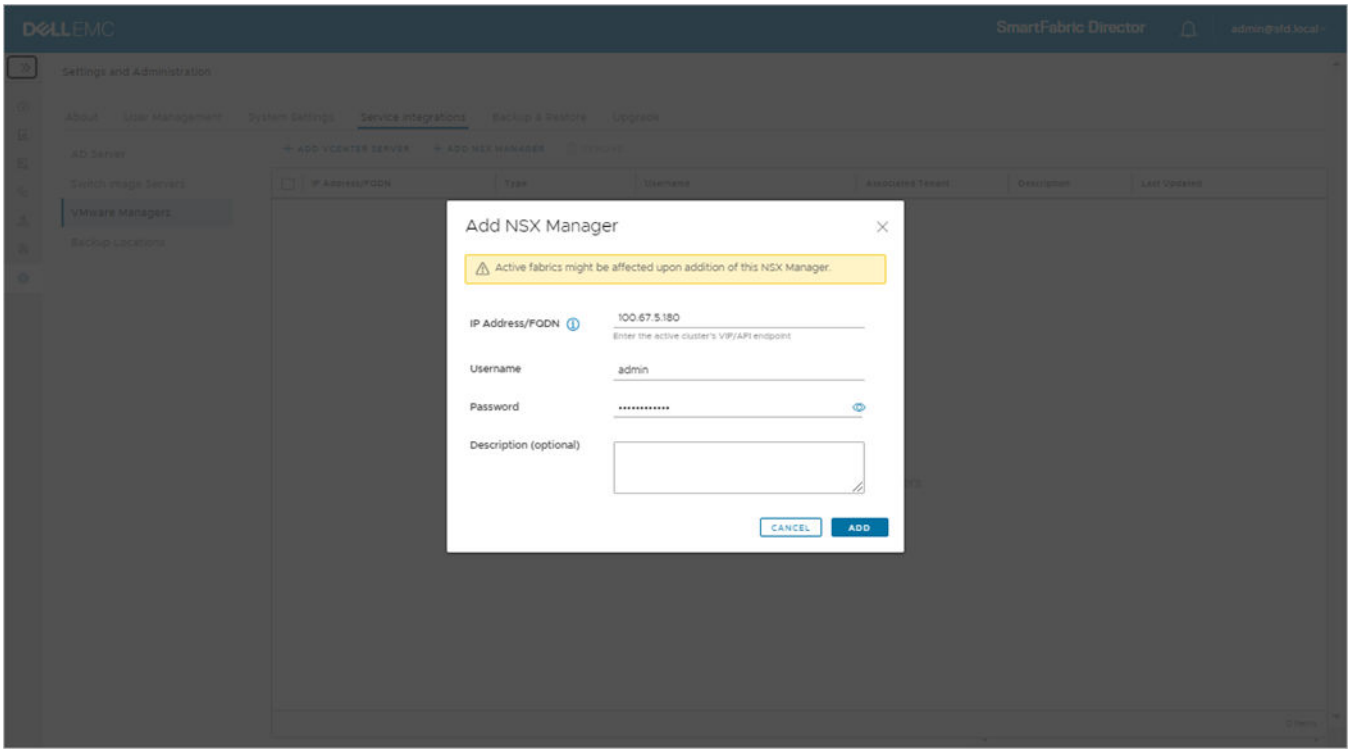
NOTE: If you are using an ESXi host and remove the current VMware Manager, you must add a new connection to SFD.

Add NSX Manager

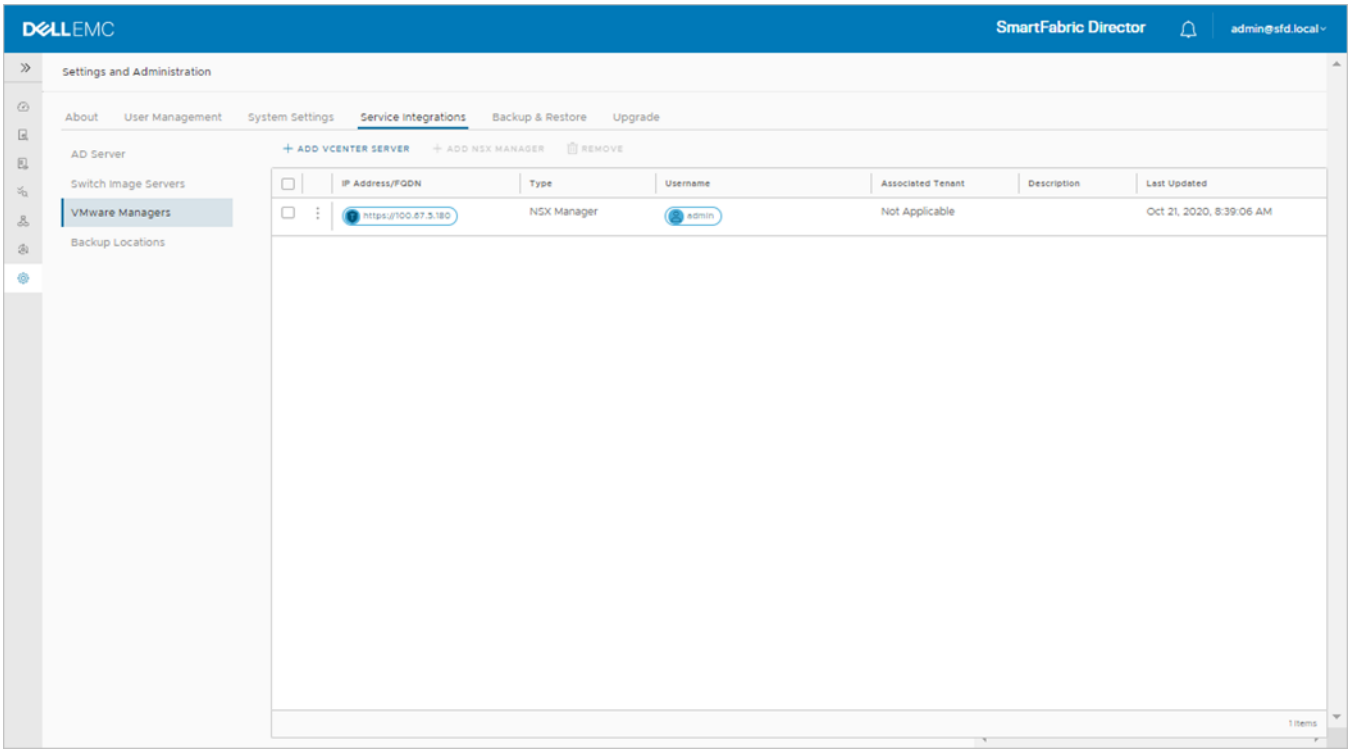
1. Select **Settings and Administration > Service Integrations**, then select **VMware Managers**.



2. Click **Add NSX Manager** to configure integration.



3. Enter the IP address/FQDN, username, password, optional description, then click **Add**.

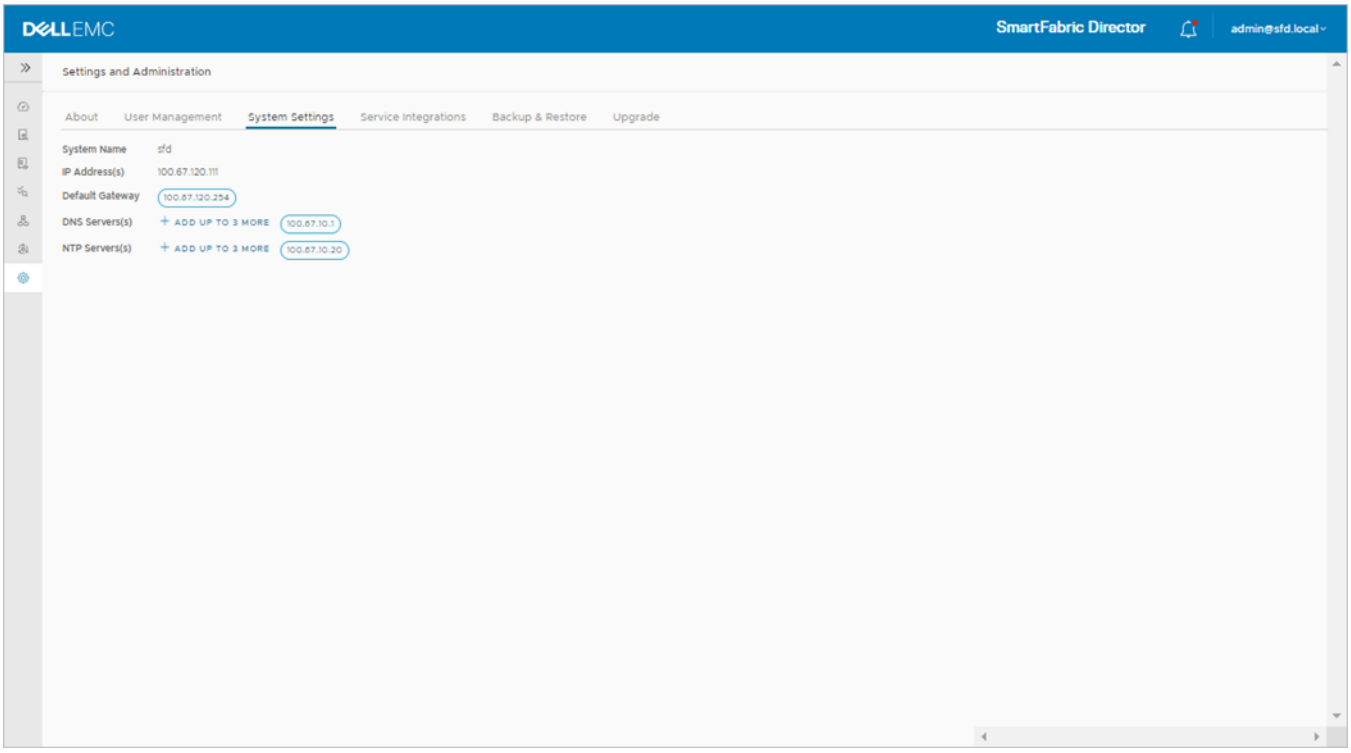


4. (Optional) Select the NSX Manager to delete, then click **Remove** and follow the steps.

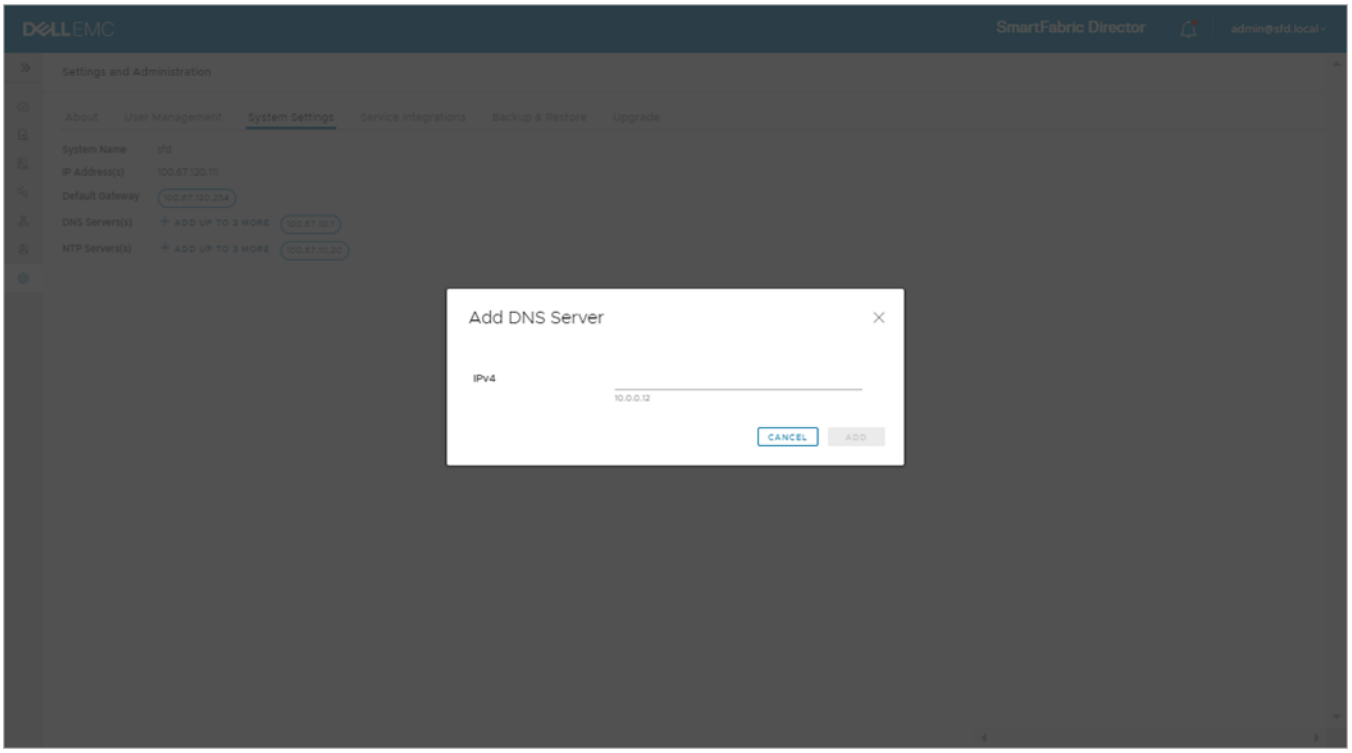
NOTE: If you are using an ESXi host and remove the current VMware Manager, you must add a new connection to SFD.

Add additional DNS or NTP servers

1. Select **Settings and Administration > System Settings**.



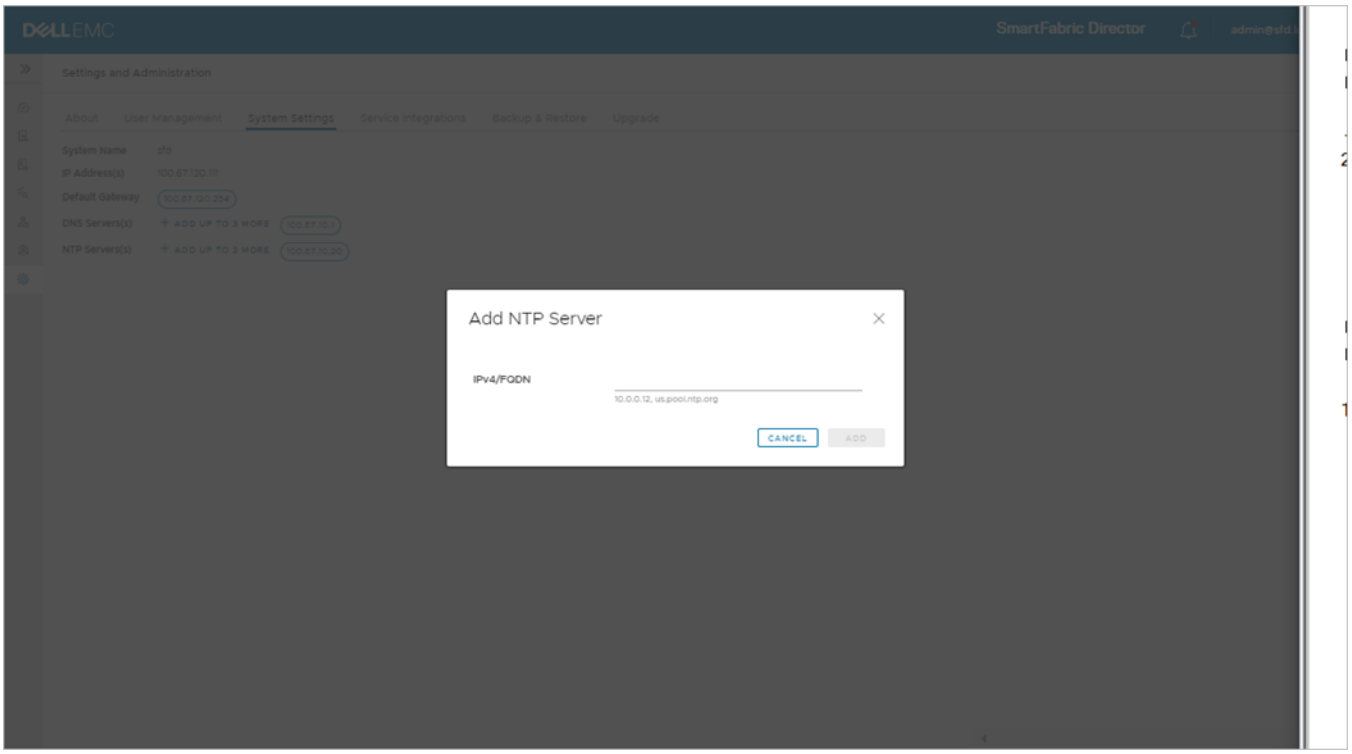
2. (Optional) Click **Add up to 3 more** to add additional DNS servers, enter the **IPv4 address**, then click **Add**.



NTP server

The NTP server was adding and configured on the switch during VM deployment (see Installation using vCenter 6.7). Use these steps to add or modify the NTP server after installation.

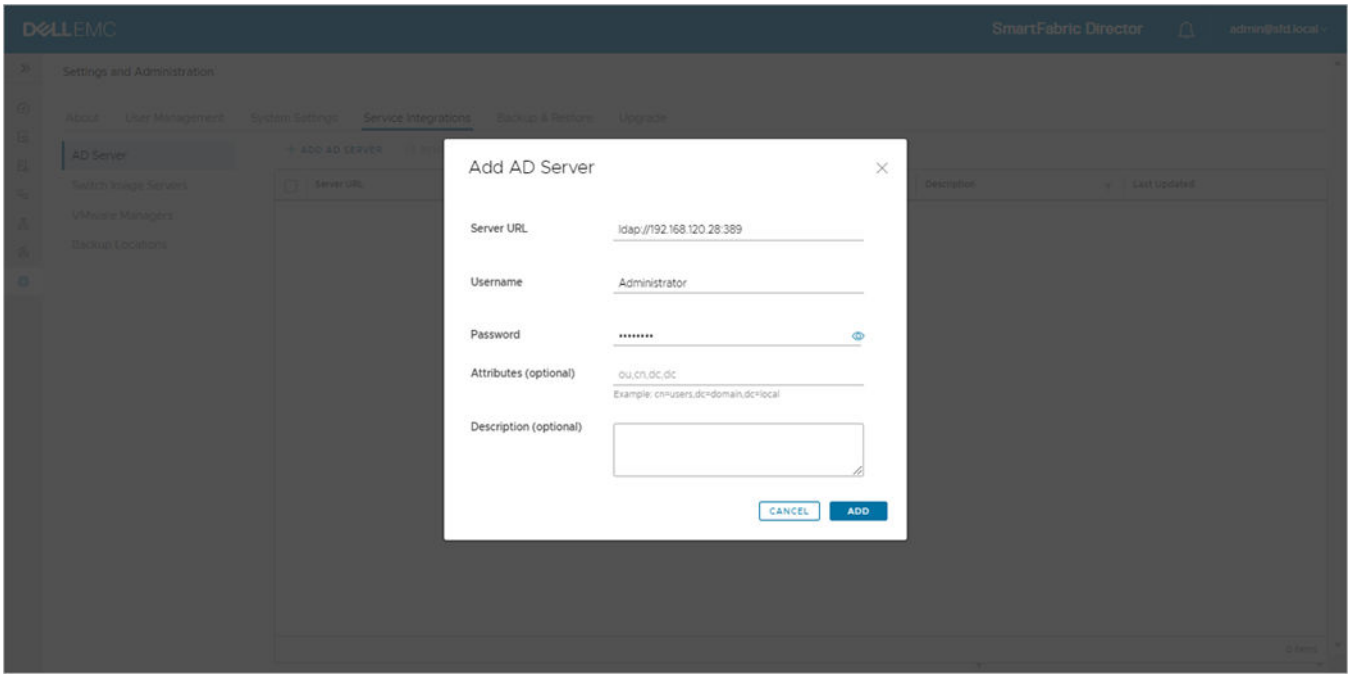
1. Select **Settings and Administration > Service Integrations**.
2. (Optional) Click **Add up to 3 more** to add additional NTP servers, enter the **IPv4/FQDN**, then click **Add**.



Add AD server

NOTE: If you do not set up an Active Directory Server, you must create user accounts.

1. Select **Settings and Administration > Service Integrations**.
2. Select **AD Server**, then click **Add AD Server**.

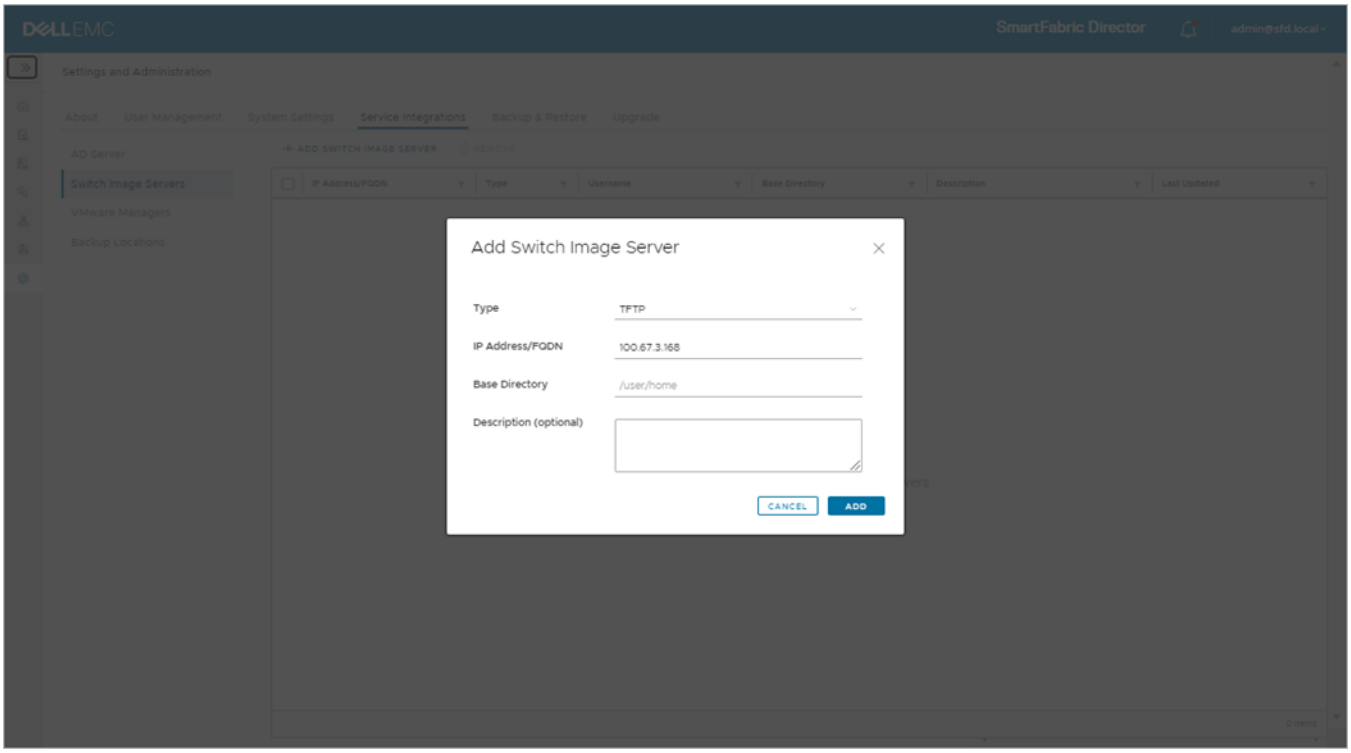


3. Enter the server URL, username (admin), password, optional attributes, and optional description, then click **Add**.

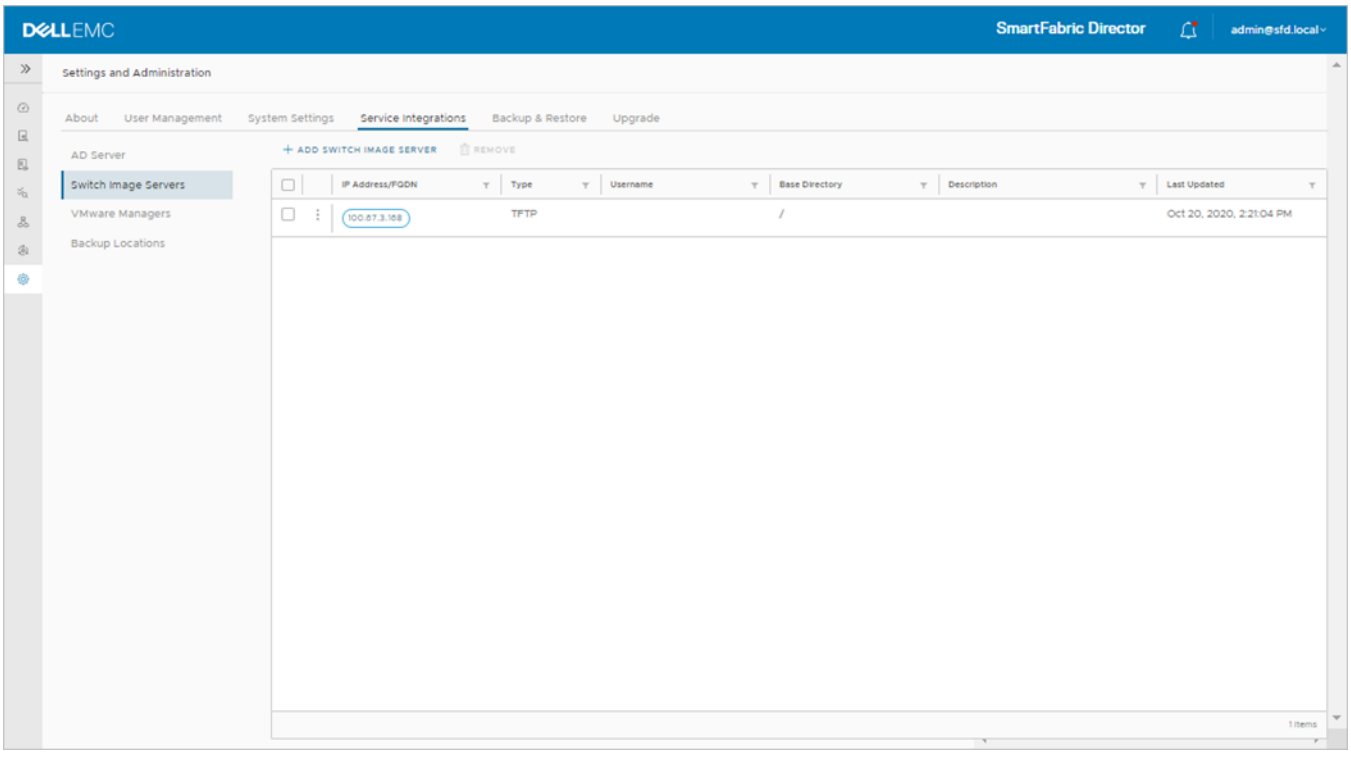
Add switch image server

The image server is where the switch software images are stored. See Download SFD image for more information about how to download a software image.

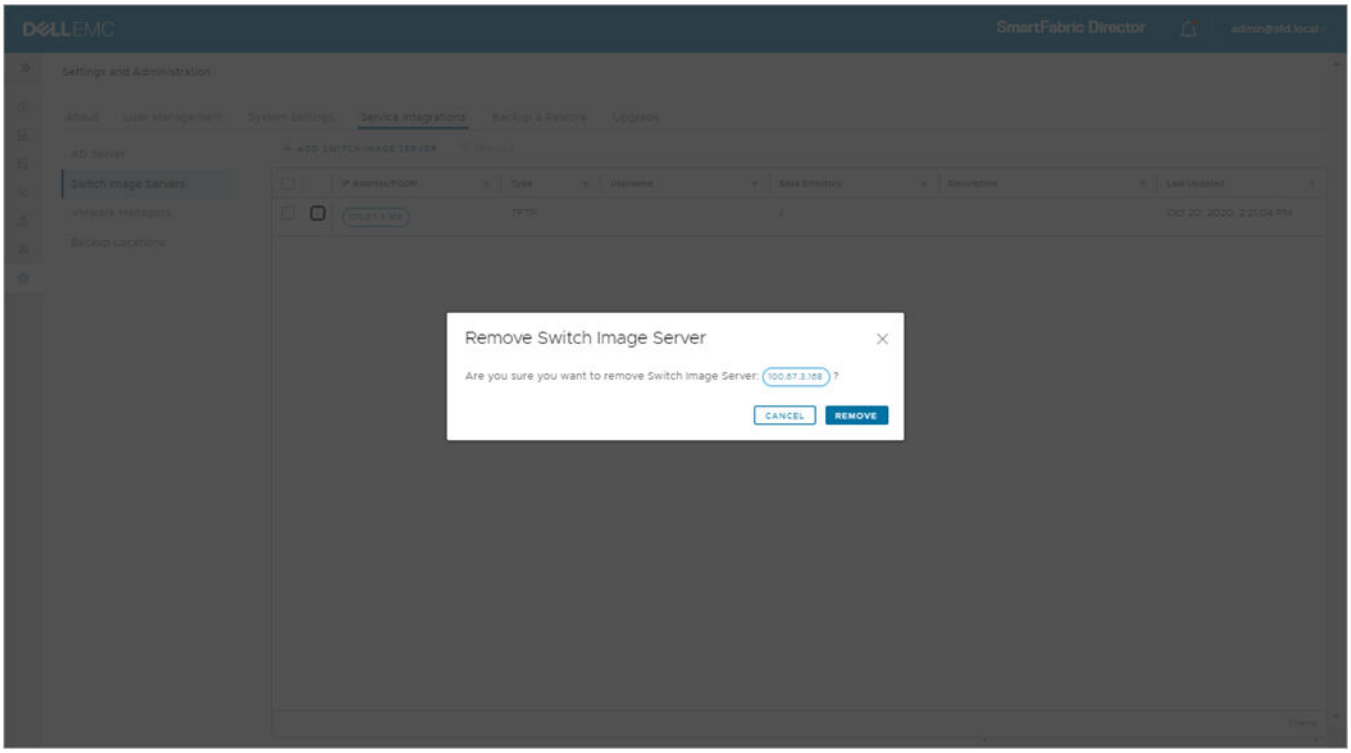
1. Select **Settings and Administration > Service Integrations**.
2. Select **Switch Image Servers**, then click **Add switch image server**.



3. Select the image transport type (TFTP, FTP, SFTP, SCP or HTTP), enter the IP address/FQDN, enter the username and password, enter an optional description, then click **Add**.



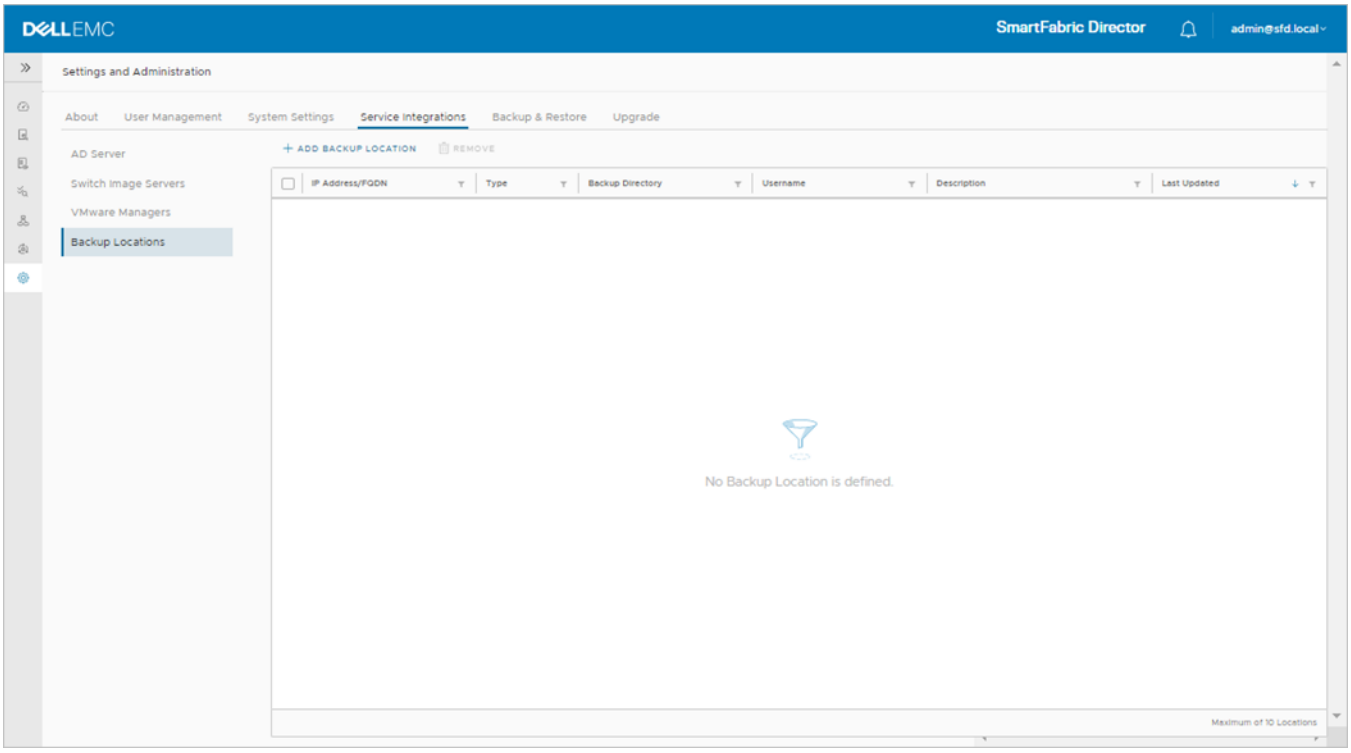
4. (Optional) Select the switch image server, click on the three dots, select **Remove** and follow the steps. You can also select **Edit** to modify the settings for the switch image server.



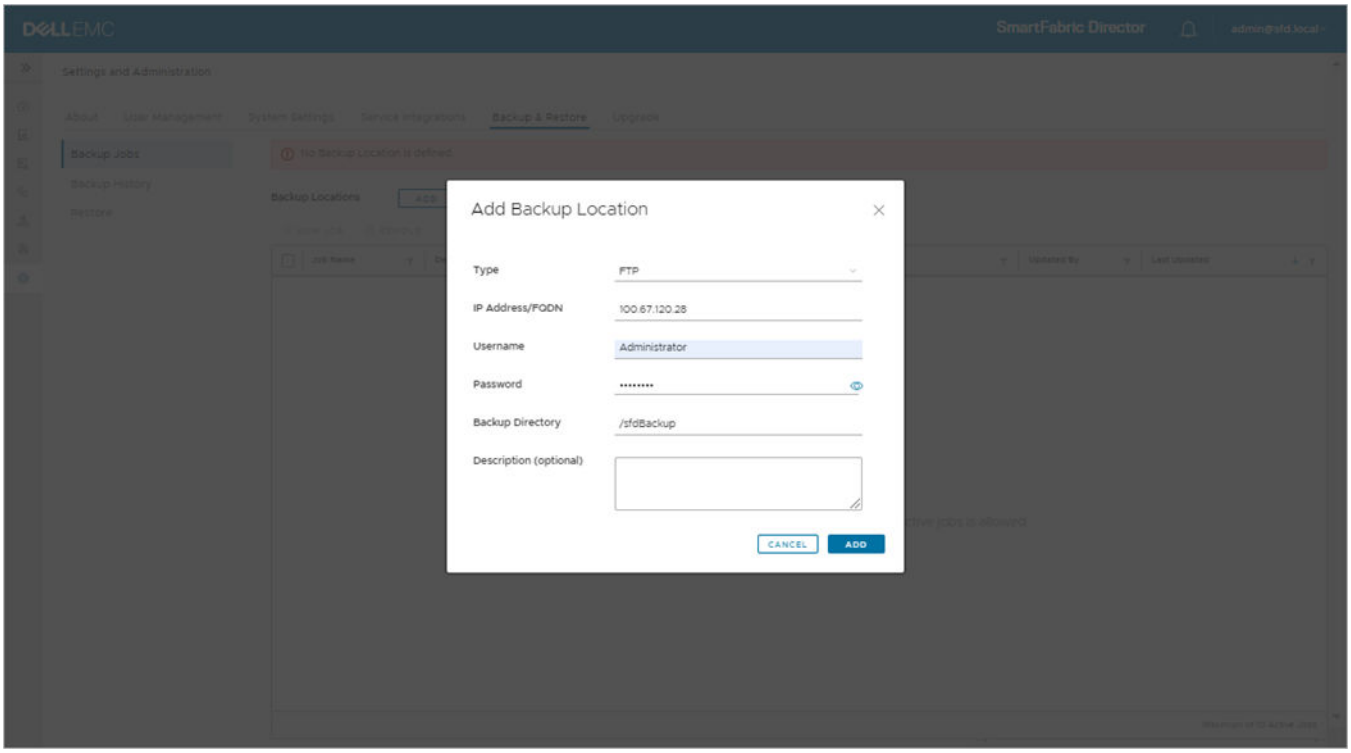
Add backup location

For a new installation, you must first add a backup location before you can schedule backups.

1. Select **Settings and Administration > Service Integrations > Backup Locations**.

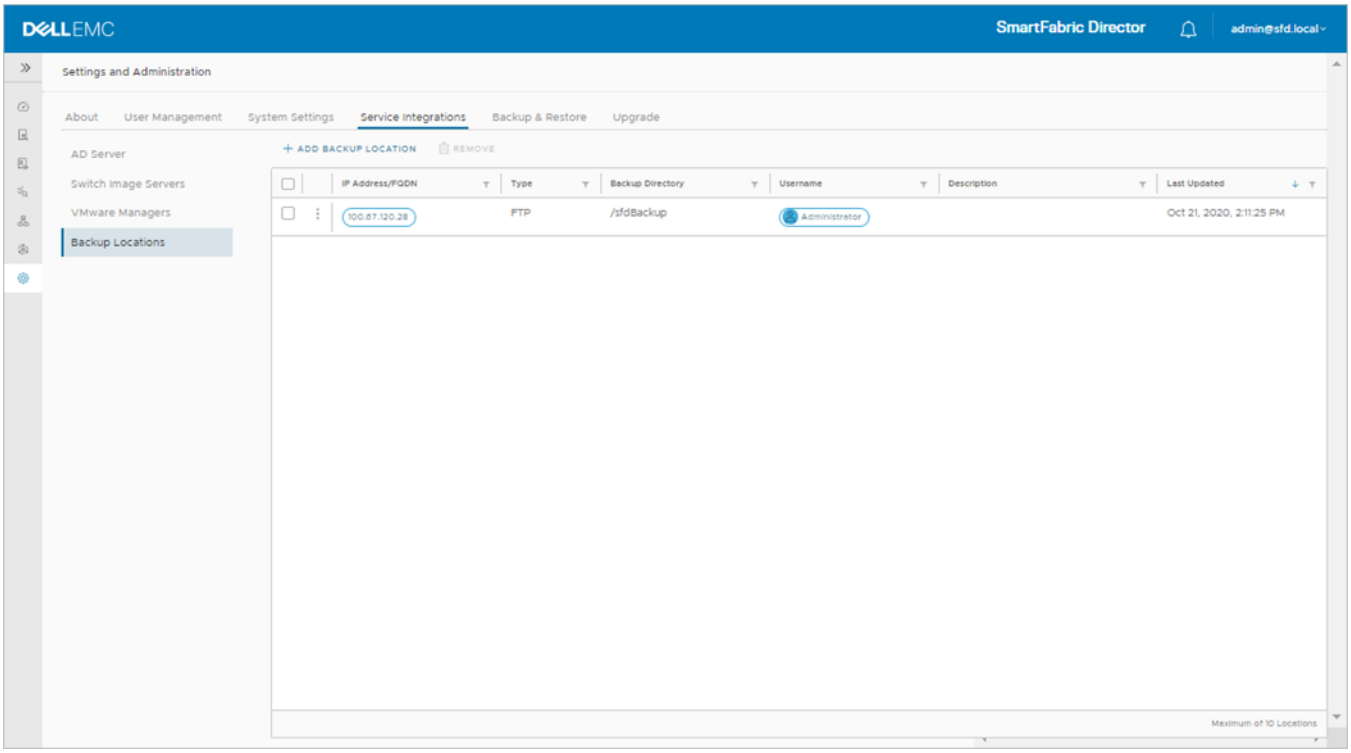


2. Click **Add backup location**.
3. Select the backup type (FTP or SFTP), IP address or FQDN, username and password, optional description, then click **Add**.



The new backup location is added. Click on the three dots to edit or remove a backup location.

NOTE: You cannot remove a backup location if backup jobs are connected to the location. You must first remove the backup jobs, then you can remove the backup location.

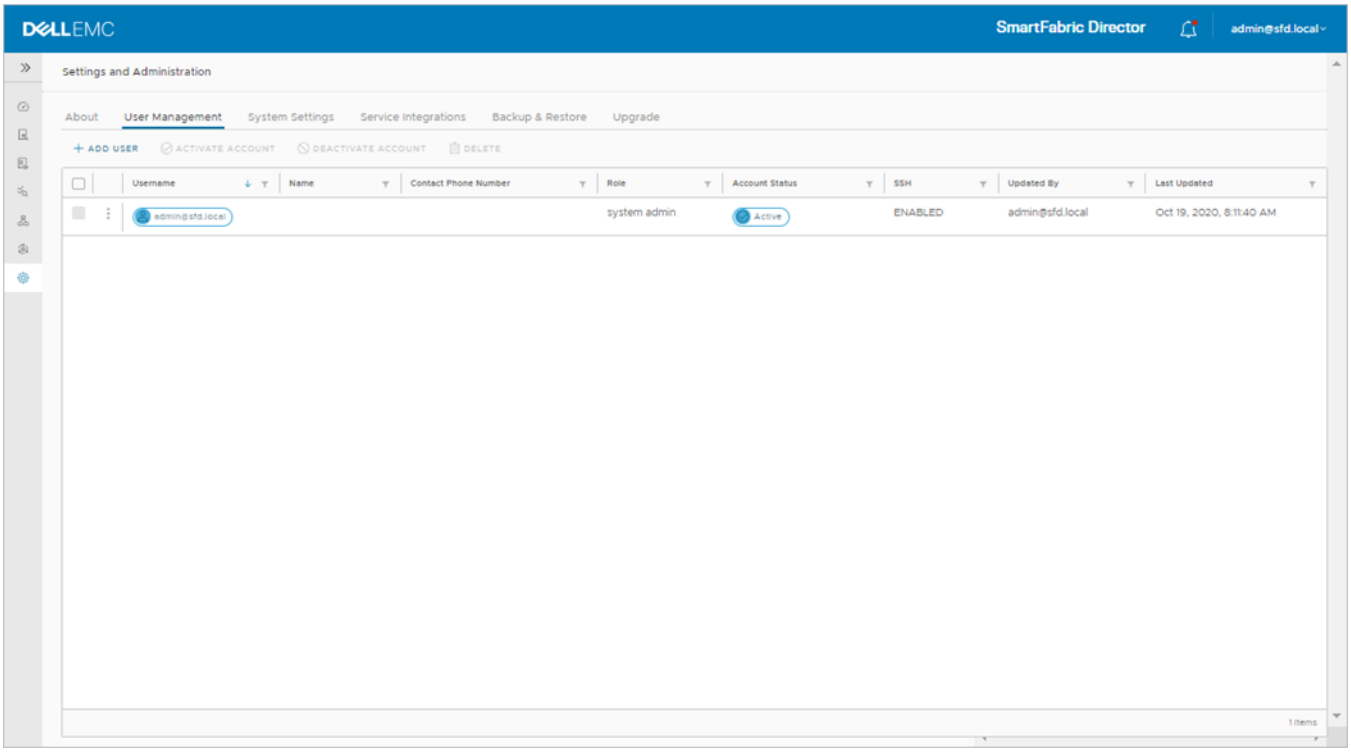


Create user accounts

This information describes how to add user accounts to SmartFabric Director. You can add local users through SmartFabric Director, or you can use the Active Directory Server. You can enable or disable SSH access for a local user, activate or deactivate, and remove a local user.

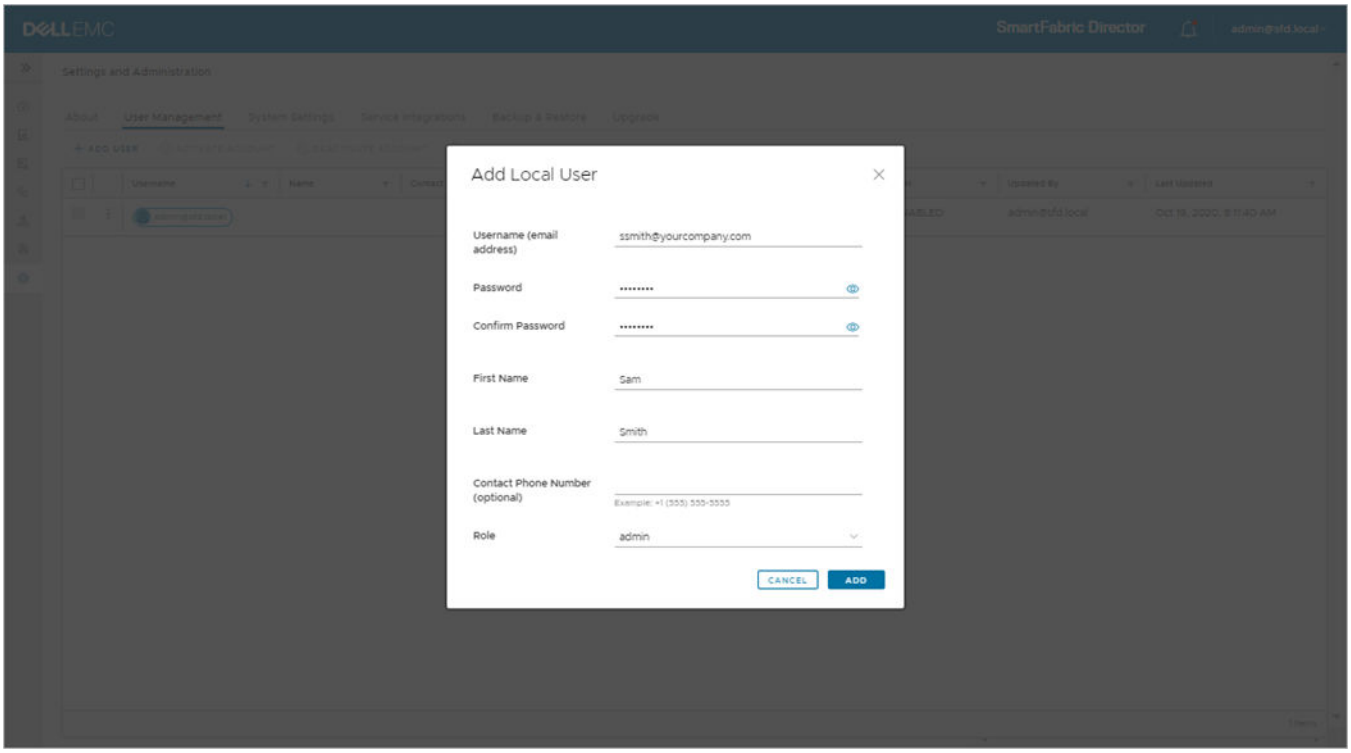
NOTE: If you have setup an Active Directory Server, you do not need to add local users. Skip to Using SmartFabric Director.

1. Select **Settings and Administration > User Management** to add local users.



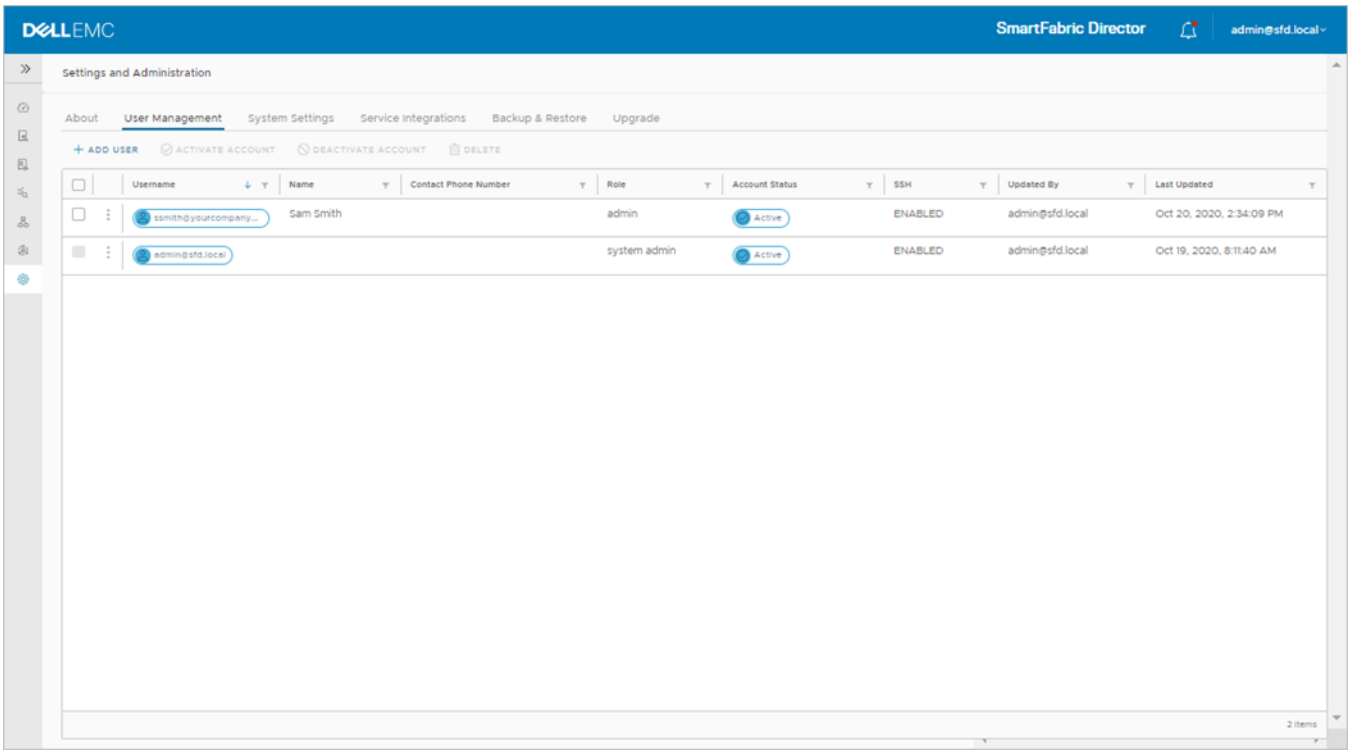
2. Click **Add user**, enter the user email address (username), password twice, first and last name, optional phone number, then click **Add**.

   NOTE: Each new local user has admin role privileges automatically, and SSH status is enabled by default. Ampersand (&), percent (%), greater than (>), less than (<), and single quote (`) are not allowed in user names.

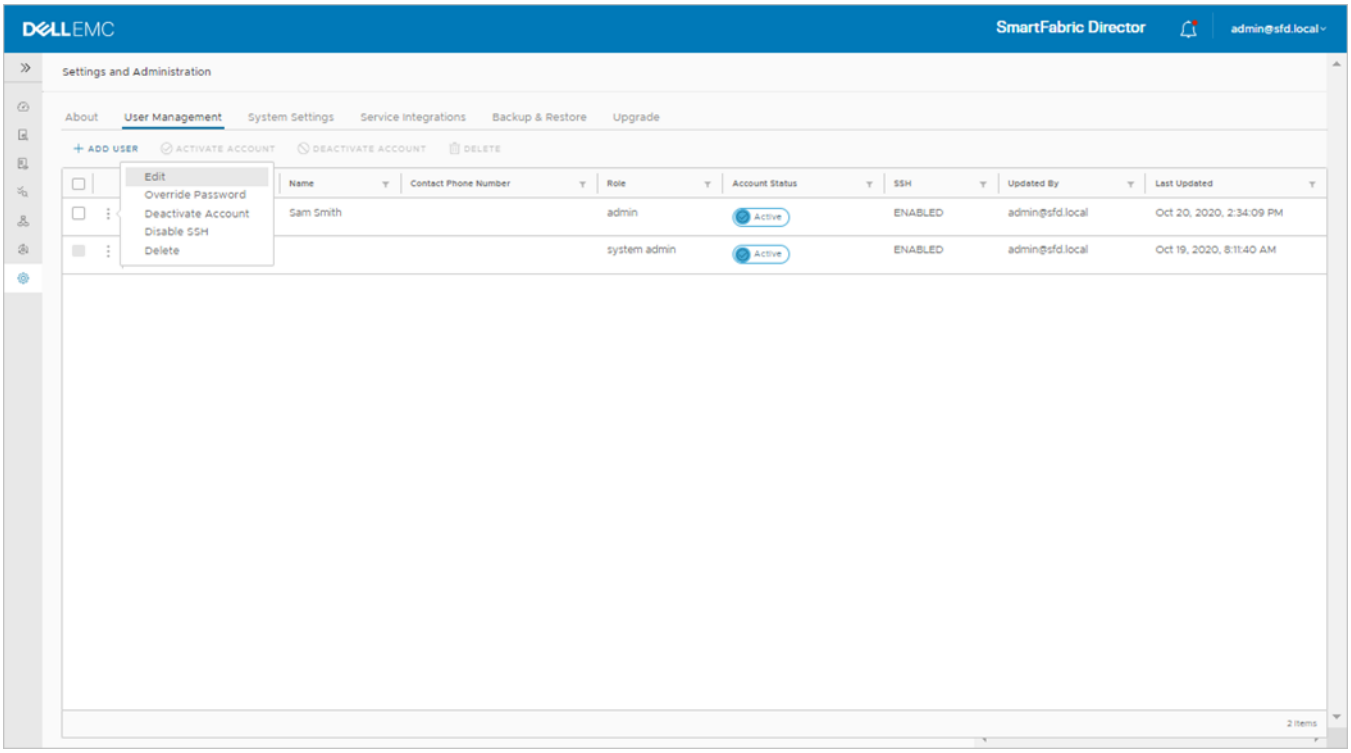


The new user is added. Note that the new user's role is admin, while the administrator has the system admin role.

NOTE: There can only be one system admin role.

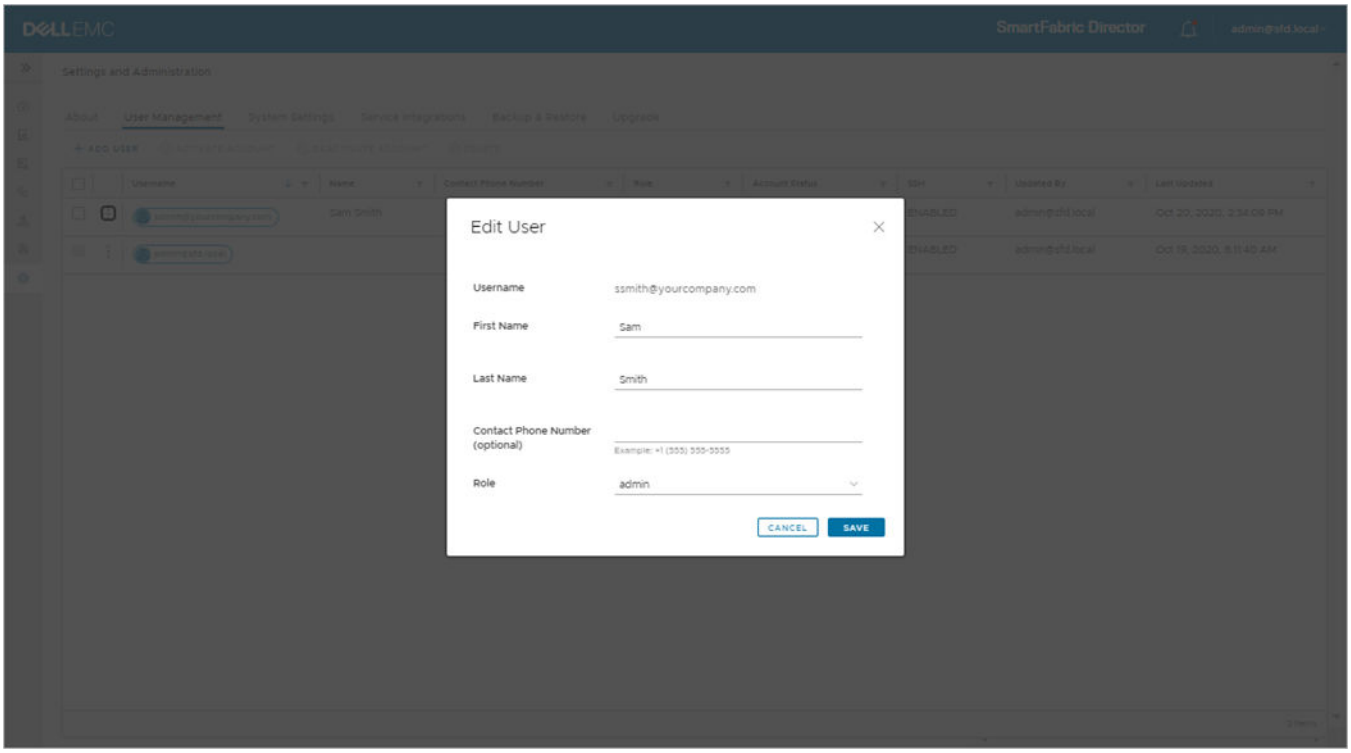


3. (Optional) Continue adding new users, or select a user then click on the three dots to view the available options.



Edit user

1. Select the user name, click on the three dots, then select **Edit**.

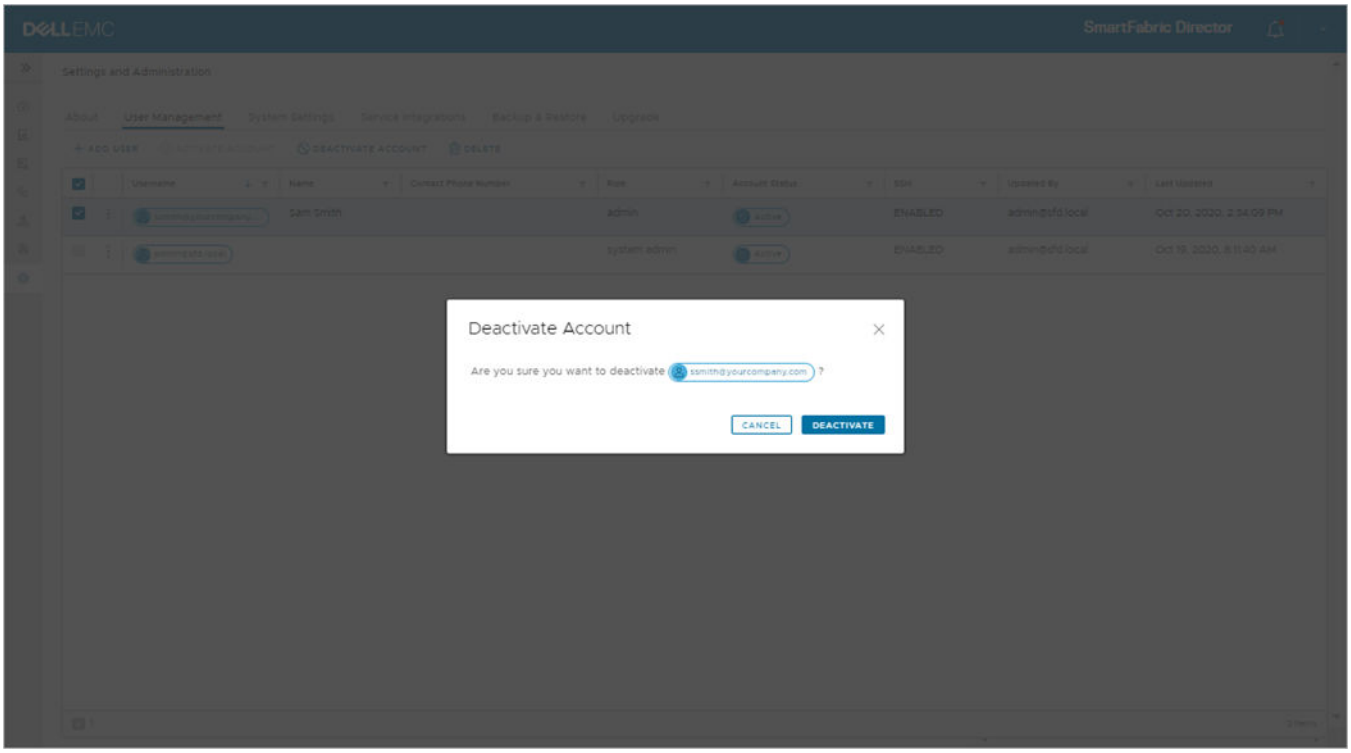


2. Make changes, then click **Save**.

Deactivate account

You may want to deactivate an account of a user leaves your company.

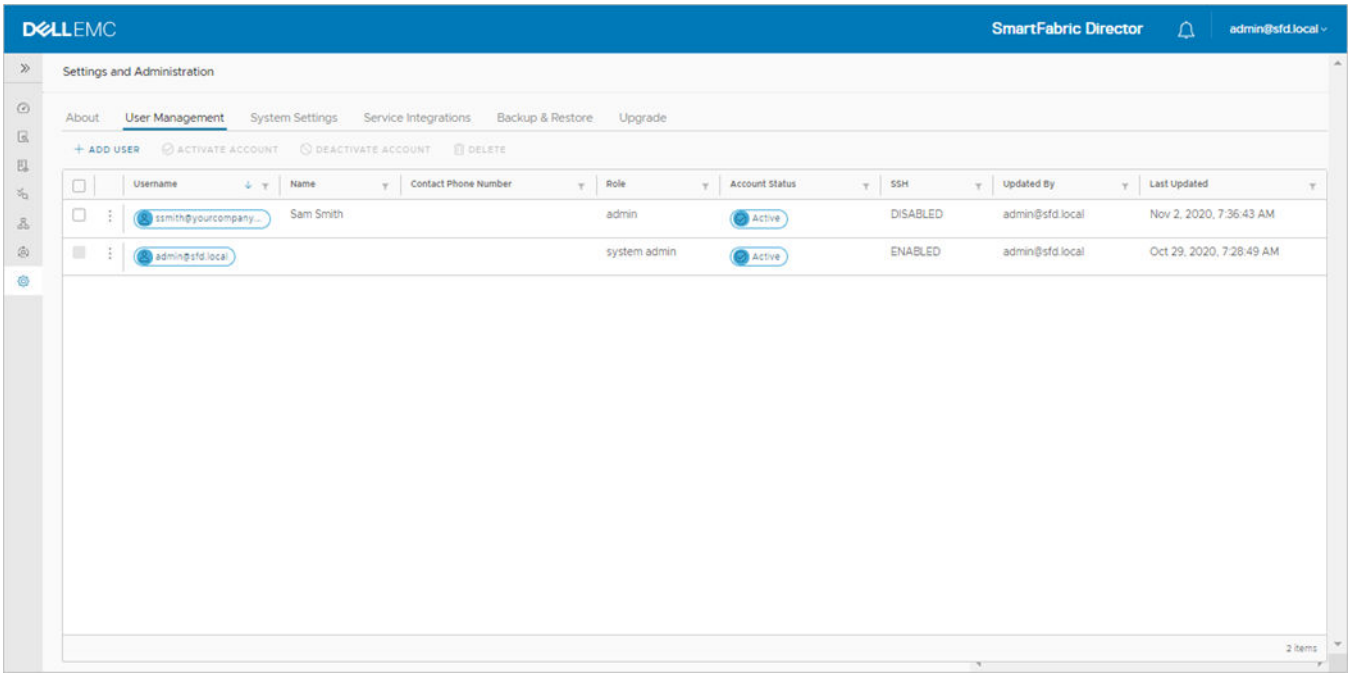
1. Select the user name, click on the three dots, then select **Deactivate account**.
2. Click **Deactivate**.



Disable SSH

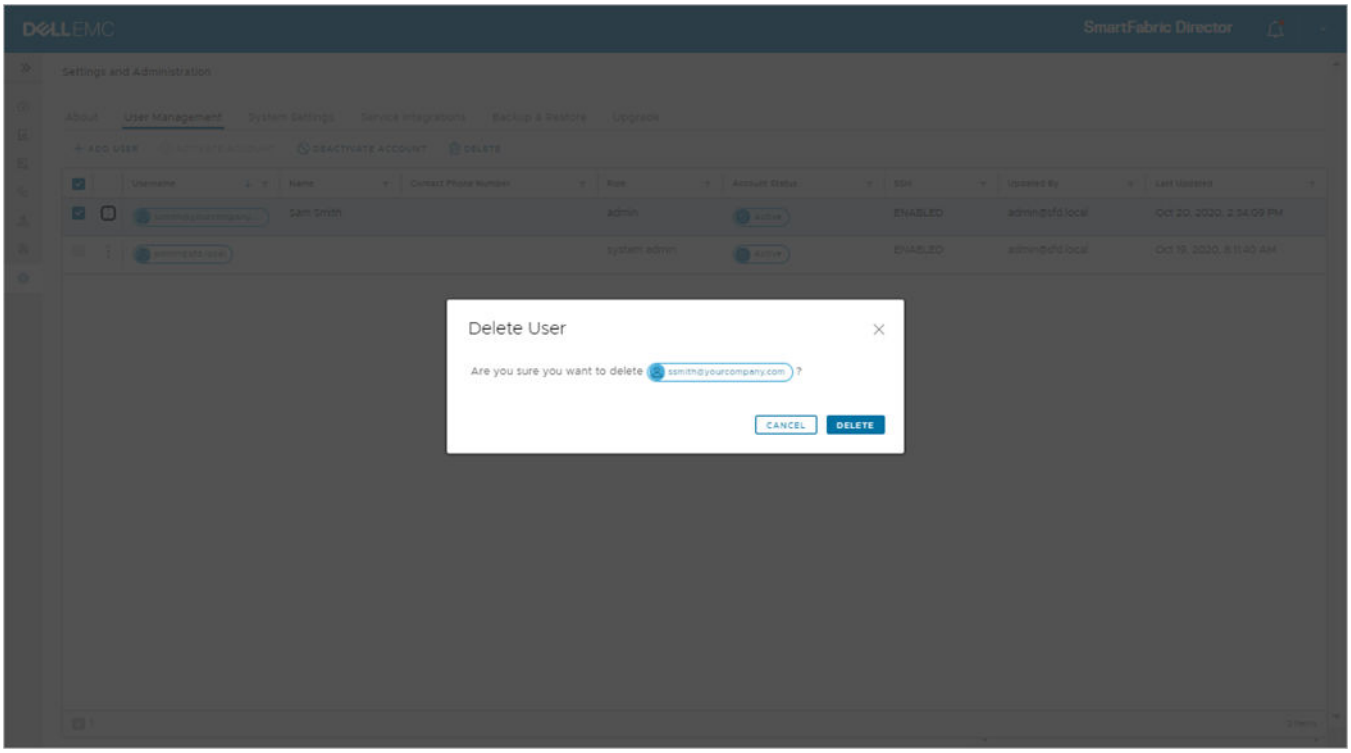
NOTE: SSH is only for remote access to the console. Disable SSH to prevent access to the console through SSH.

1. Select the user name, click on the three dots, then select **Disable SSH**.
2. Click **Disable SSH**.



Delete user

1. Select the user name, click on the three dots, then select **Delete**.



2. Click **Delete**.

7

Using SmartFabric Director

This information describes how to build, define, and deploy a data center SmartFabric. After completion of the SFD bootstrap and integration into your data center network operations, you are now ready to build, define, and deploy a SmartFabric. The steps outline a deployment where the operator specifies the SmartFabric for the first time, starting with a clean state.

Topics:

Import fabric wiring diagram

This information describes how to use the fabric definition screens to import a fabric wiring diagram. Fabric definition describes the switches, their roles (spine, leaf, or edge leaf), and the wiring diagram of how these switches interconnect.

You must specify the reachability information, such as the Management IP and credentials (username and password) of each switch, so that SFD can connect to the switches.

NOTE: The fabric wiring diagram must be edited manually using a text or JSON editor. Using Fabric Design Center enables generation of the JSON file.

It is assumed that the switches have been racked, stacked, and connected as per the wiring diagram. All switches must have the minimum version of SmartFabric Director and OS10.5.2.0P1 installed, along with the base configuration to connect, and communicate through the gNMI and gNOI interfaces. For more information about the base configuration, see Switch configuration.

You must define the role of each switch, and the interface type such as interlink, host, edge facing, or VLT link. It is expected that the switches are wired per the definition in the wiring diagram.

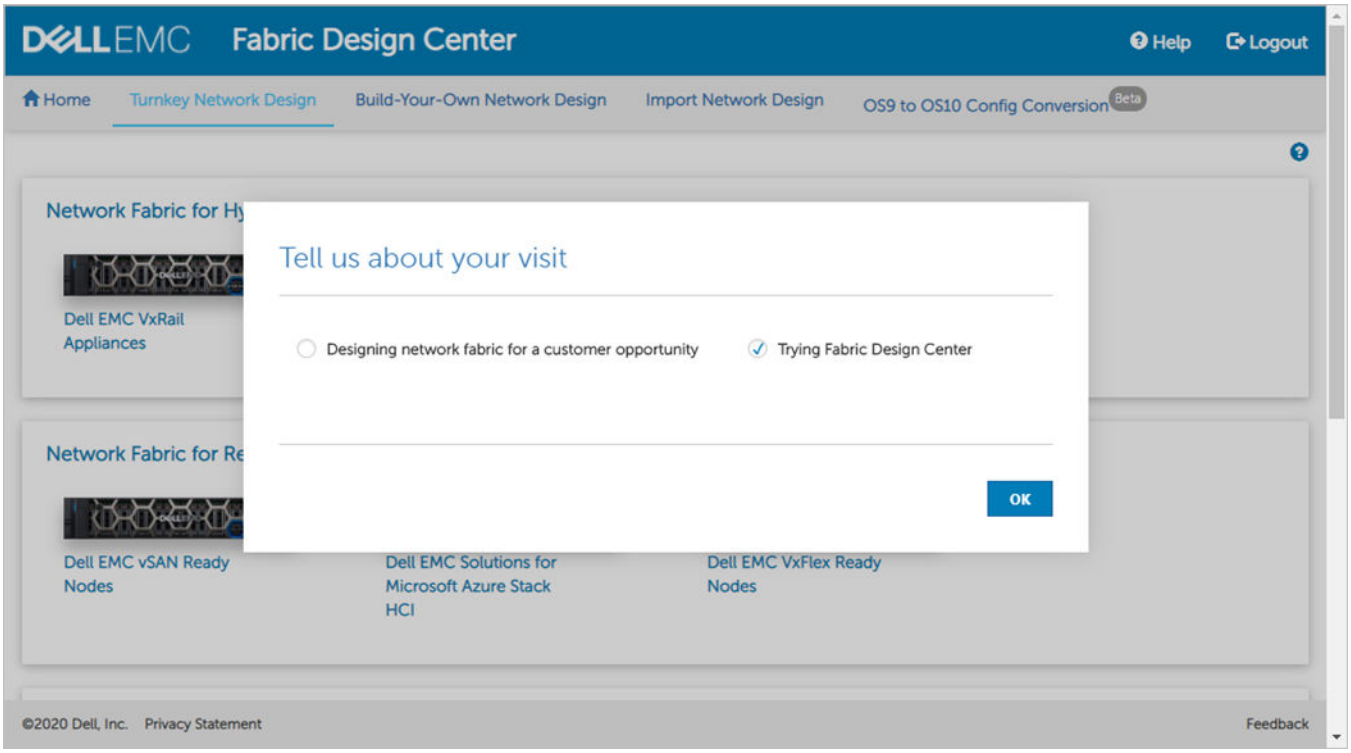
- Interlinks are switch ports that are used to connect a leaf switch to a spine switch
- Host interfaces are switch ports that are connected to host
- Edge interfaces (on an edge leaf) are switch ports that are connected to an external switch

Using Fabric Design Center

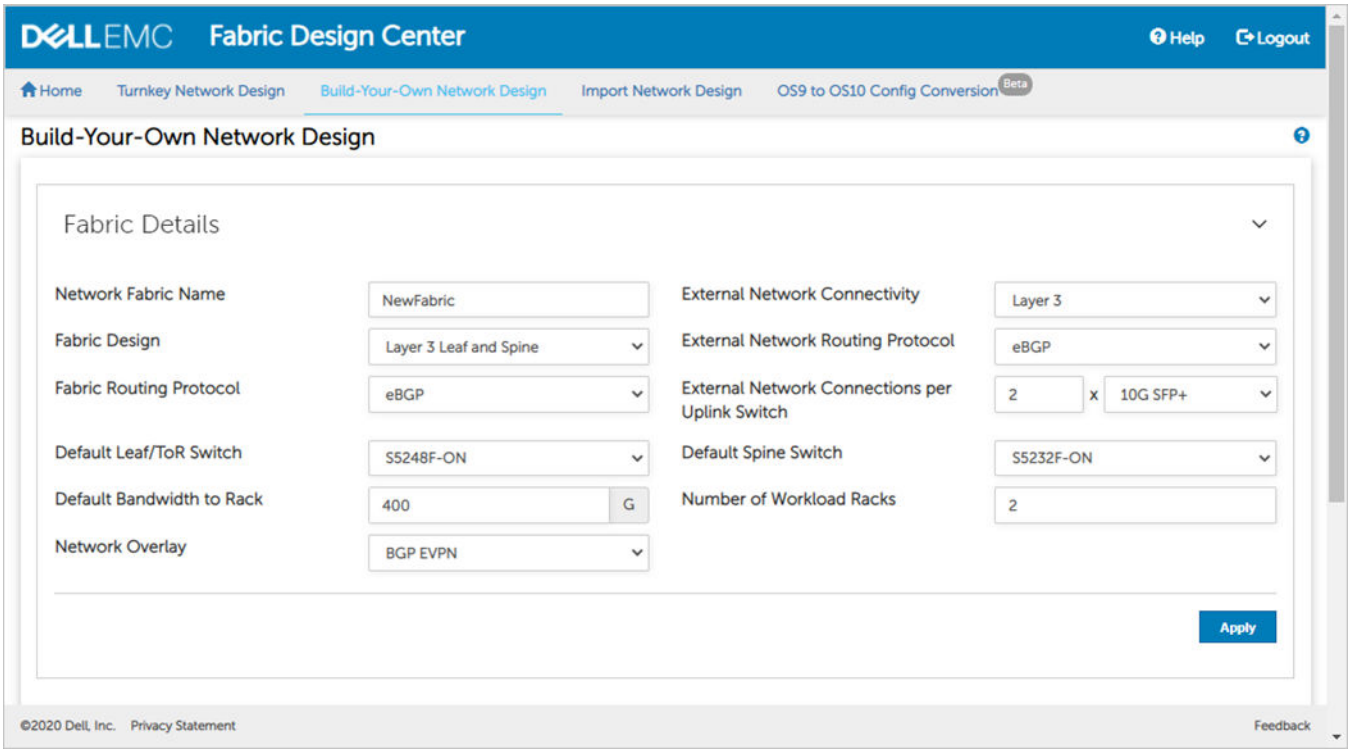
Dell EMC Fabric Design Center allows you to automatically create a JSON file based on your selections. You can import a JSON wiring diagram file through SFD. On reading the JSON file, SFD displays the fabric graph as described in the JSON file. You can download a JSON wiring template from DDL.

NOTE: If you have previously configured the switch, the wiring diagram JSON results generated from FDC may need modifications to work with your switch.

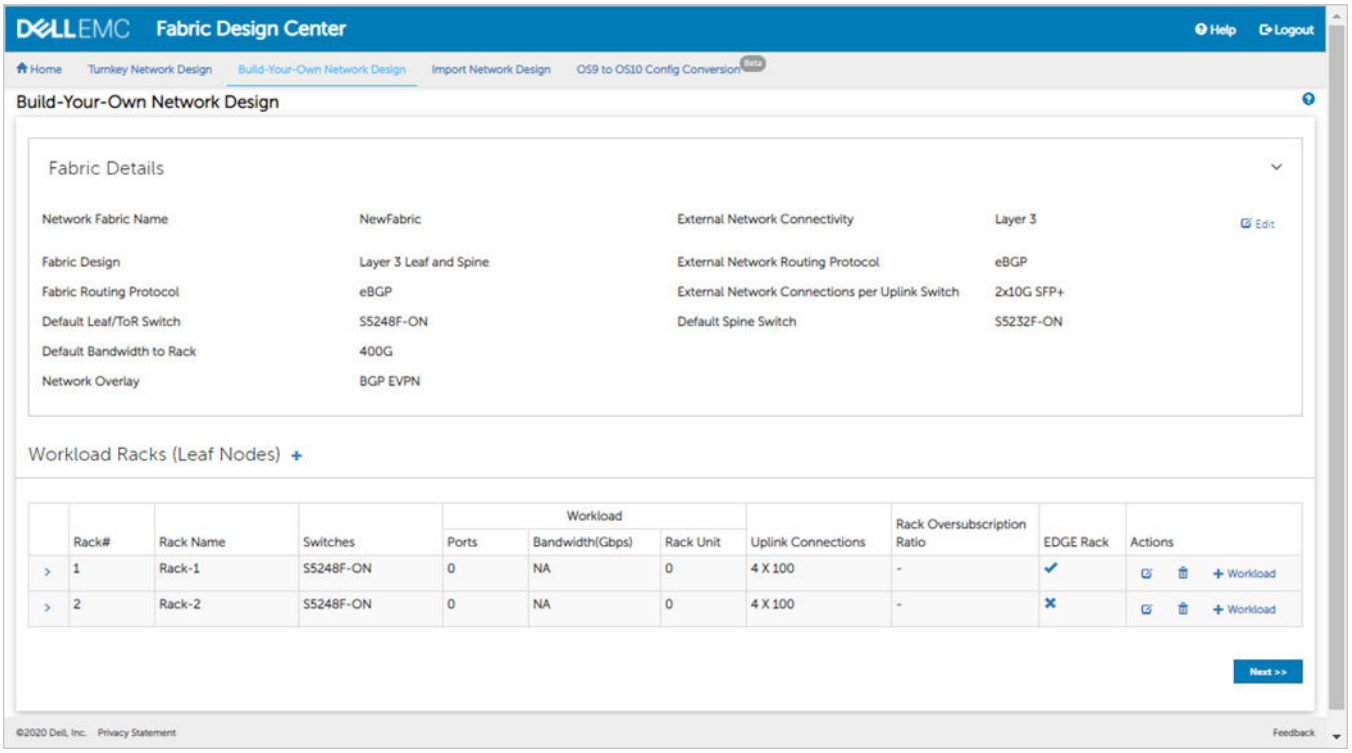
1. Open a browser, then go to fdc.emc.com and log in with your Dell Customer/Partner credentials.
2. Select the checkbox to agree to the terms of use, then click **OK**.
3. Select either *Designing network fabric for a customer opportunity* or *Trying Fabric Design Center*, then click **OK**.



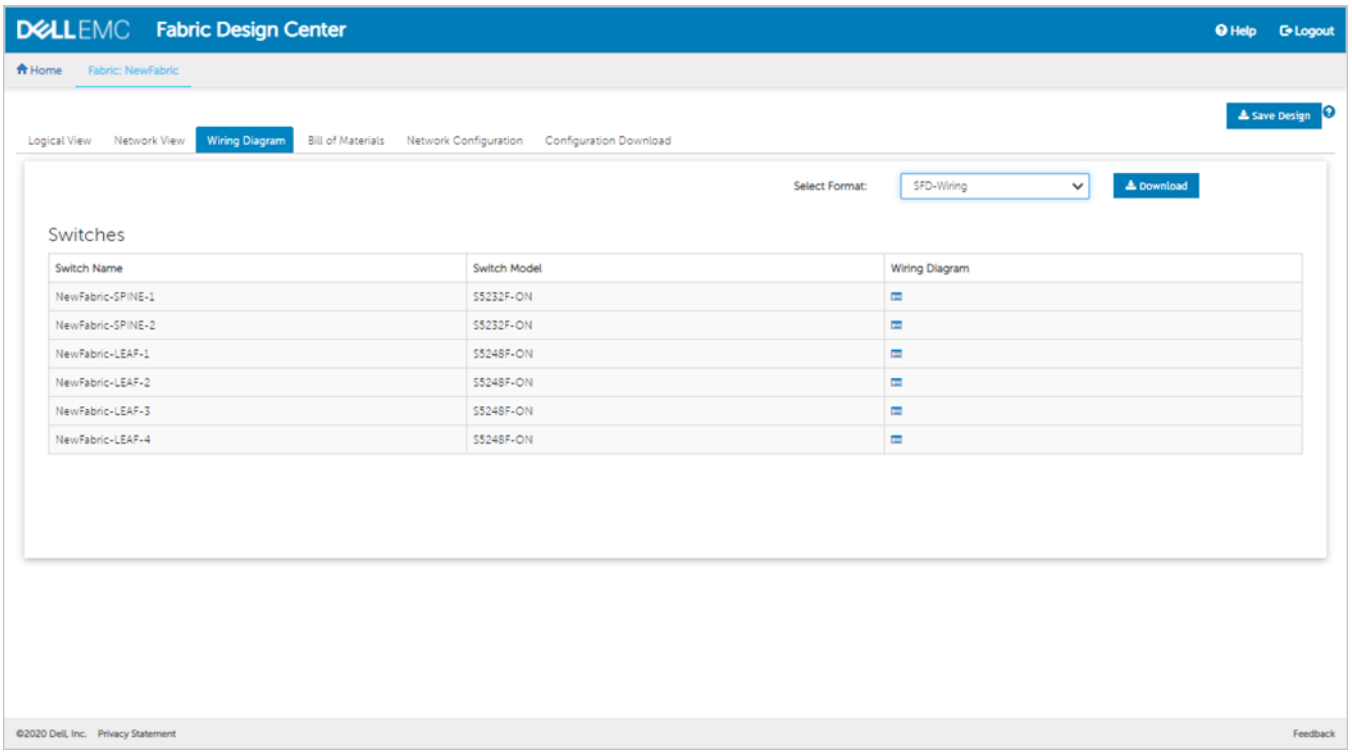
4. Select **Build-Your-Own-Network Design** at the top.
5. Create your Layer 2 or Layer 3 network, then click **Apply**. You can select the number of racks that are needed for the design. The default number of spines is calculated based on the default bandwidth to the rack.



6. Verify the fabric design, then click **Next**. You can also click Edit and make any necessary changes to meet your requirements.



7. Select **Wiring Diagram**, select **SFD-Wiring** for the format, then click **Download** to save the JSON file for importing into SFD.



8. Click **Save** to save the file for import into SFD.

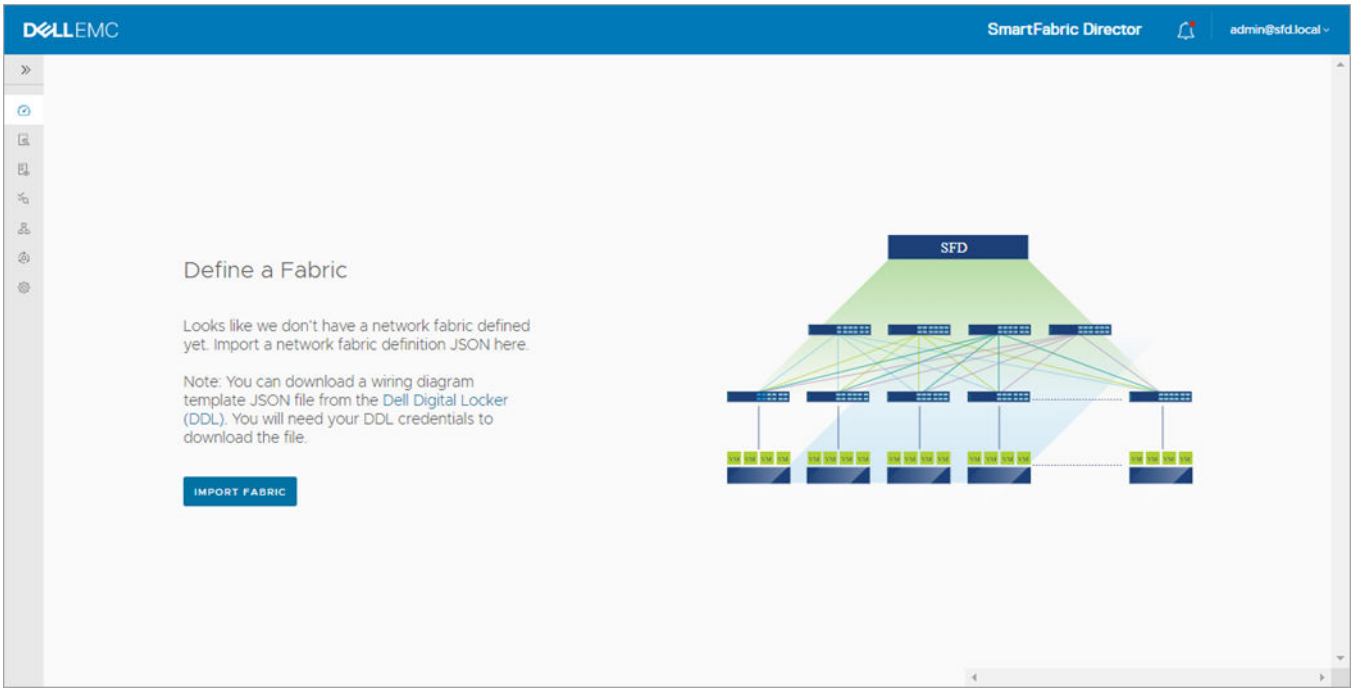
For complete information, see the *Dell EMC Fabric Design Center User Guide*.

Import a wiring diagram

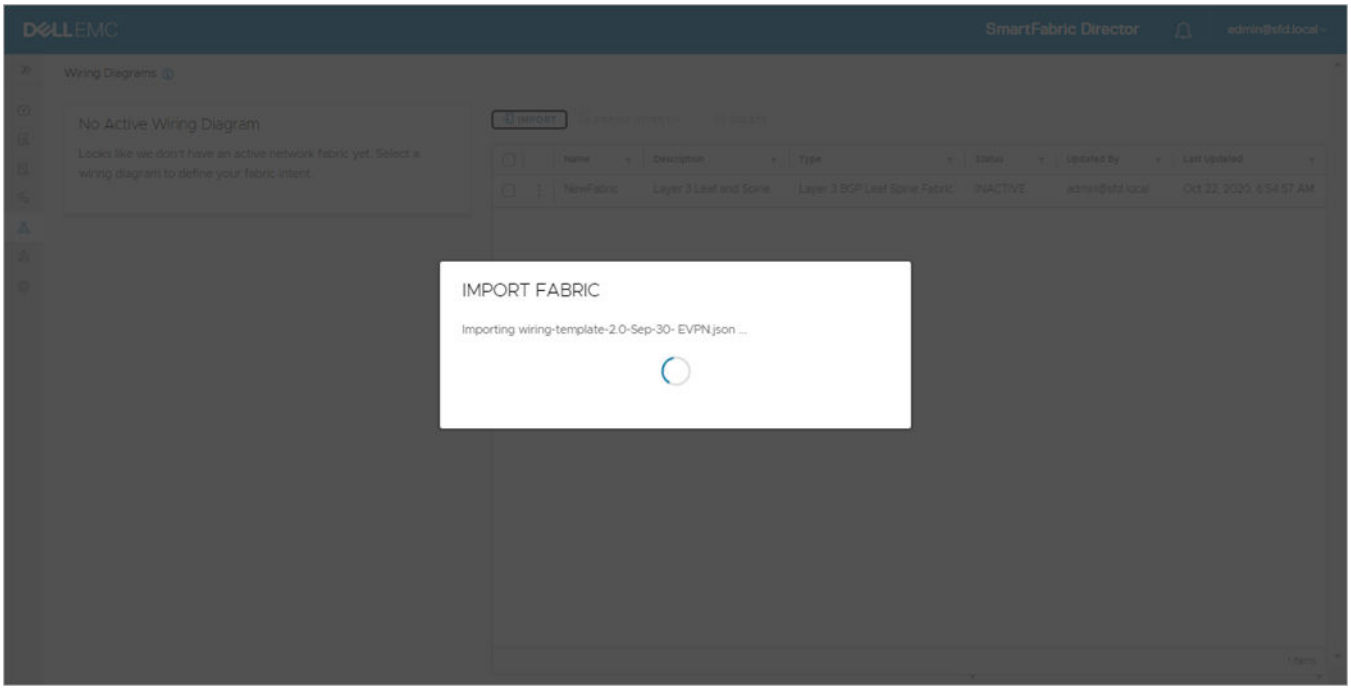
You can import a JSON wiring diagram file through SFD. On reading the JSON file, SFD displays the fabric graph as described in the JSON file. You can download a JSON wiring template from DDL .

NOTE: Once the JSON file is imported or activated, any active intent of the fabric is no longer valid, and a new intent must be defined and submitted for approval.

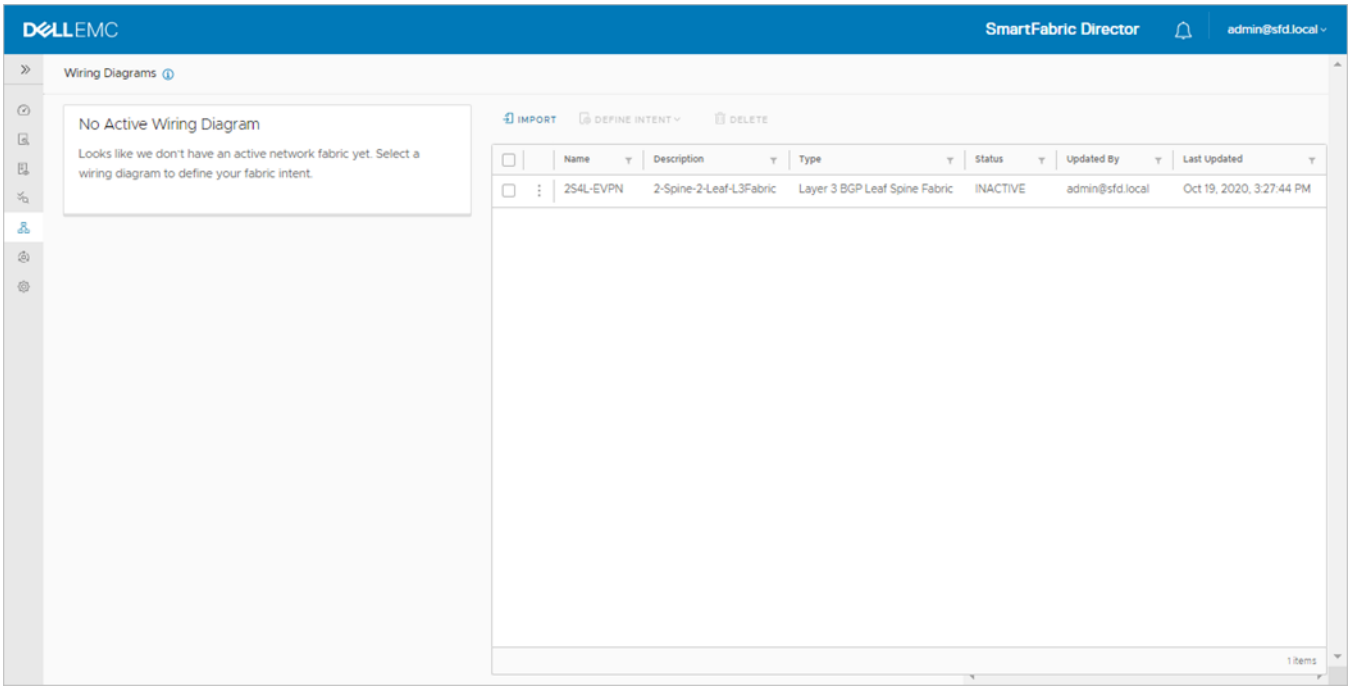
1. Click **Import Fabric** from the dashboard or **Wiring Diagrams > Import**.



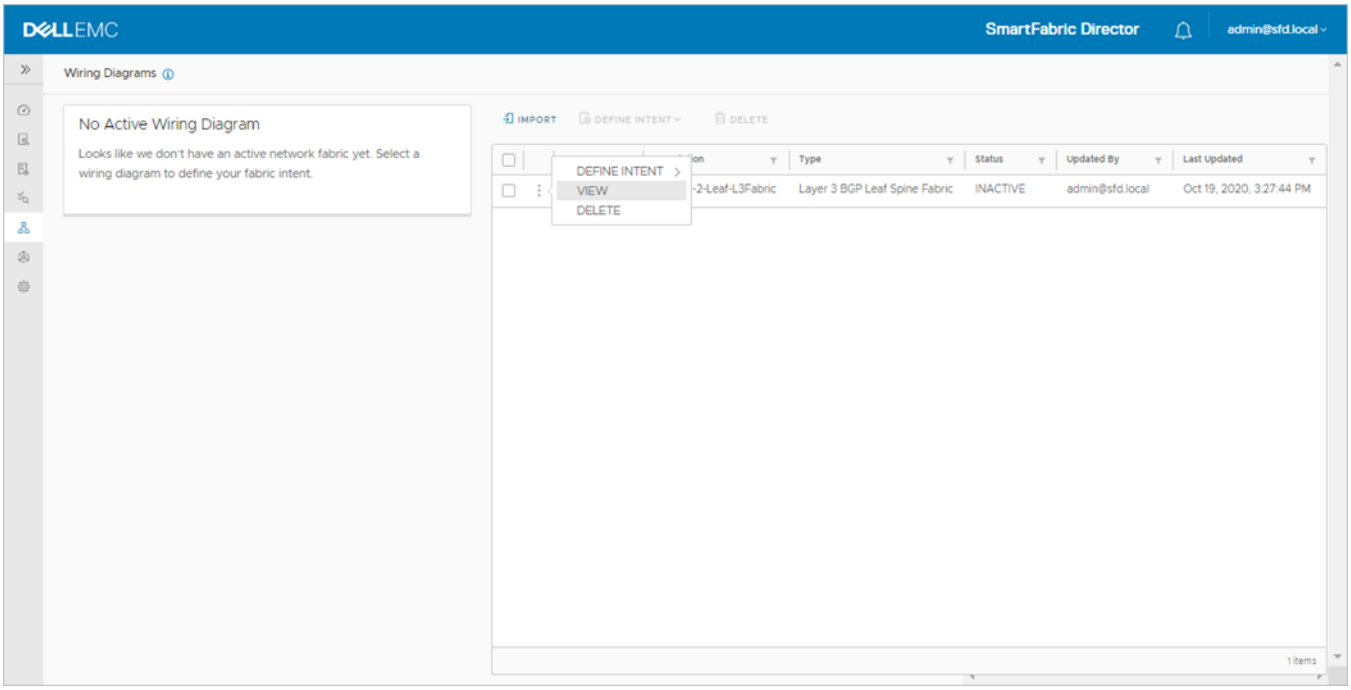
2. Go to where you saved the file, then select the JSON file to import.



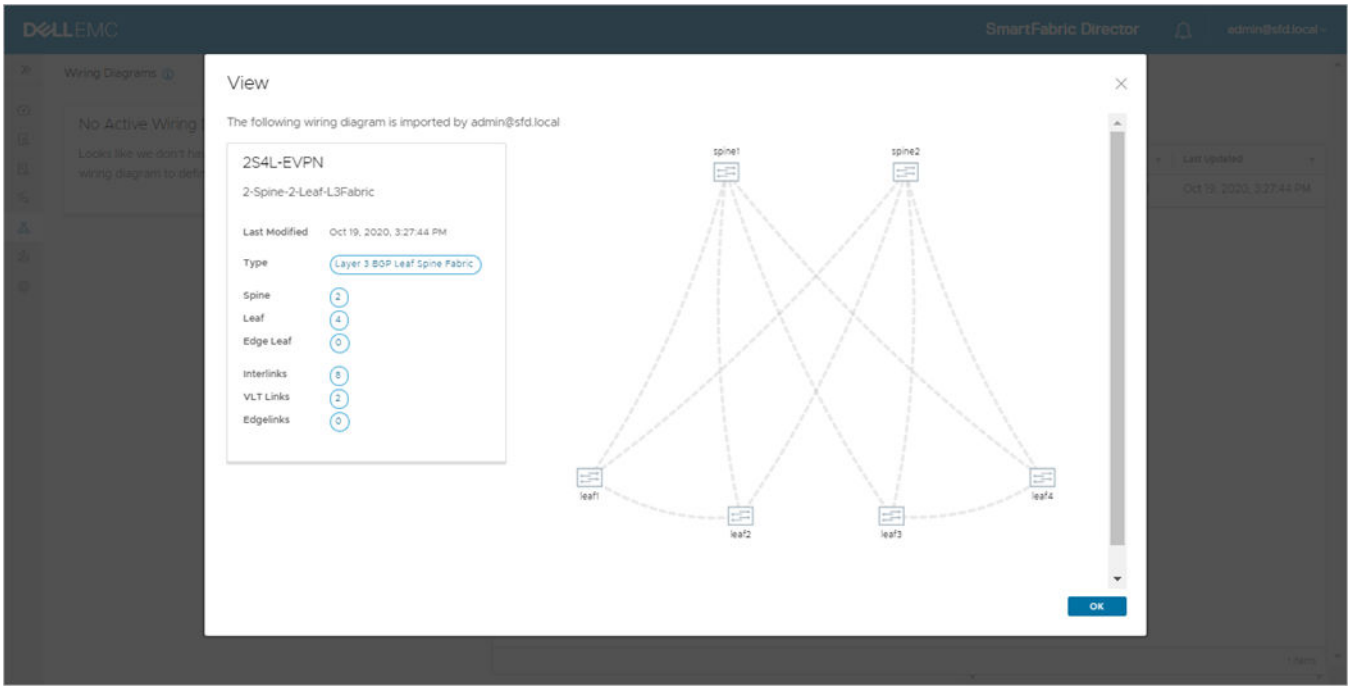
Wiring import success.



3. Select the fabric intent, click the three dots, then select **View** to display the wiring diagram.



4. Click **OK** to close the wiring diagram.



Fabric intent configuration

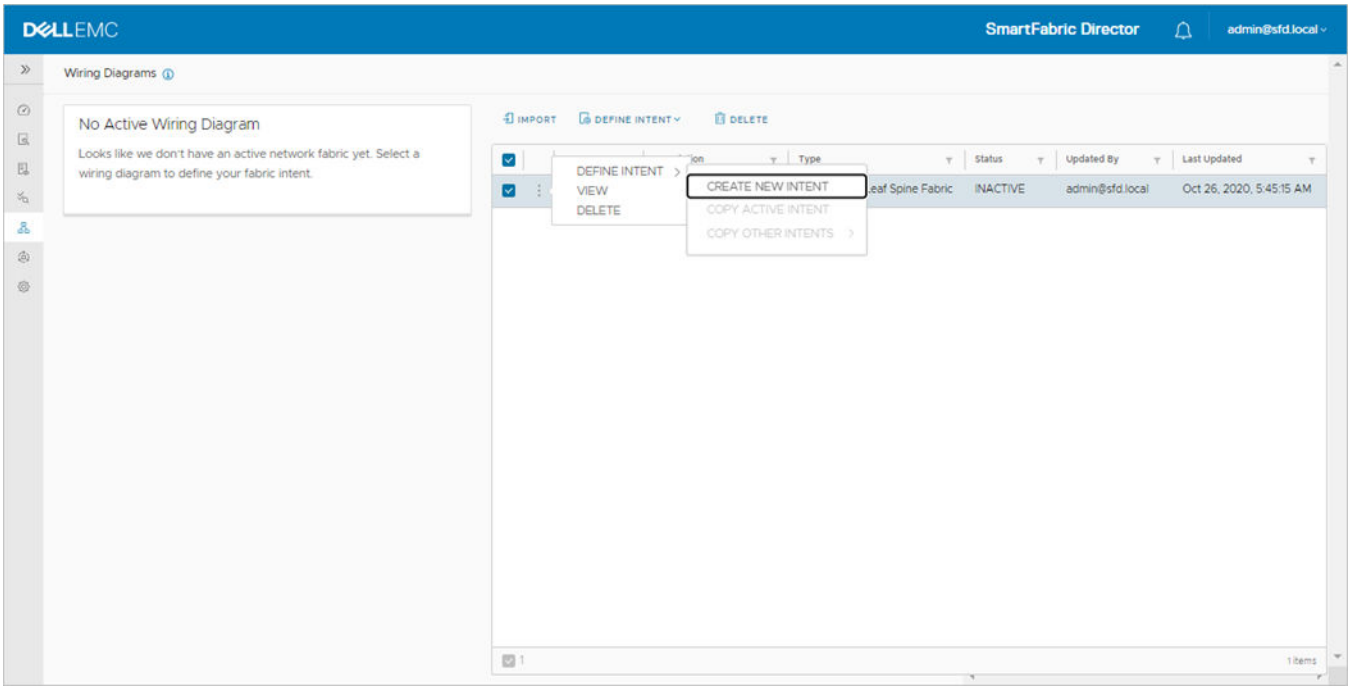
This information describes how to define a fabric intent, approve the fabric intent, then deploy it. You can either import a previously defined fabric intent or start a new one from scratch.

Layer 3 BGP leaf spine fabric

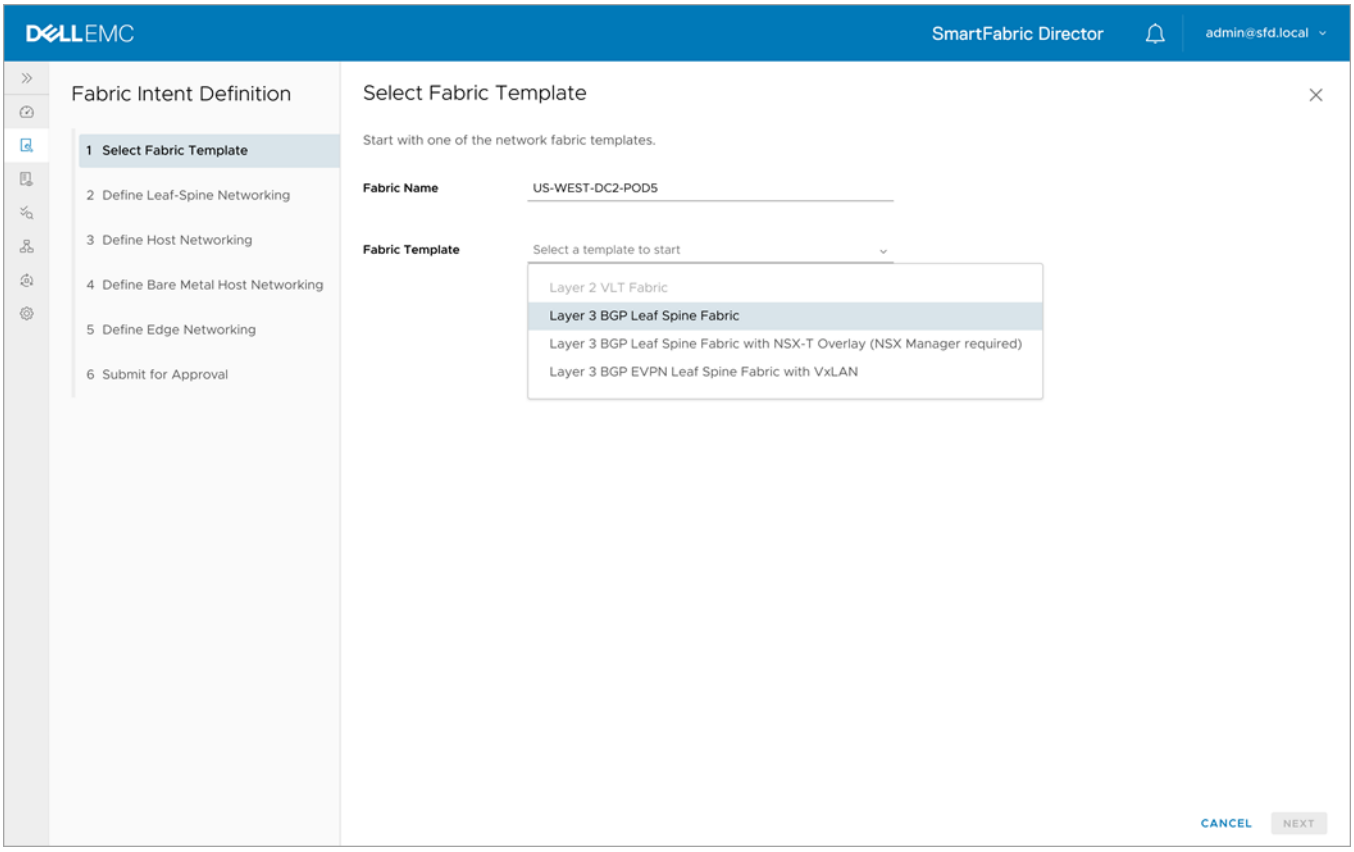
In SFD fabric intent definition, you can specify the fabric type as *Layer 3 BGP leaf spine fabric* to enable step-by-step guidance to operationalize BGP EVPN fabric.

Select fabric template

1. Select the fabric, click on the three dots, then **Define intent > Create new intent**. If modifying an active intent, make a copy of an intent from the table of intents (active or otherwise), then make the necessary changes.

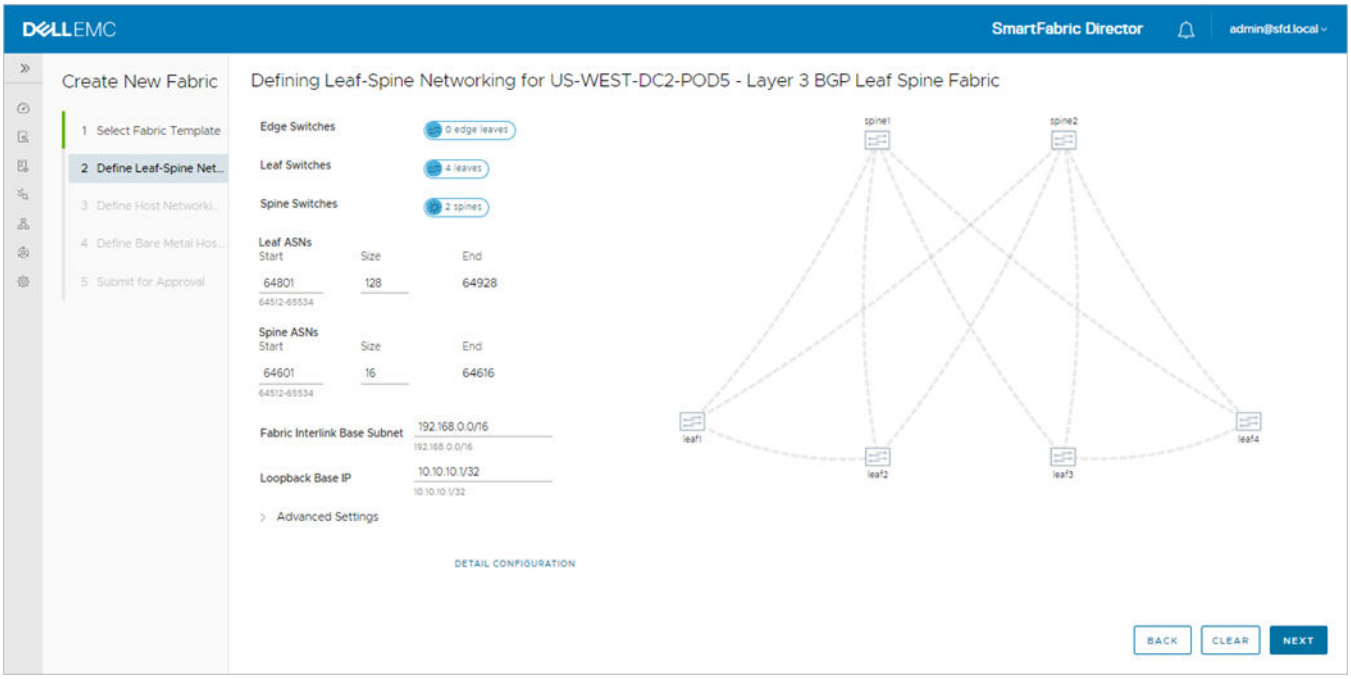


2. Select **Layer 3 BGP Leaf Spine Fabric** as the fabric template, then click **Next**.



Define leaf spine networking

1. Specify the fabric interlink subnet, the /32 loopback IP address seed, then click **>** to expand advanced settings. SFD generates a per-switch configuration for the interlinks between the leaf and spine switches.



Keep the default values for the leaf and spine ASNs, especially the size, to allow for future expansion. If the size is made restrictive, adding spine or leaf pair switches could result in a failure due to nonavailability of ASN numbers.

SFD allocates the interlink subnets and IP addresses to the loopback interfaces for each switch. You can specify the base addresses for these which are used as the starting point for allocation. These addresses are used within the fabric.

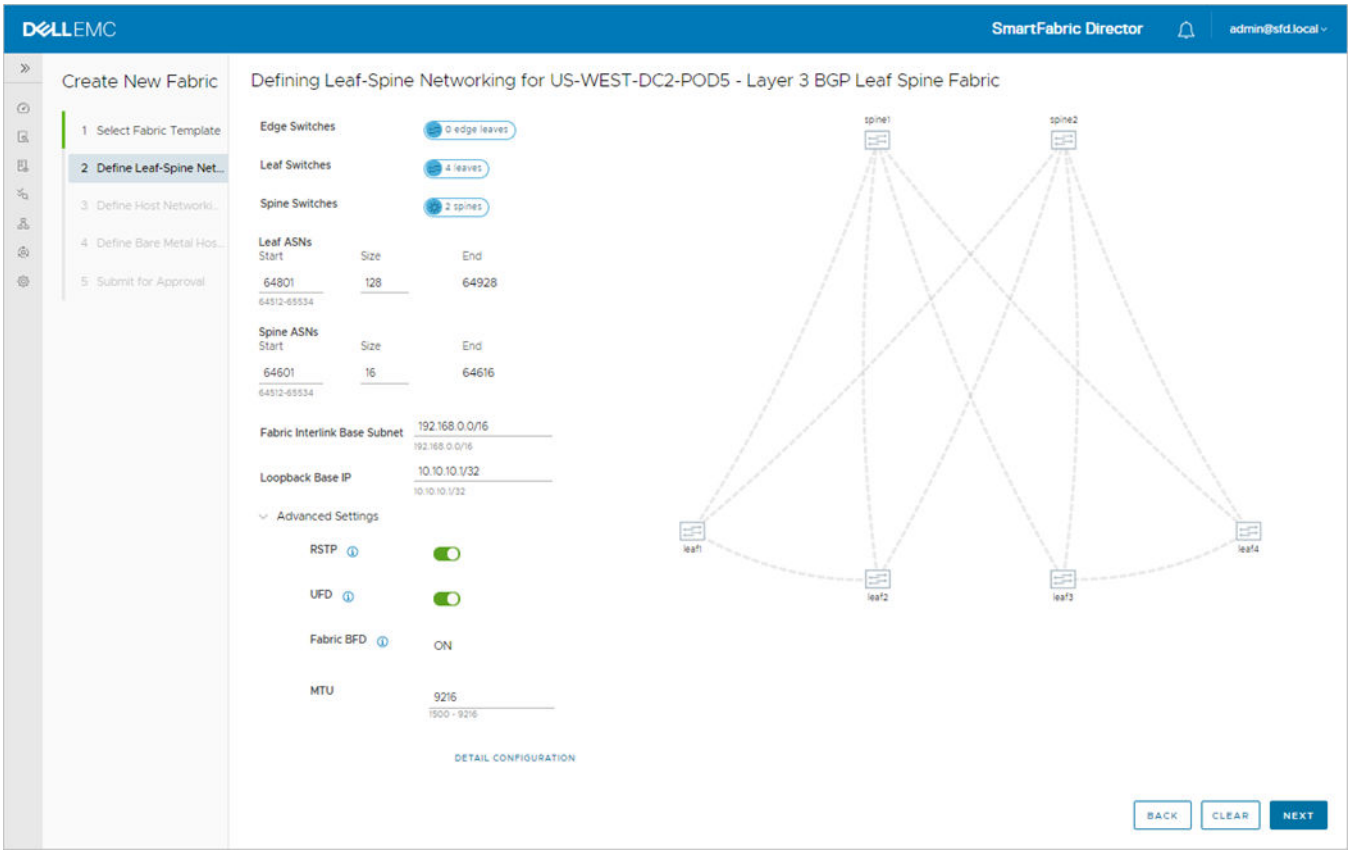
If switches are removed and added back, the individual IP addresses assigned to the newly added switch may not be in monotonically increased order. It not guaranteed that a previously allocated IP address will be used. The functionality of the fabric is not dependent on any specific order that the addresses are allocated by SFD. There can be no duplicate IP addresses within the fabric, and the addresses must be within the range starting with the specified base value.

Advanced settings

By default, rapid spanning-tree protocol (STP) is enabled to ensure a loop-free topology, as well as uplink failure detection (UFD) which detects the loss of upstream connectivity. An uplink state group is configured on each leaf switch which creates an association between the uplinks to the spins, and the downlink interfaces. In the event all uplinks fail on a switch, UFD automatically shuts down the downstream interfaces. This propagates to the hosts attached to the leaf switch.

Bidirectional forwarding detection (BFD) detects faults between two forwarding engines connected by a link. It provides low overhead detection of faults, even on physical media that does not support failure detection of any kind such as Ethernet. This is enabled by default on all switches in a fabric and cannot be modified.

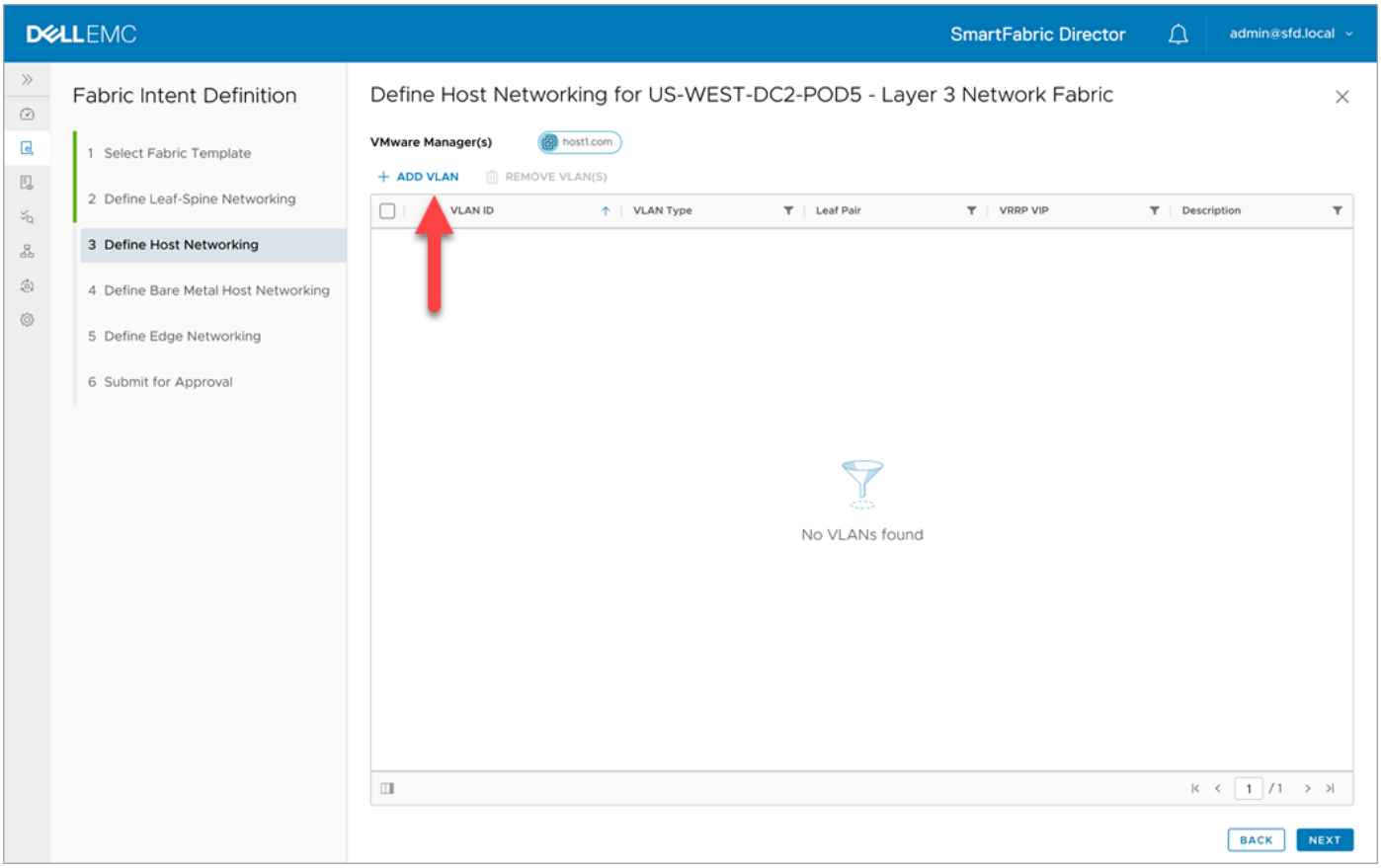
2. Specify the maximum transmission units (MTUs) for the fabric, then click **Next**. SFD ensures that the MTU is set to a specified value on all switches in the fabric.



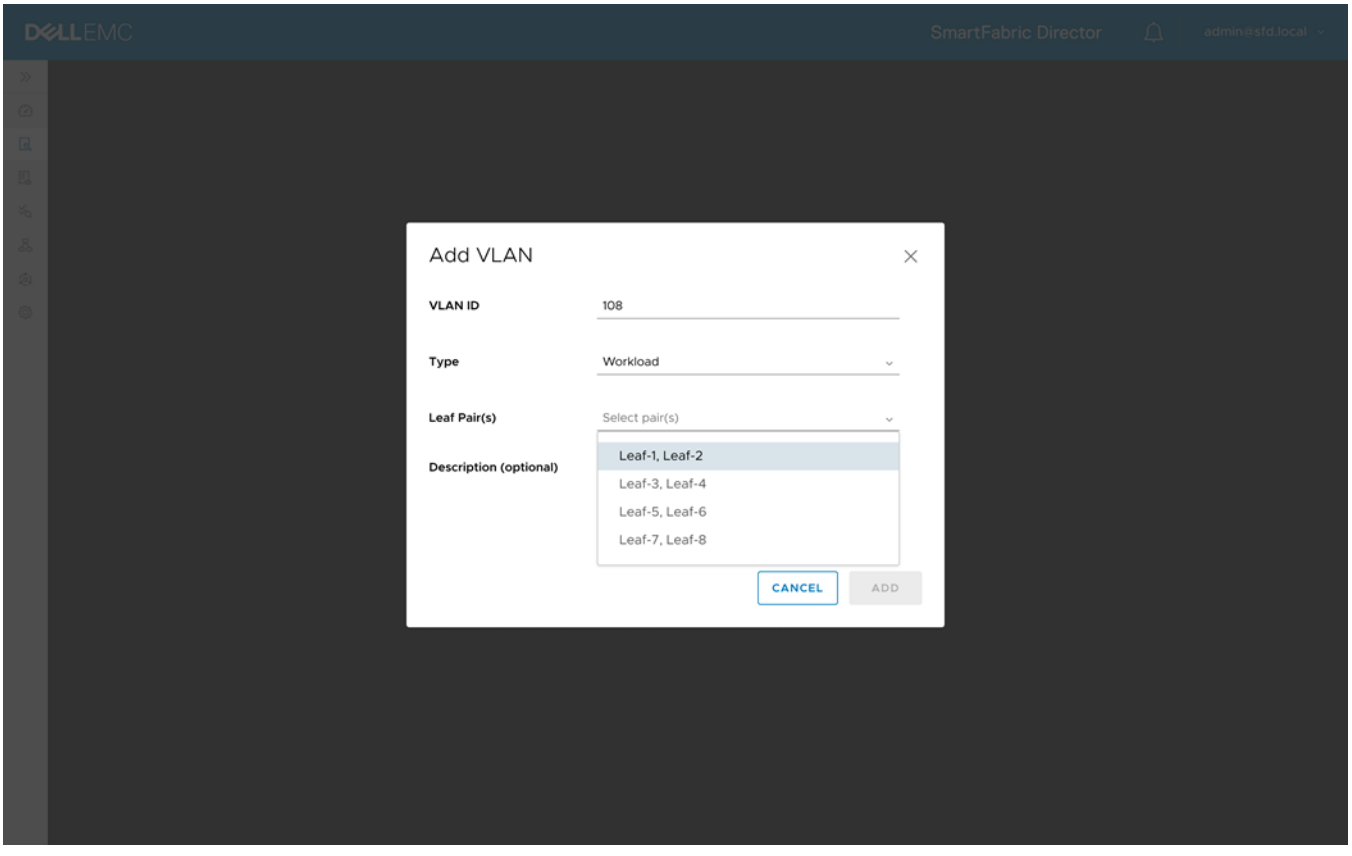
Define host networking

You can specify configuration to support servers carrying virtualized workloads, which are managed by vCenter. SFD interfaces with vCenter to retrieve the port group information when a workload (VM) is deployed. It uses the workload to configure the switch to bind the port to the VLAN.

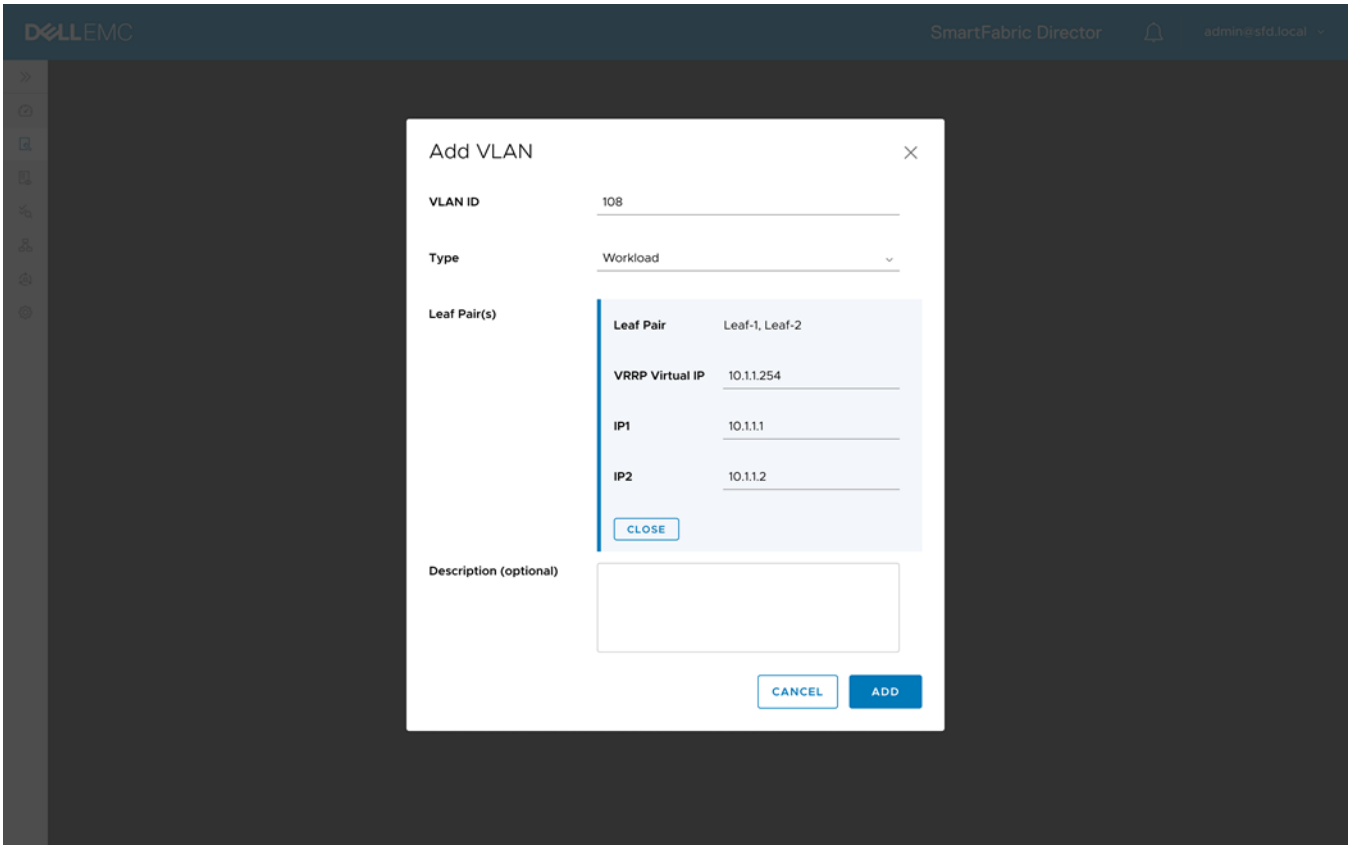
1. Click **Add VLAN** to add the configuration for each port group for the vCenter Server, then click **Next**.



2. Enter the VLAN ID corresponding to the port group, select the Type, then associate one or more VLT pairs to a VLAN ID from the list of available VLT pairs (from the wiring diagram).

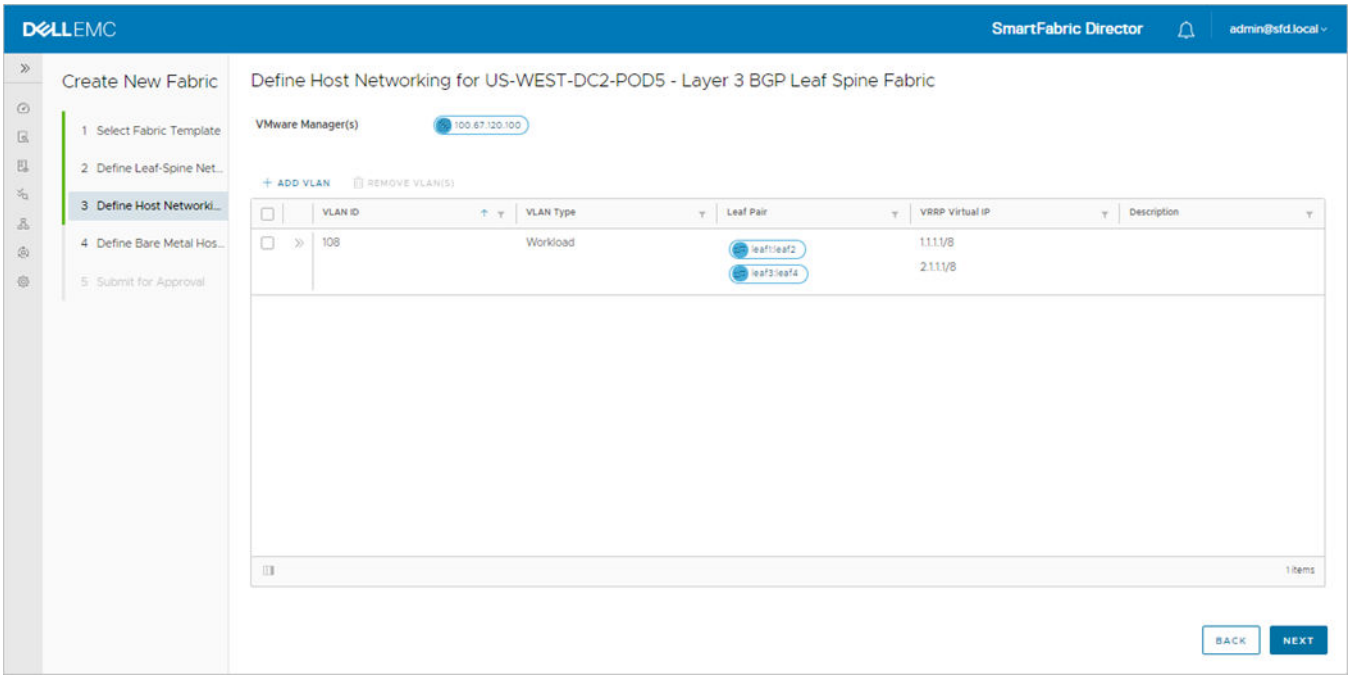


3. Enter the VRRP Virtual IP, IP1, IP 2 information, then click **Close**.

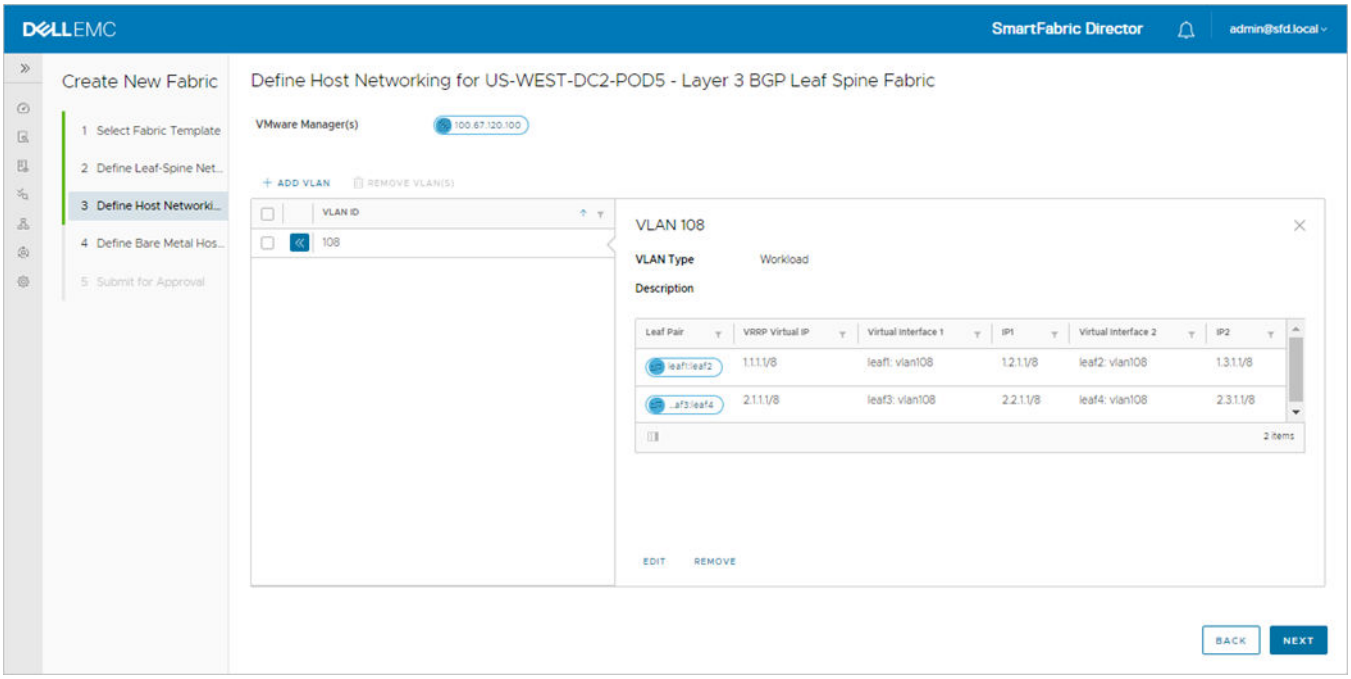


4. (Optional) Click **Add more pairs** and repeat the steps.
5. Enter an optional description, then click **Add**. Each leaf in the VLT pair has its own IP, and each VLAN in the VLT pair has a VRRP virtual IP in the same subnet as the VLAN.

   The VLAN displays as each host is added.



6. Click **>>** to provide more details, then click **Next**.

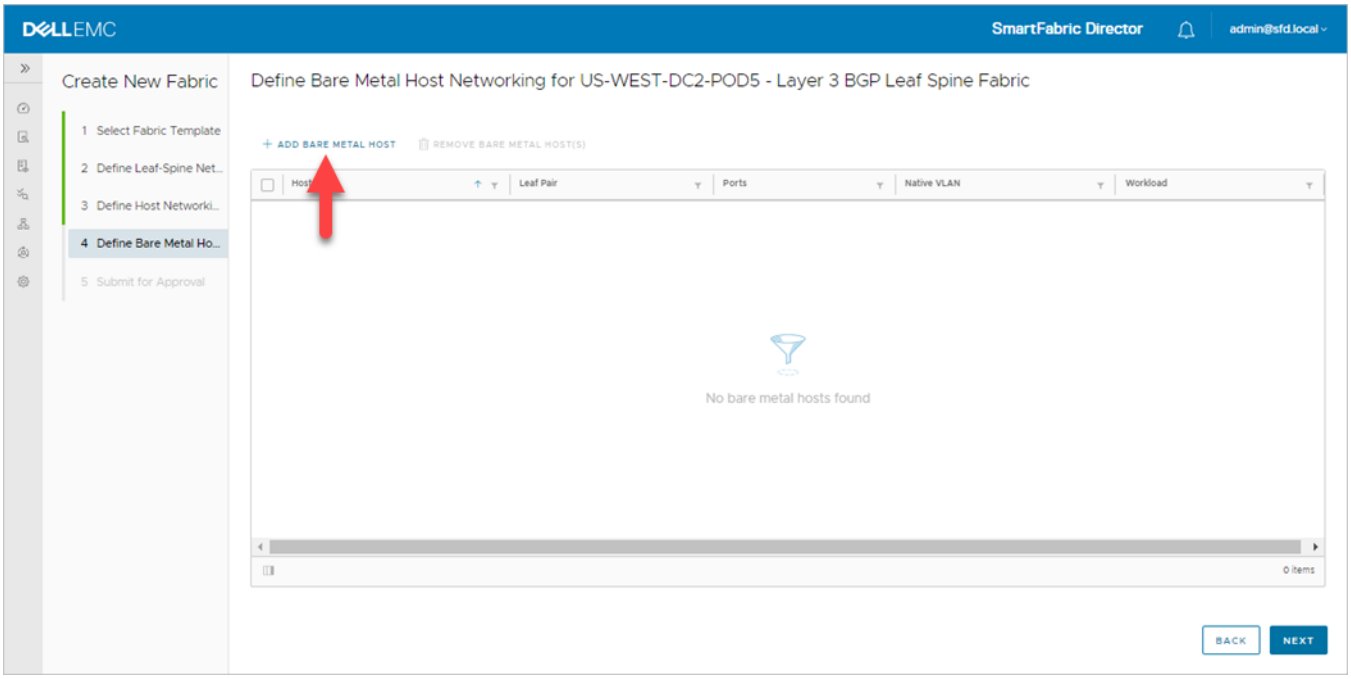


Define bare metal host networking

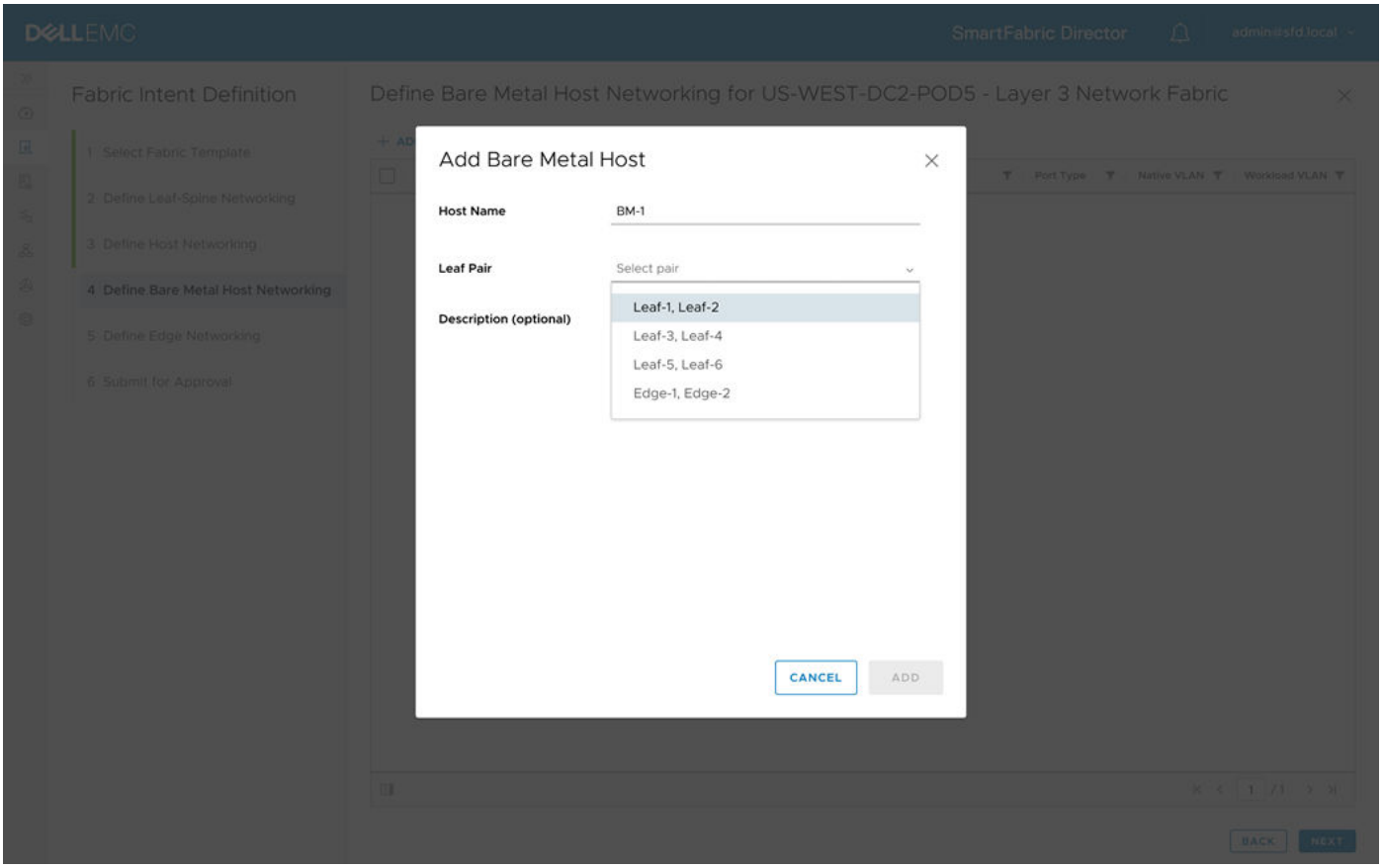
Not all applications can be virtualized, and you may need to deploy non-virtualized workloads. Hosts used to deploy non-virtualized workloads are called *bare metal hosts*. SFD 2.0 supports bare metal hosts.

NOTE: Define bare metal host networking is an optional step. Bare metal is required to add a VLAN in access or trunk mode. If there are no non-virtualized workloads (bare metal hosts), you can skip this step.

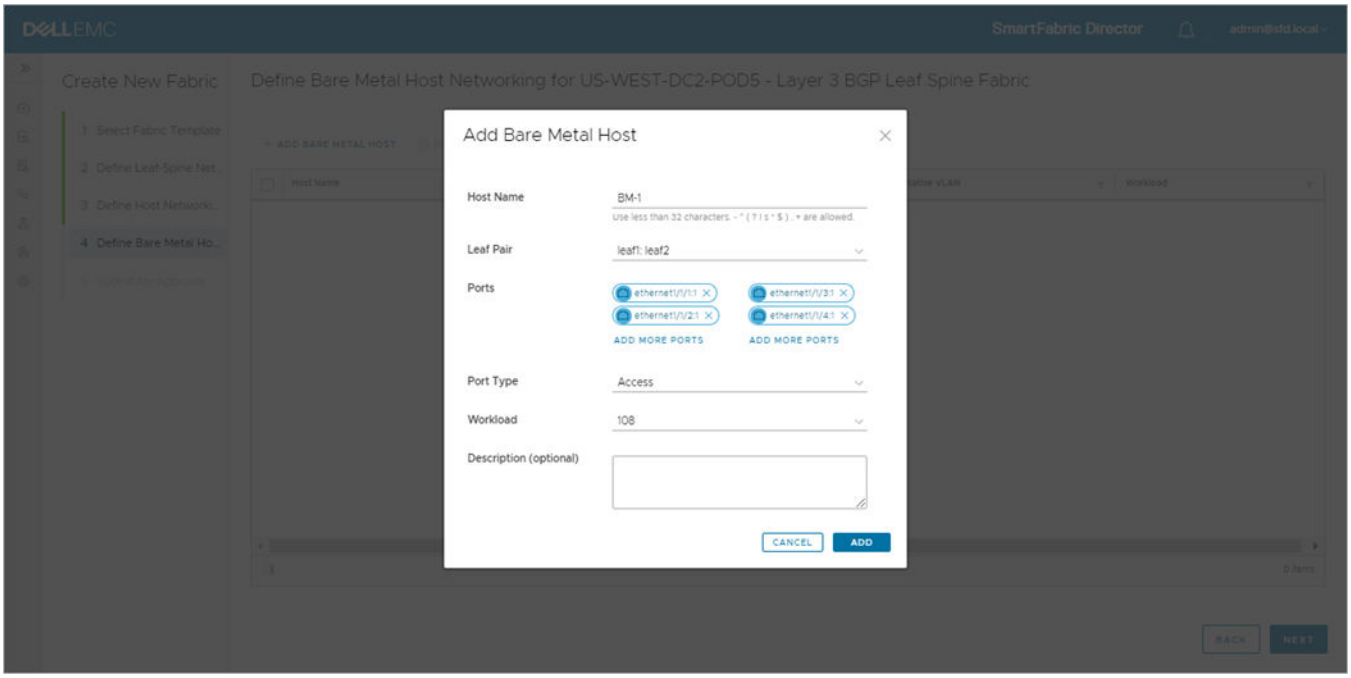
1. Click **Add bare metal host**.



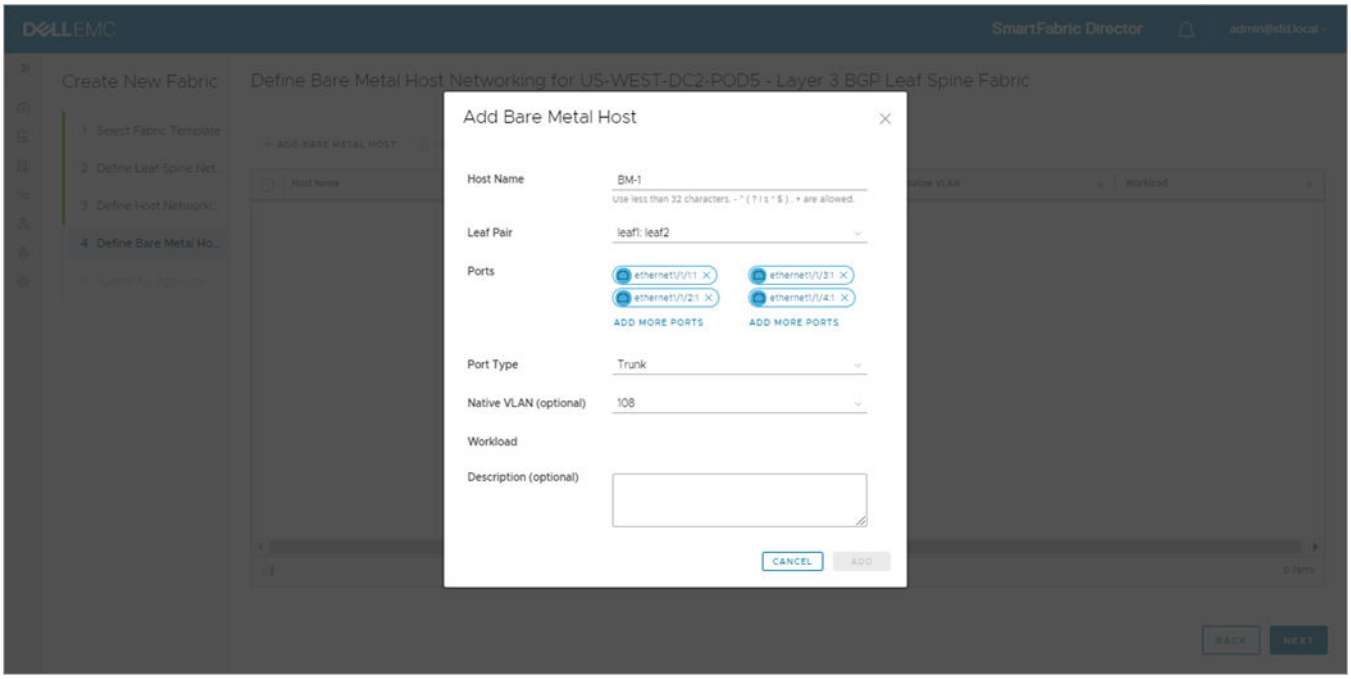
2. Enter the Host Name to identify the VLT pair to which the host is connected to, then select the Leaf Pair.



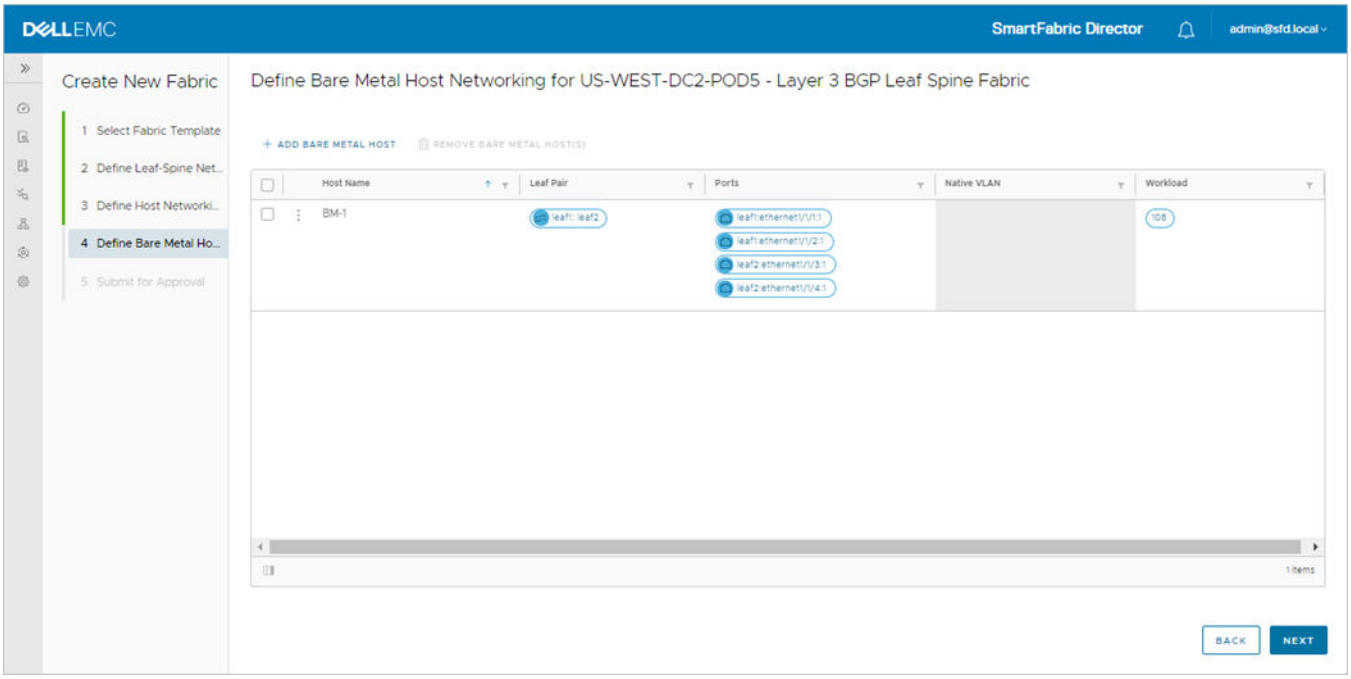
3. Specify one or more switch ports that the server is connected to, select Access or Trunk for the port type, select the workload VLAN, an optional description, then click **Add**.



A trunk port type requires a native VLAN in addition to the workload VLAN. The switch default configuration has a native VLAN, and the switch native VLAN option is prepopulated. If you select trunk as the port type and would like to specify the native VLAN explicitly, enter a VLAN number. Similar to an access port type, a workload VLAN needs to be specified.



4. With a trunk port, the host can have more than one workload VLAN. Click **Add more VLANs** to add additional workload VLANs, then click **Add**.
5. The configured bare metal host displays in the bare metal host table. Click **Next** to proceed to edge networking.

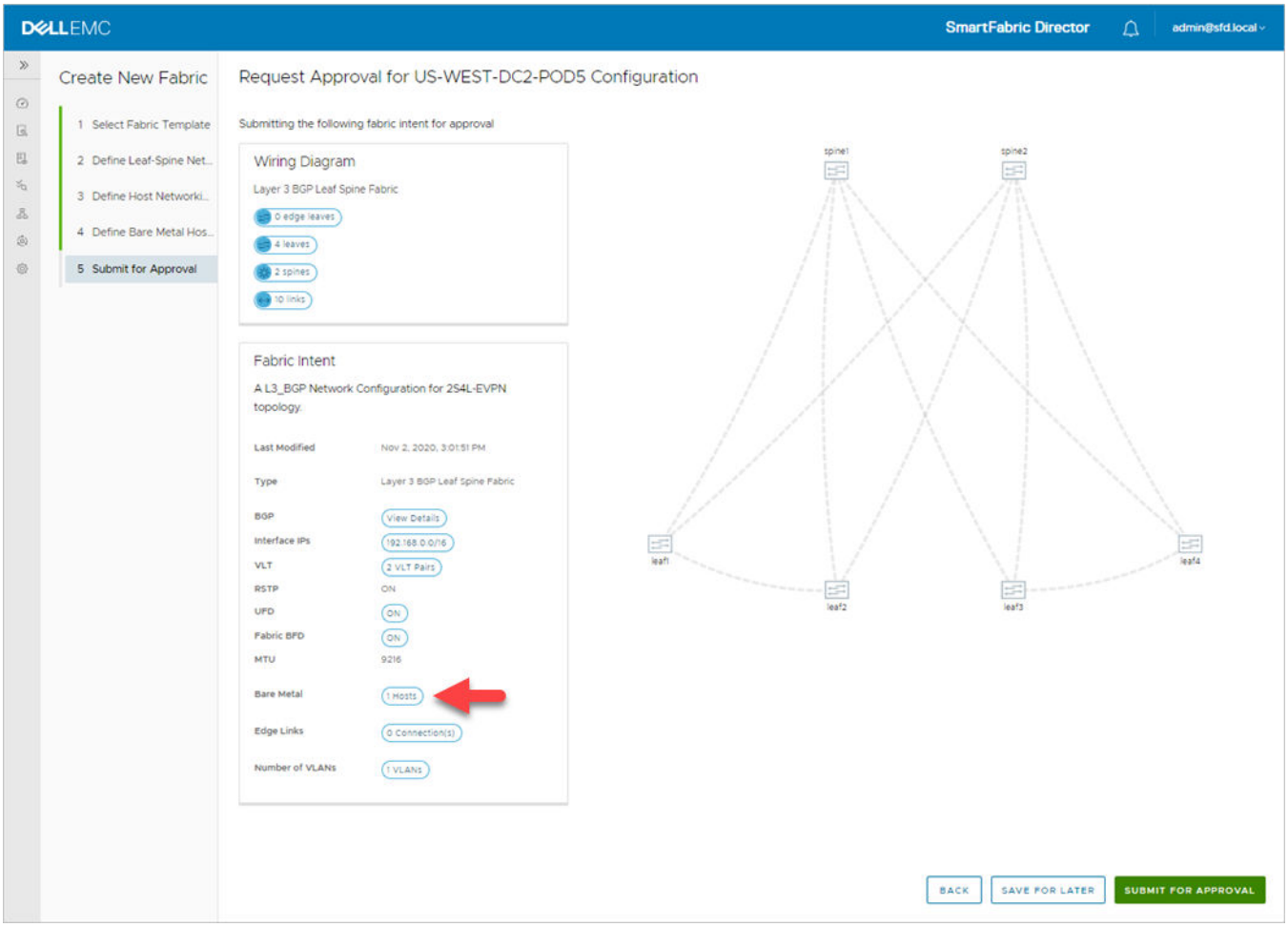


6. (Optional) Select the bare metal host, click the three dots, then select **Edit** to modify the configuration.

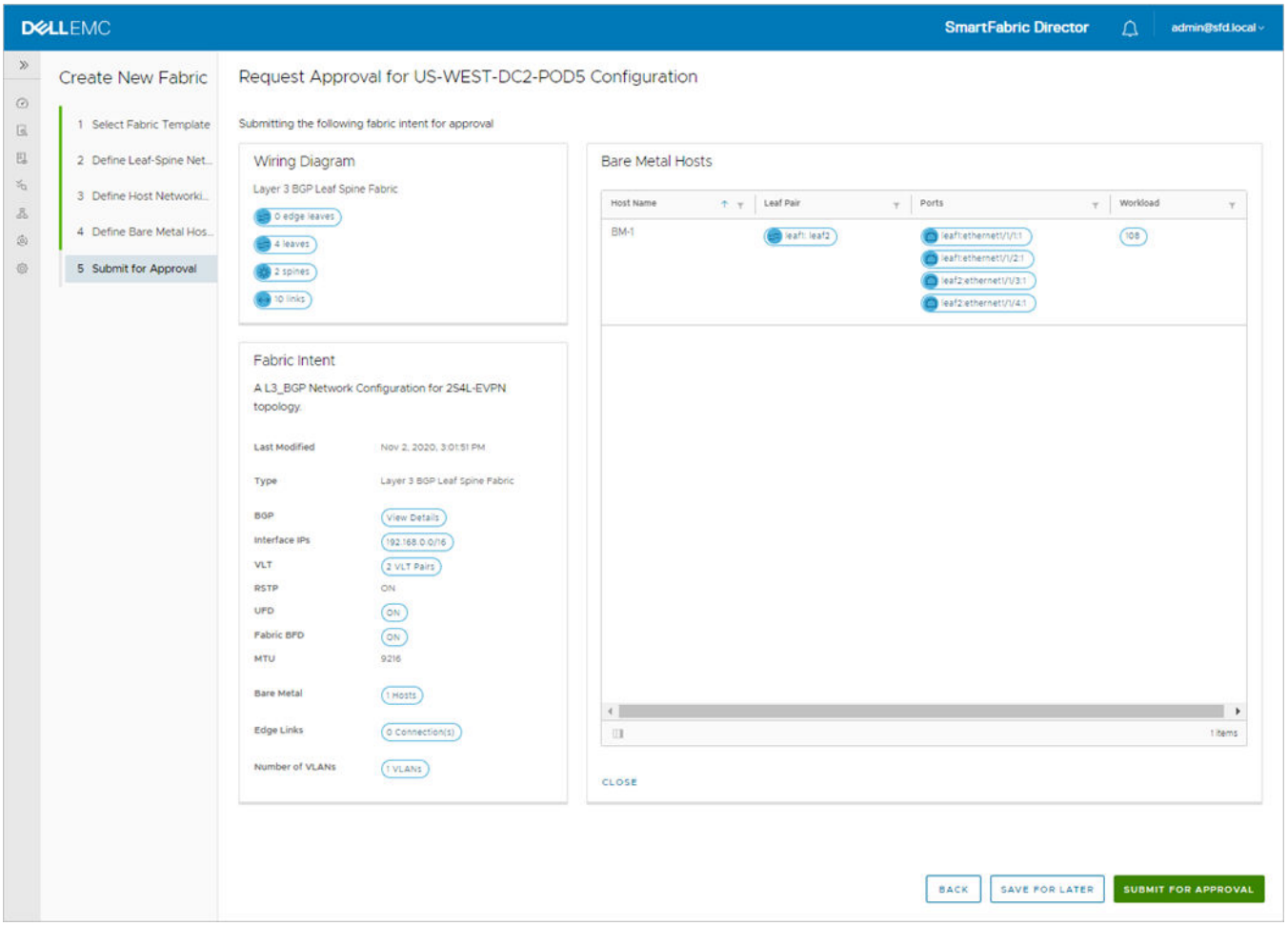
Submit for approval

Once the fabric intent has been specified, it needs to be approved before deployment. Only approved fabric intents can be deployed. SFD provides a summary of the wiring diagram and the fabric intent.

1. Click on the individual tiles to view details of the intent before submitting it for approval.



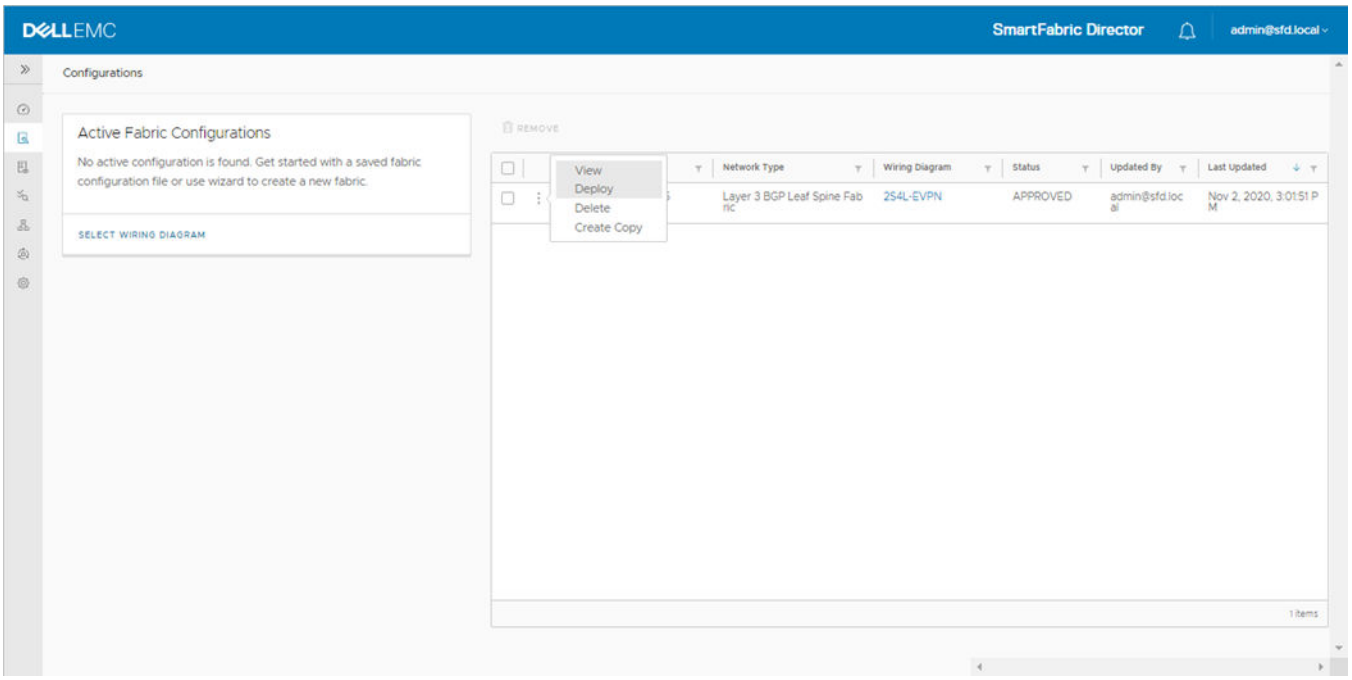
2. Details display in the right section. Click **Submit for approval** to continue.



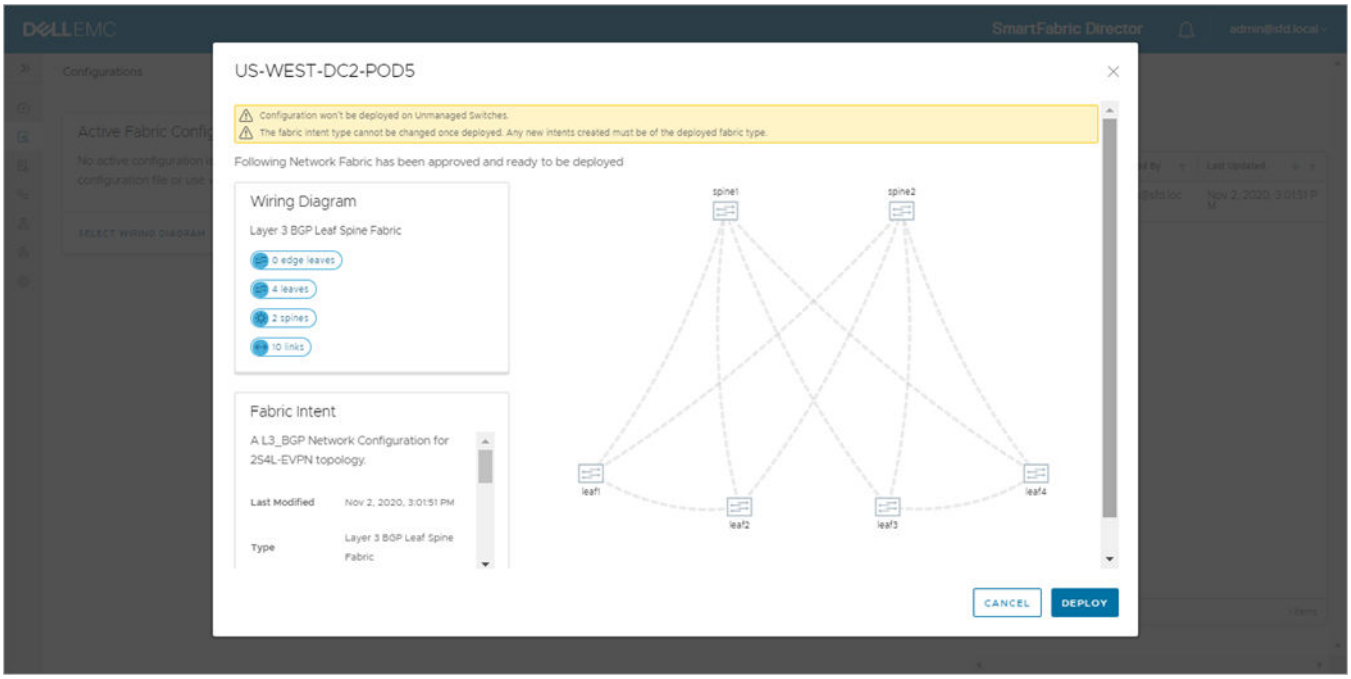
The fabric intent is approved automatically in SFD 2.0, and will display in the Fabric intent table.

Deploy an approved fabric intent

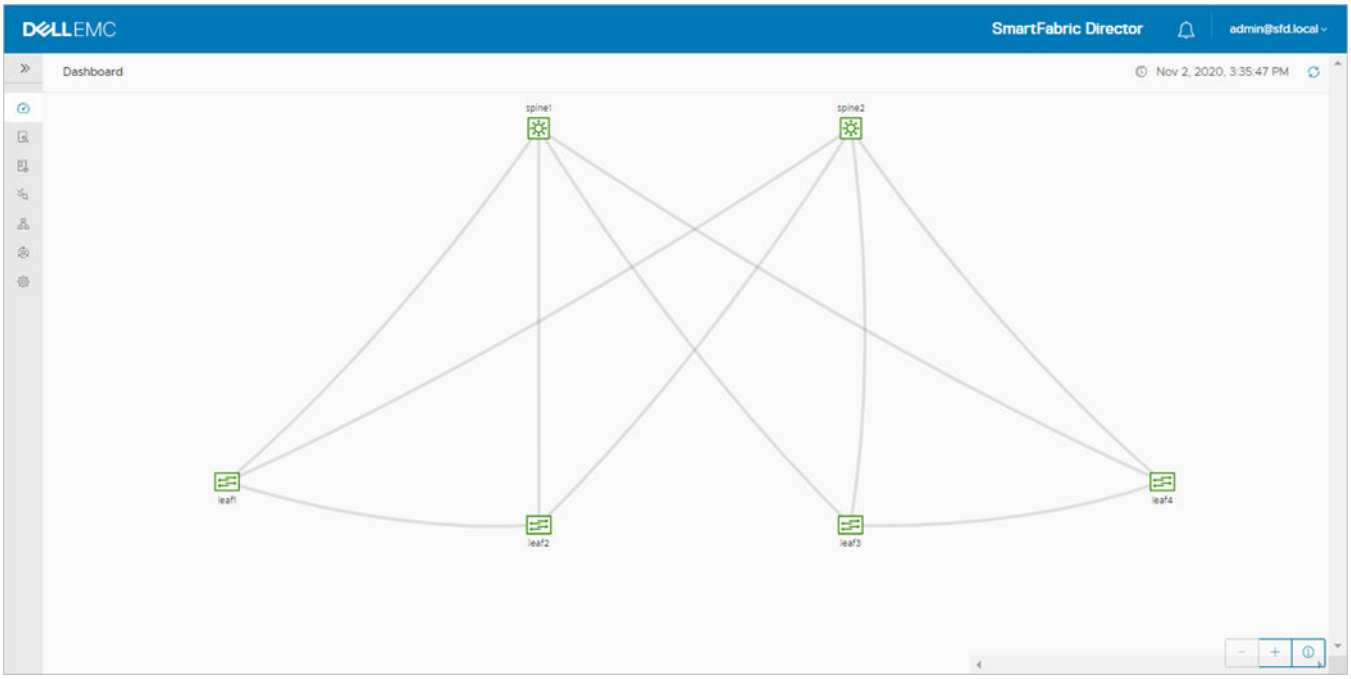
The Fabric intent table displays all fabric intents that are active (if there is one deployed), approved, or in draft state.



Click **Deploy** to deploy an approved fabric intent, or click **Create copy** to make a copy of the fabric intent and make edits to the intent.



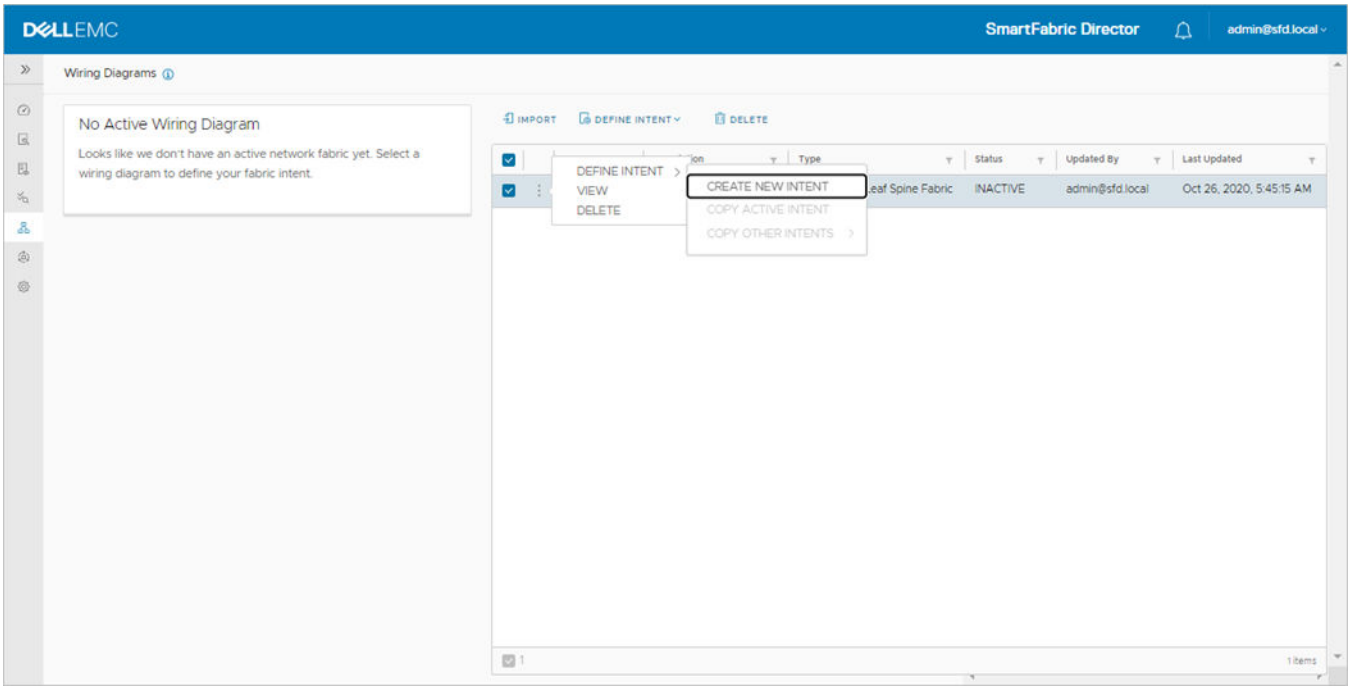
SFD generates a per switch configuration and sends that to the switches using the gNMI interface. The progress of deployment can be viewed on the Topology page, as well as Job activities. As a switch is successfully configured, the color turns to green. The icons change from gray to blue, then to green.



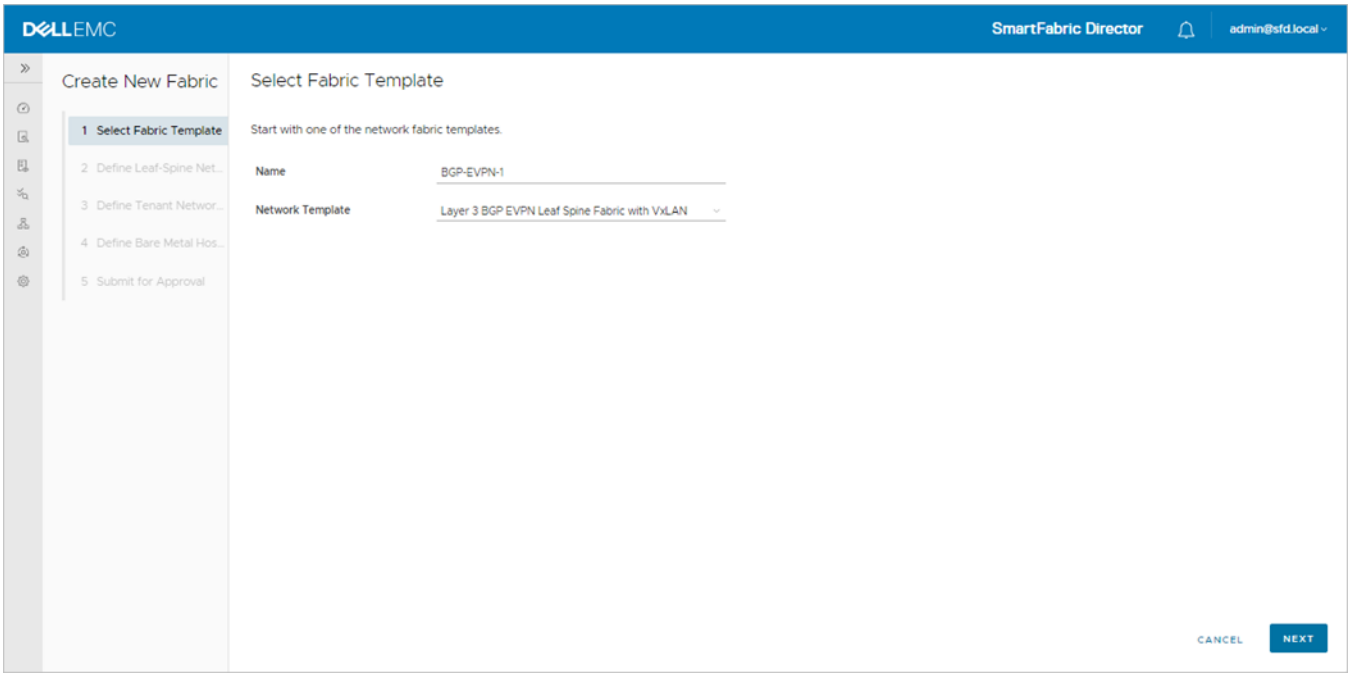
Layer 3 BGP EVPN leaf spine fabric with VxLAN

Select fabric template

1. Select the fabric, then **Define intent** > **Create new intent**. If modifying an active intent, make a copy of an intent from the table of intents (active or otherwise), then make the necessary changes.



2. Select **Layer 3 BGP EVPN leaf spine fabric with VxLAN**, then click **Next**.

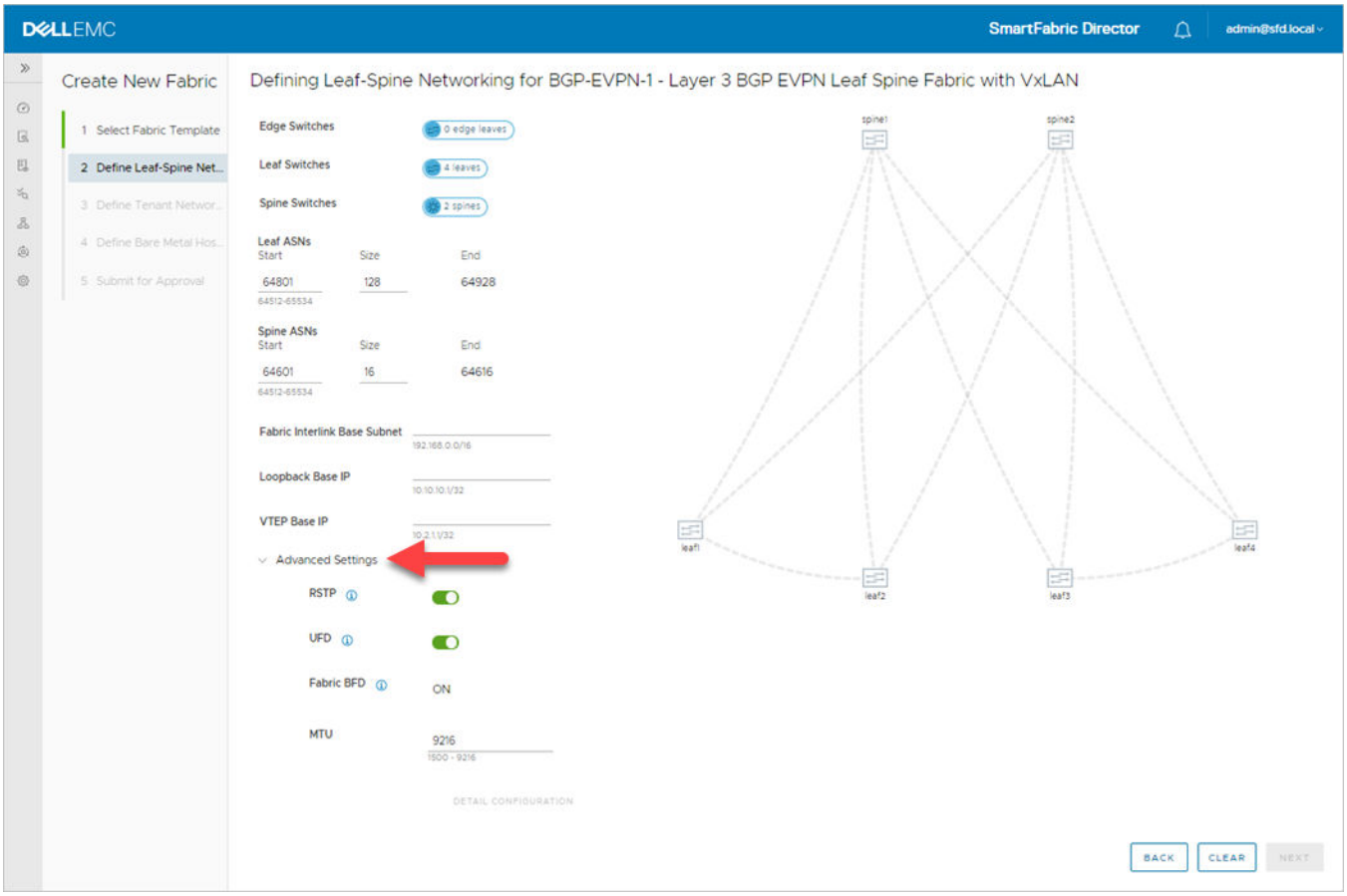


Define leaf spine networking

Define underlay for BGP EVPN

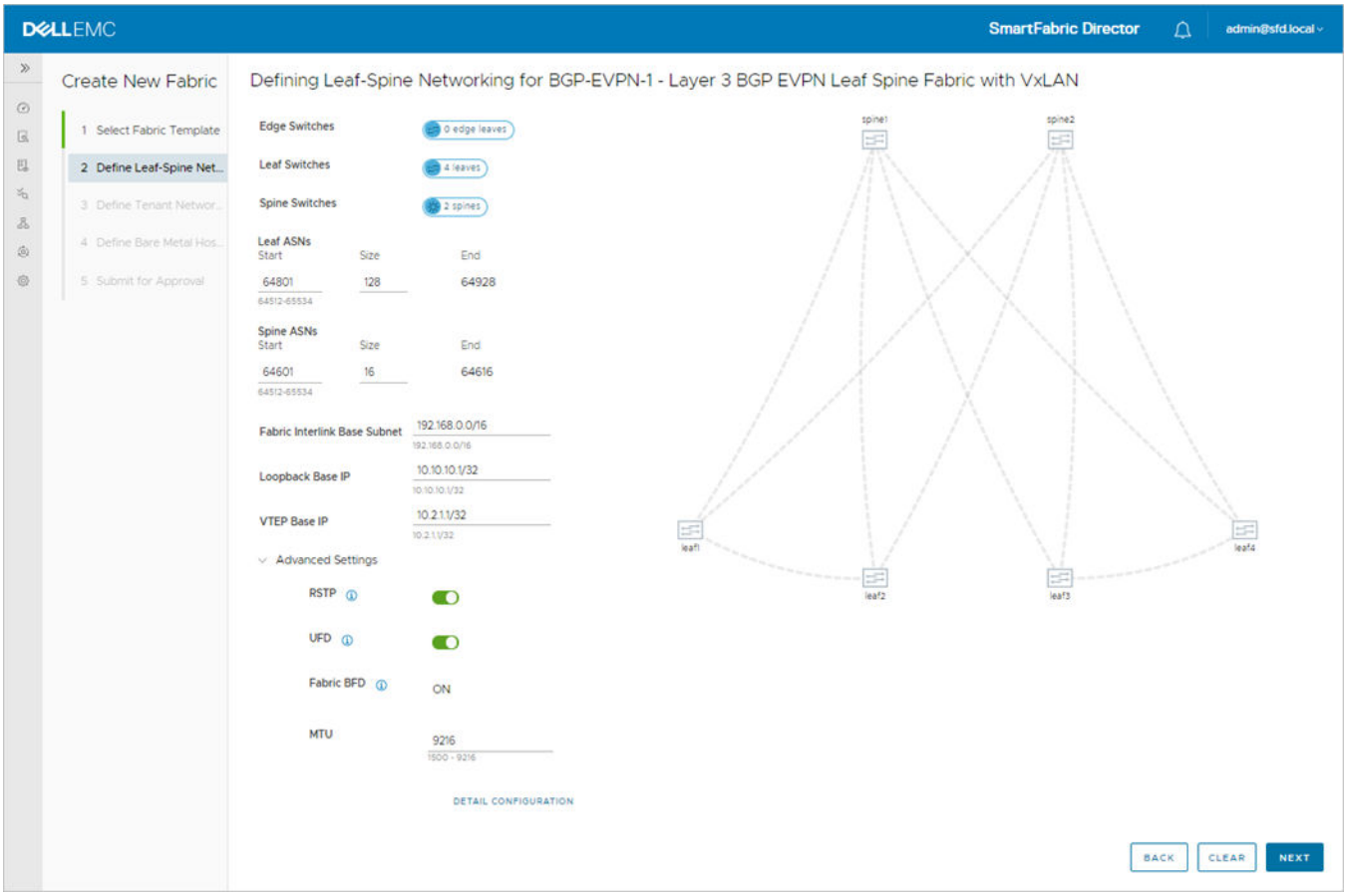
NOTE: The fabric type cannot be changed once deployed.

1. It is recommended to keep the default values for the leaf and spine ASNs to allow for future expansion. If the size is made restrictive, adding spine or leaf pair switches could result in failure due to nonavailability of ASNs. Click **Advanced settings**.



2. Specify the base addresses to be used as the starting point for allocation. SFD allocates the interlink subnets, IP address to the loopback interfaces, and the VTEP IP address for each switch. These addresses are used within the fabric.

   NOTE: Underlay network configuration can not be changed after deployment for future development. Advanced settings can be changed.



If switches are removed and added back, the individual IP addresses assigned to the newly added switch may not be in monotonically increasing order and it is not guaranteed that a previously allocated IP address is reused.

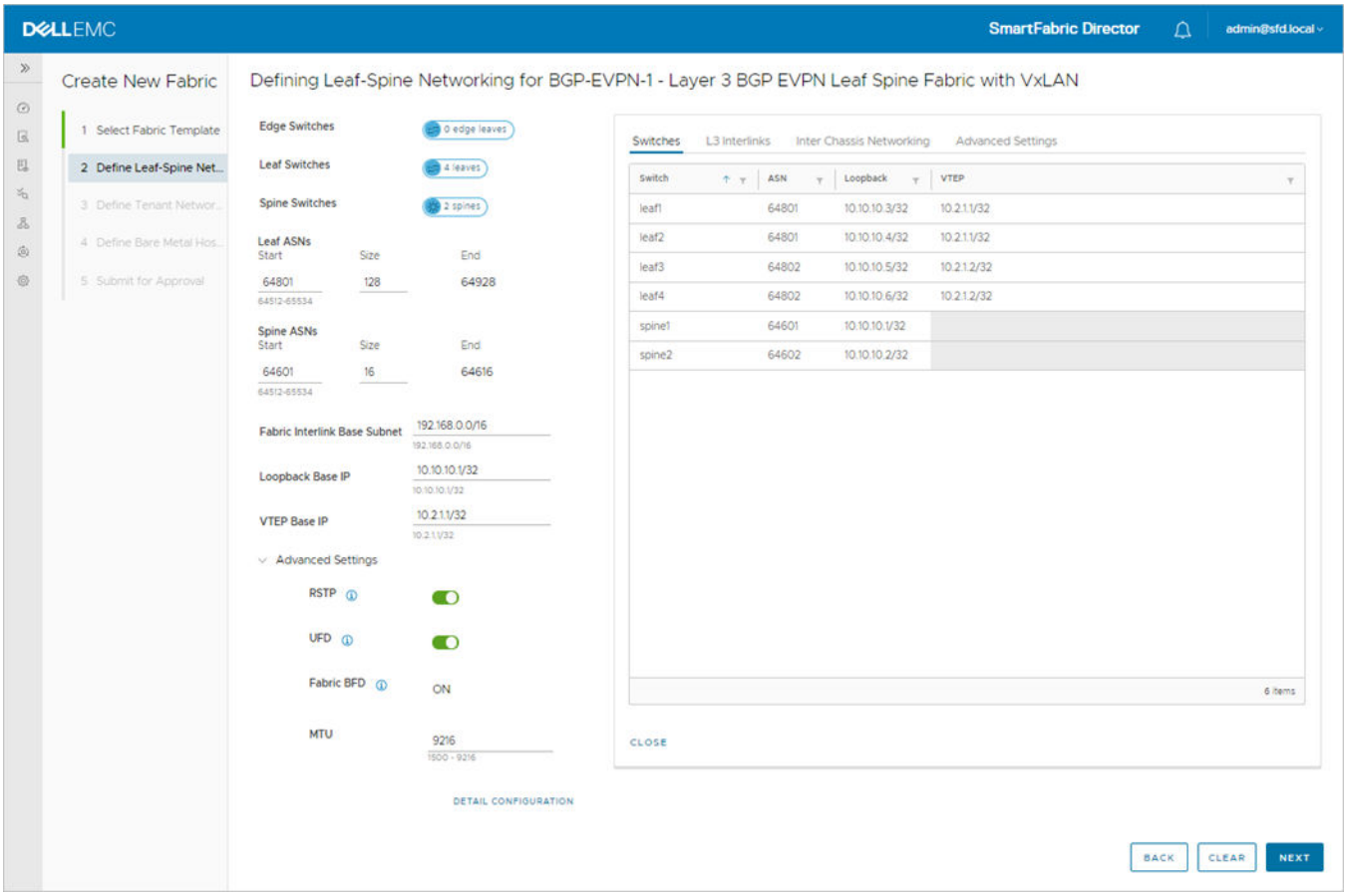
The functionality of the fabric is not dependent on any specific order that the addresses are allocated by SFD. There cannot be duplicate IP addresses within the fabric, and the addresses must be within range starting with the specified base value.

3. Enable rapid spanning-tree protocol (**RSTP**) to ensure a loop-free topology. Disabling STP would disable the functionality on all switches in the fabric.
4. Enable uplink failure detection (**UFD**) to detect the loss of upstream connectivity. An uplink state group is configured on each leaf switch, creating an association between the uplinks to the spins and the downlink interfaces.

   If all uplinks fail on a switch, UFD automatically shuts down the downstream interfaces. This propagates to the hosts attached to the leaf switch. The host then uses its link to the remaining switch to continue sending traffic across the leaf-spine network. Disabling UFD disables the functionality on all switches in the fabric.

   Bi-directional forwarding detection (BFD) is a network protocol that is used to detect faults between two forwarding engines connected by a link. It provides low-overhead detection of faults, even on physical media that does not support failure detection of any kind (such as Ethernet). BFD is enabled by default on all switches in a fabric and cannot be modified.
5. Specify the maximum transmission unit (**MTU**) for the fabric (default 9216).

   SFD ensures that the MTU is set to the specified value on all switches in the fabric. VxLAN is an overlay technology that has an overhead due to the VxLAN header. A lower MTU value could result in slower throughput.
6. Click **Detail configuration** to view the per switch configuration parameters allocated by SFD, then click **Next**.

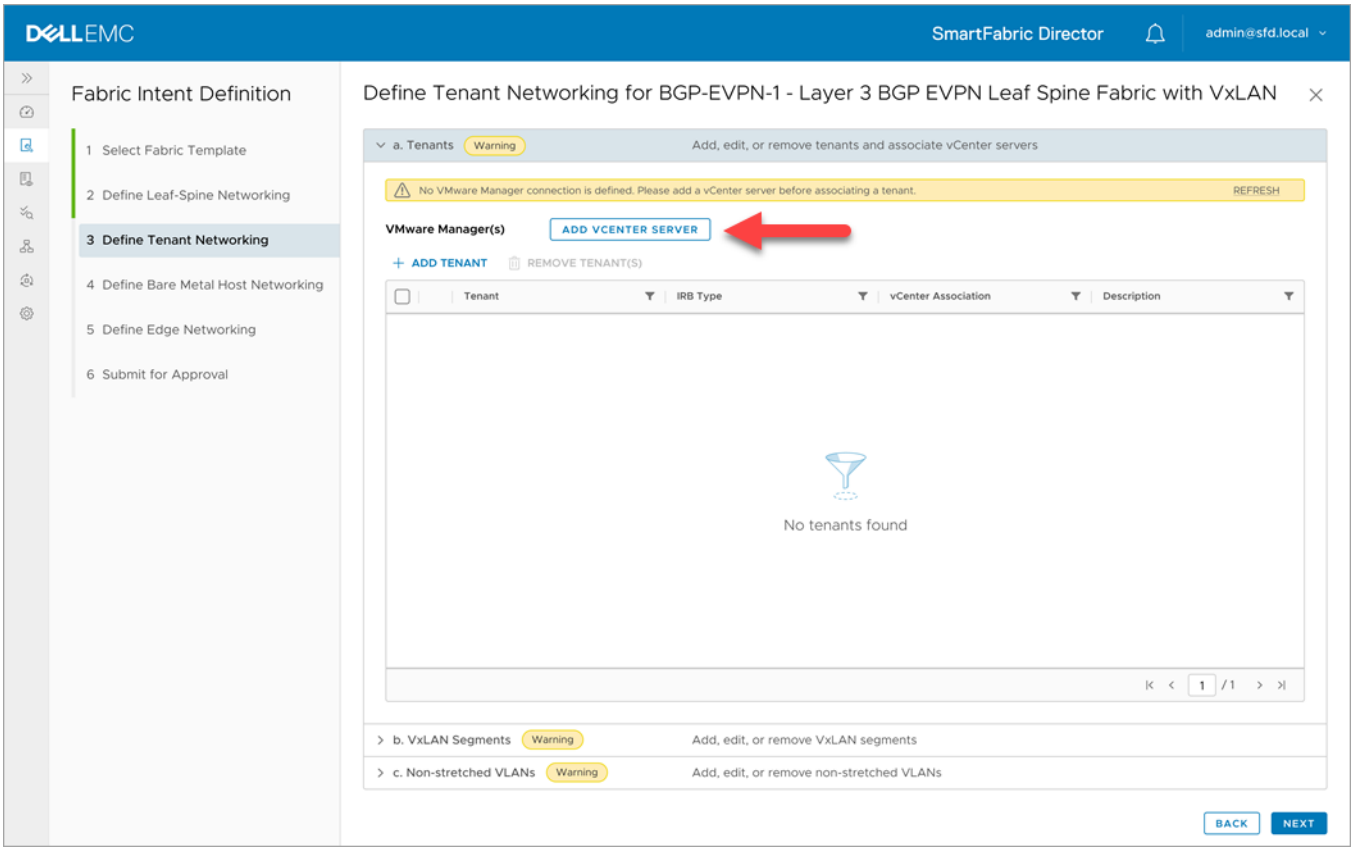


Define tenant networking

Specify a vCenter (VMware Manager)

In BGP VxLAN fabric with hardware VTEP, NSX-T is not required. For virtualized workloads, a vCenter is required. SFD interfaces with vCenter using the REST API. The reachability information (IP address) and credentials must be specified for SFD to establish a session. VMware Manager is specified as part of System settings.

1. Click **Add vCenter server**.

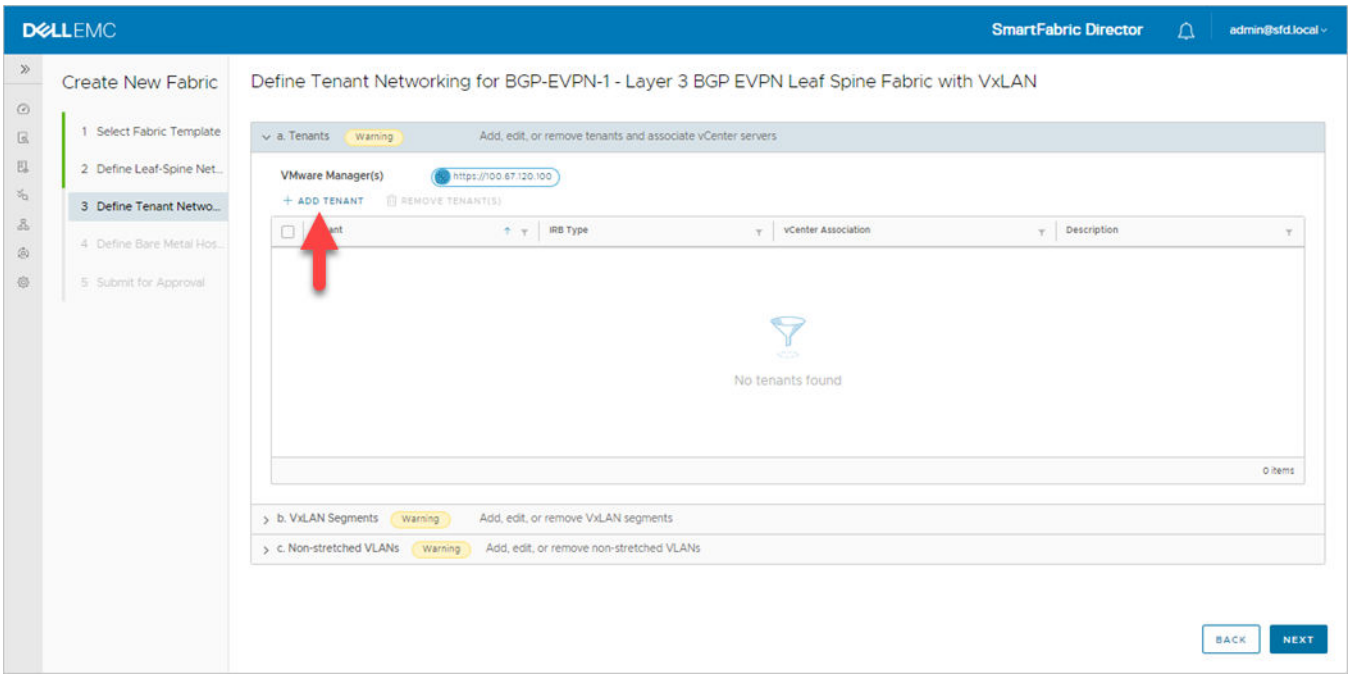


2. Specify the IP address or FQDN of the vCenter server, username, and password that is used to establish a session for REST API-based interaction with vCenter, then click **Add**.

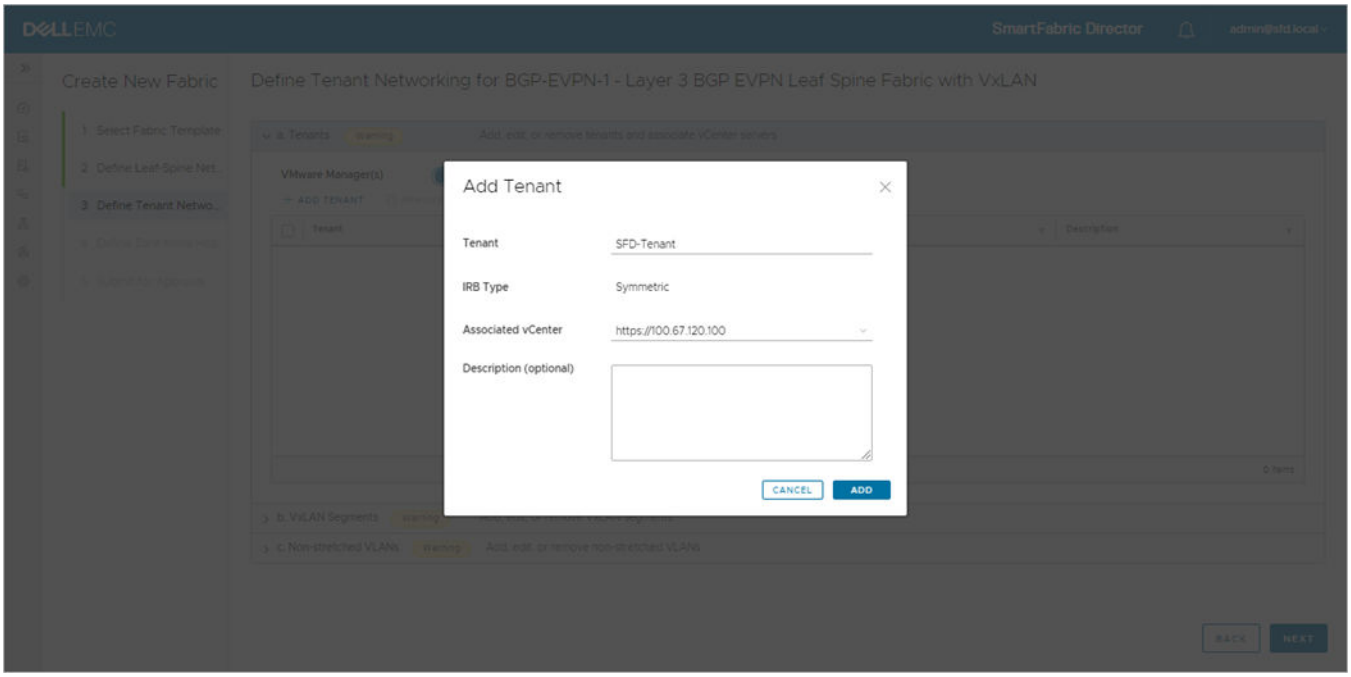
Add a tenant

EVPN allows multitenancy, but SFD 2.0 only supports a single tenant.

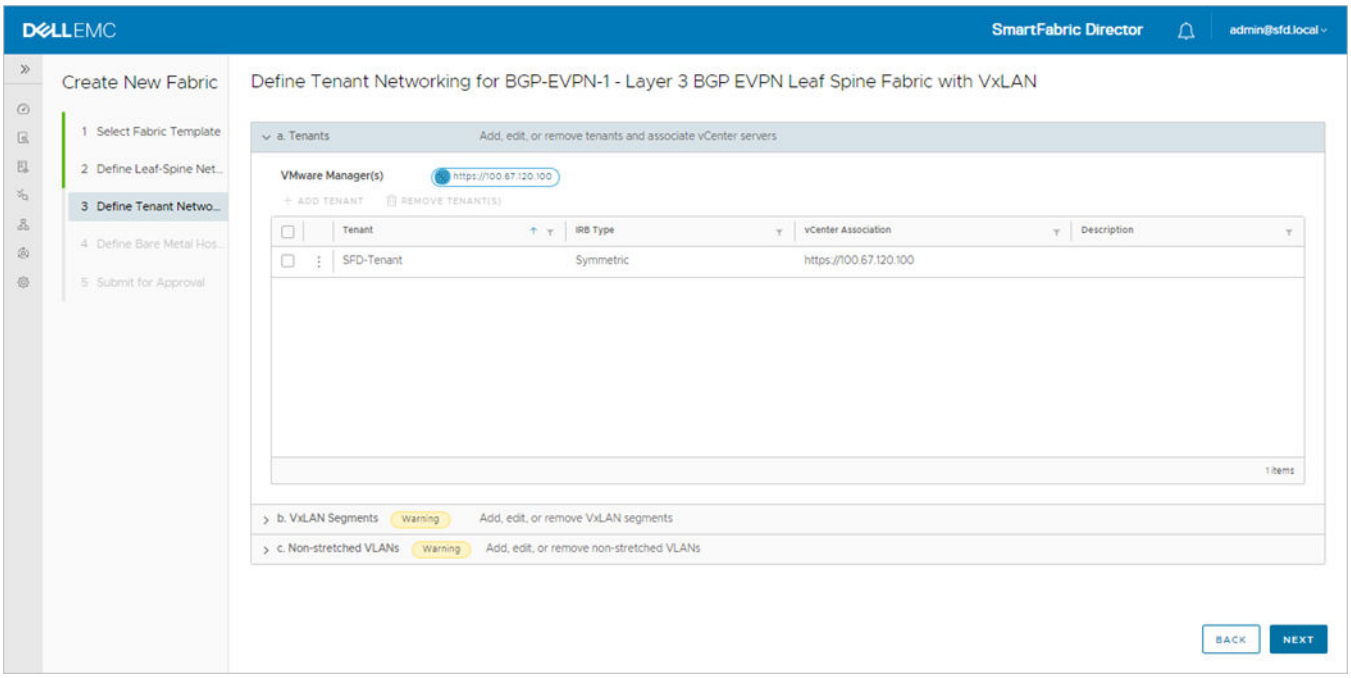
1. Click **> a. Tenants**, then **Add tenant**.



2. Specify a tenant name and associate a vCenter, then click **Add**. Symmetric IRB for the VxLAN VTEP cannot be modified.



The new tenant is added to the Tenant table. To edit the tenant, select the tenant, then click the three dots to edit or remove the tenant. If you remove the tenant, all associated configuration for that tenant will also be removed.



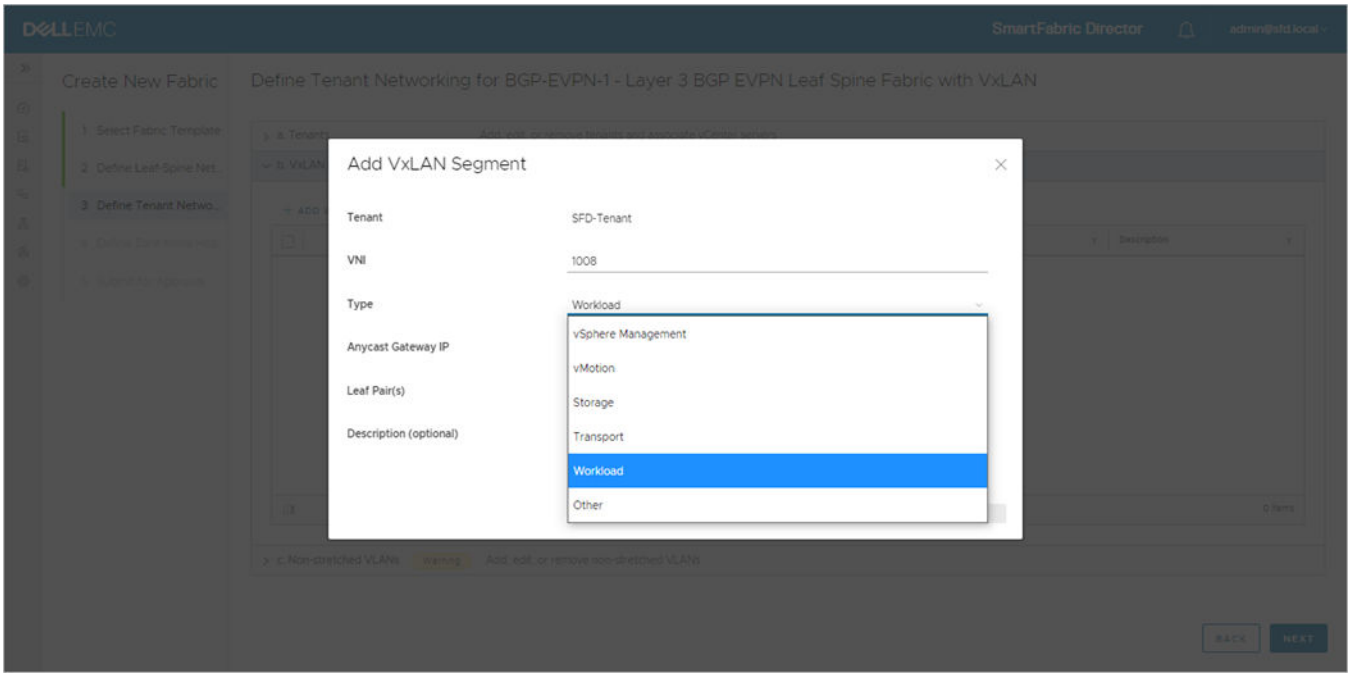
Add VxLAN segments (VNIs)

A VxLAN segment is a virtual network grouping that all related workloads belong to. It is similar to a VLAN in Layer 2 fabric, but spans across racks or data centers.

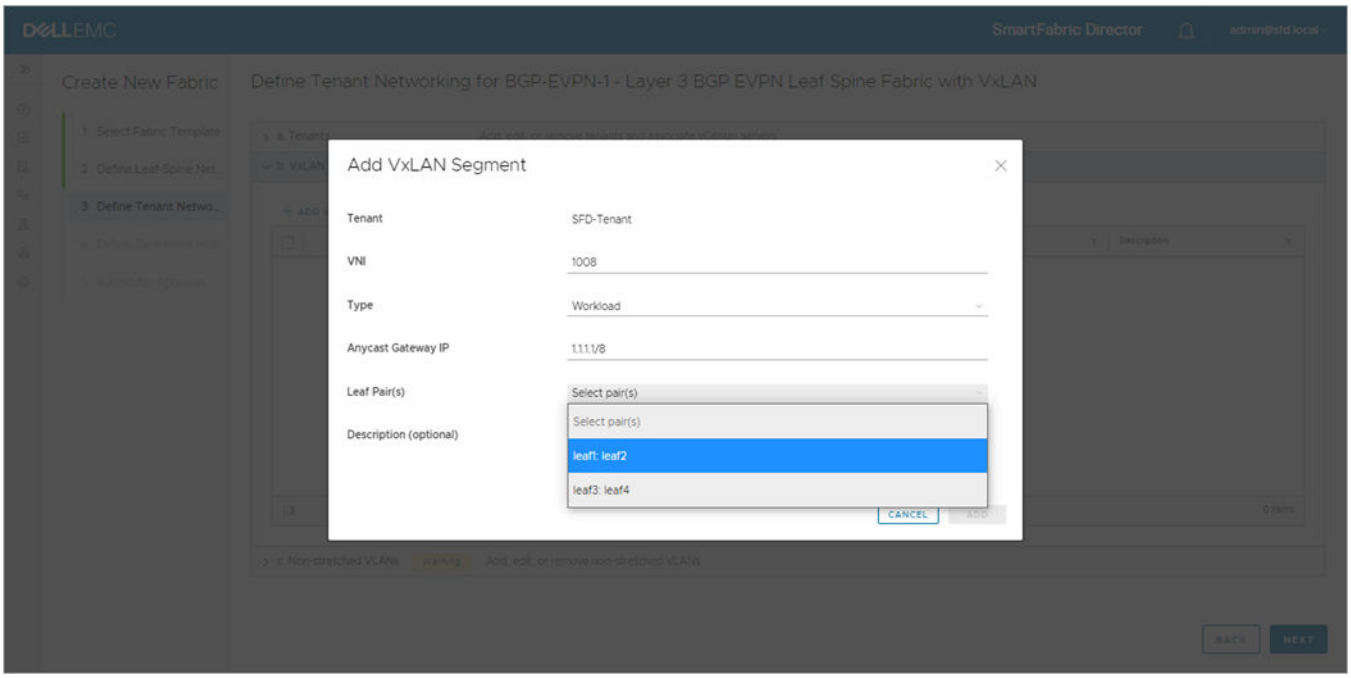
1. Click **> b. VxLAN segments**, then **Add VxLAN segment**.

   A virtual network ID (VNI) is used to identify a VxLAN segment.

2. Specify a unique VNI for each VxLAN segment across all tenants, then select the Type from the drop-down.



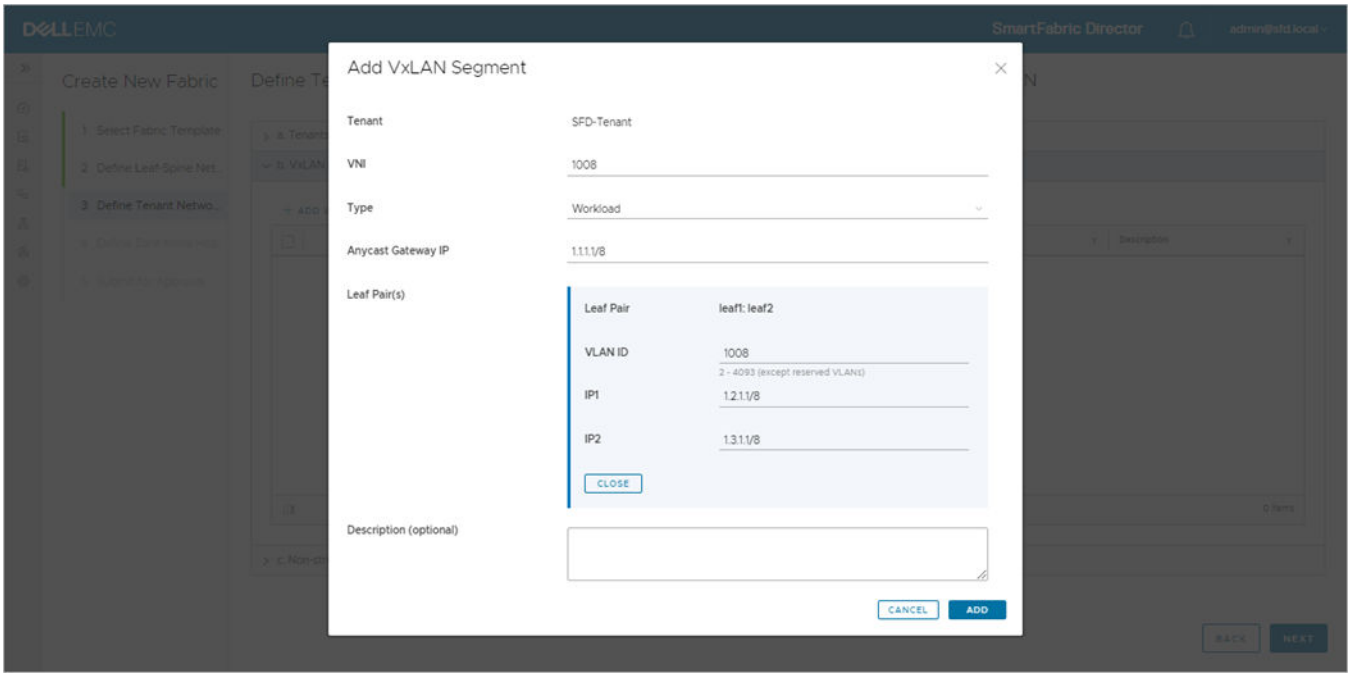
3. Select the leaf pairs from the drop-down.



Distributed anycast gateway is the default gateway that enables the use of the same gateway IP address across all leaf switches that are part of the VxLAN network. This ensures that each leaf switch can function as the default gateway for the workloads that are directly connected to it.

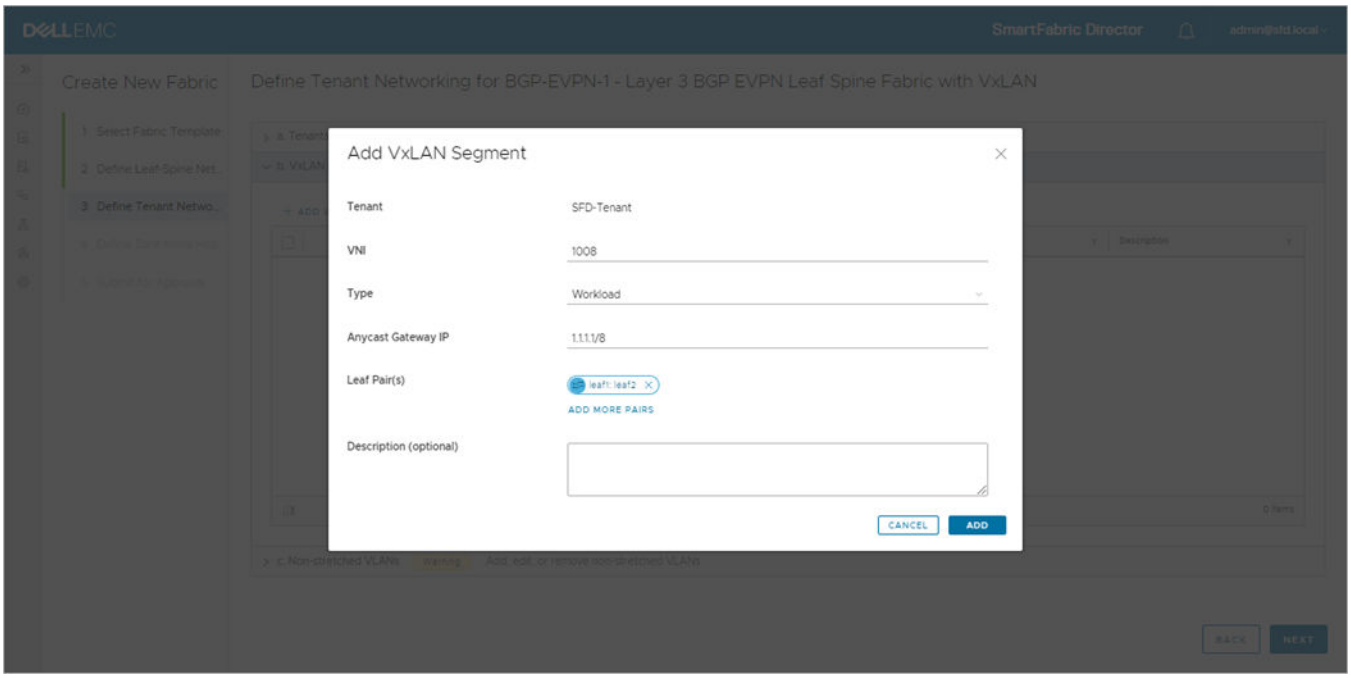
This feature facilitates flexible workload placement, host mobility, and optimal traffic forwarding across the VxLAN fabric. The specified anycast gateway IP address is used across all the leaf switches that are part of the VxLAN segment.

4. Specify the racks where the workloads belonging to a given VxLAN segment reside, then click **Close**.



The selected leaf pair displays. For each rack that would host these workloads, a local VLAN must be specified for the ToR pair. This local VLAN is associated with a specific VxLAN segment on the specified leaf pair. As in host networking, for L3 BGP fabric, the IP addresses for the two VIPs must be specified.

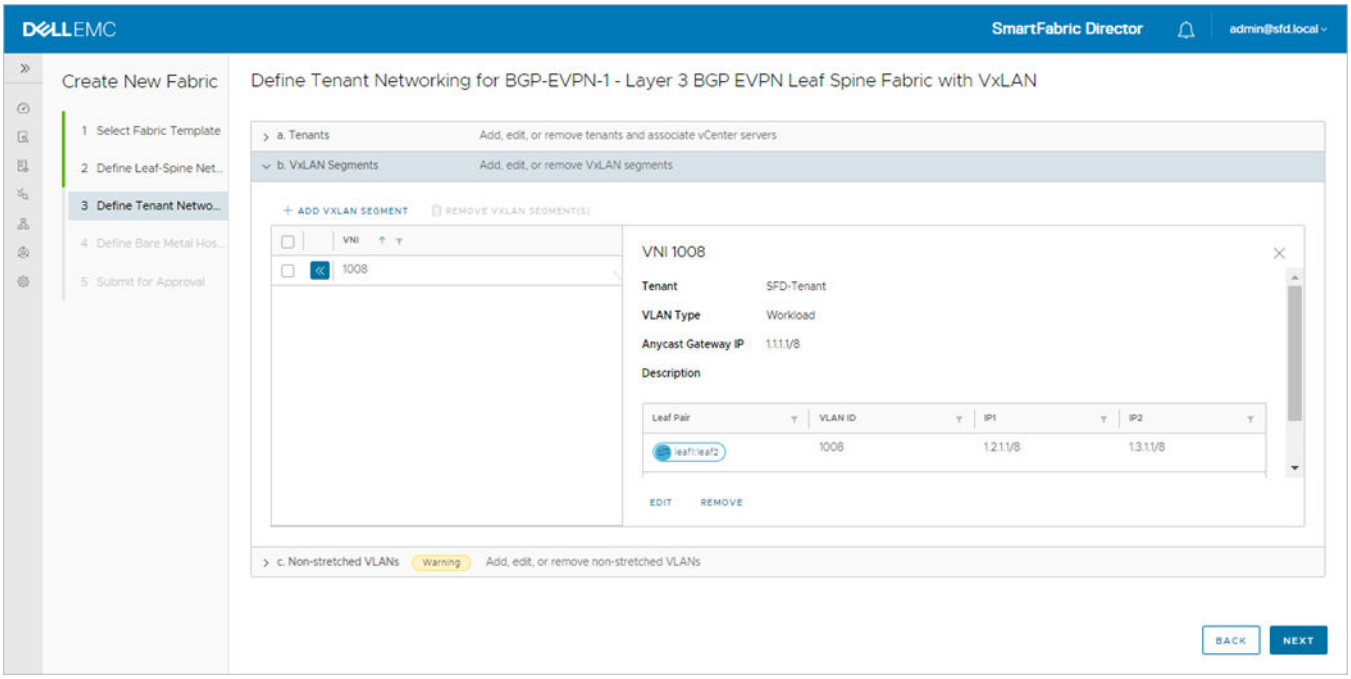
5. Click **Add more pairs** to specify additional leaf pairs corresponding to the racks where workloads can be placed.



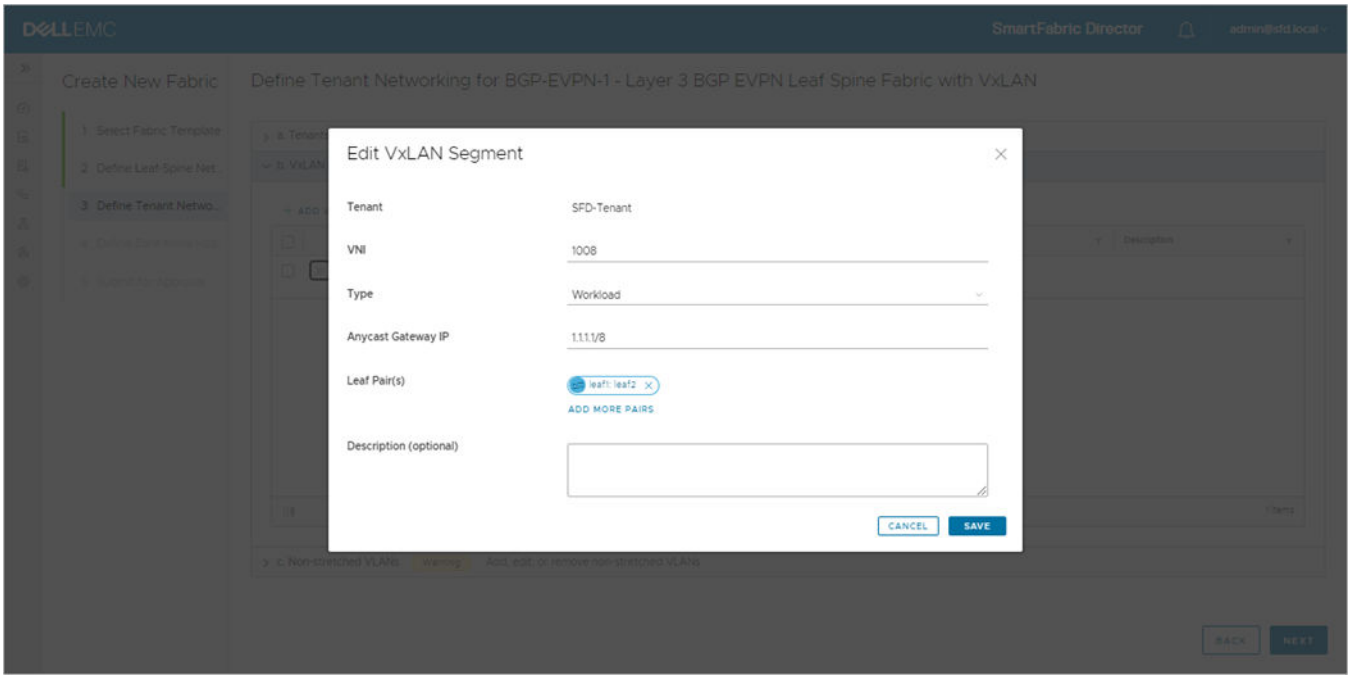
6. (Optional) Repeat the steps to add more leaf pairs, then click **Add**.

VxLAN segments

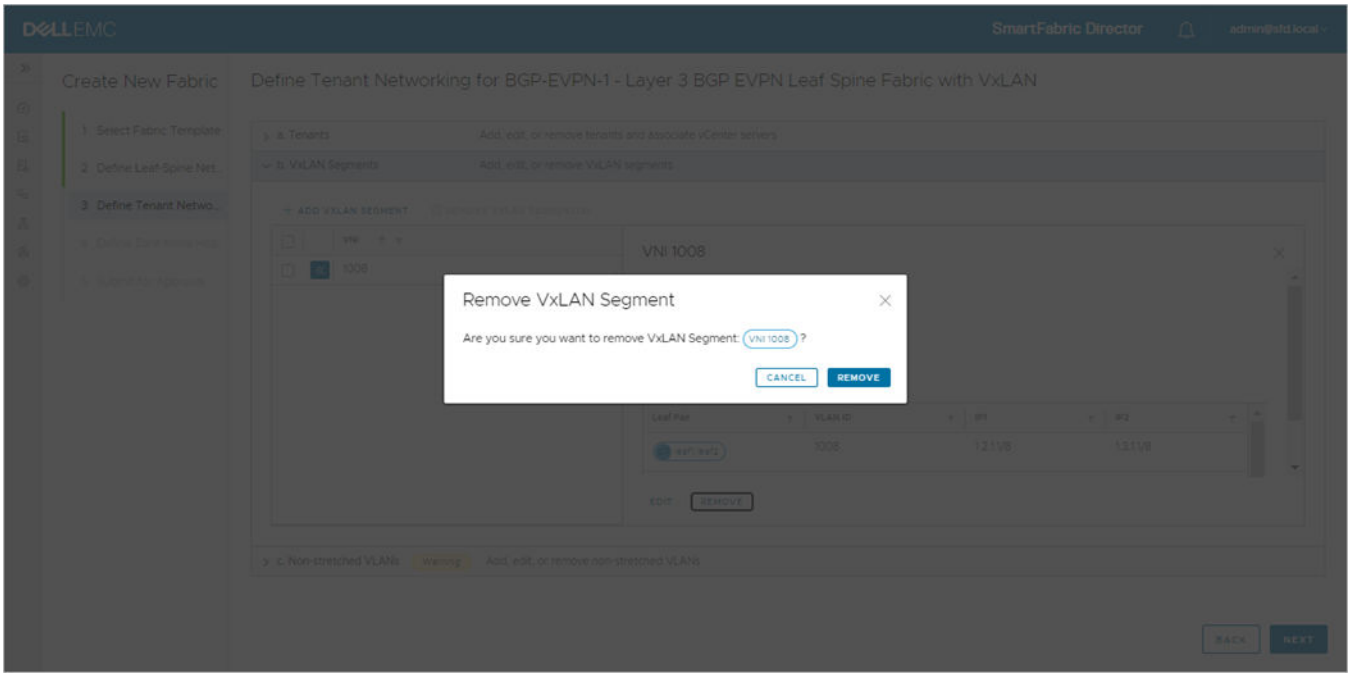
1. Each newly added VxLAN segment displays. Click **>>** to view the parameter configuration for each new segment.



2. Click **Edit** to modify an existing VxLAN segment.



3. Make changes, then click **Save** or **Cancel** to discard the changes.
4. (Optional) Click **Remove** to delete the selected VxLAN segment, then click **Remove** again to confirm deletion. You can also click **Cancel** to cancel the operation.



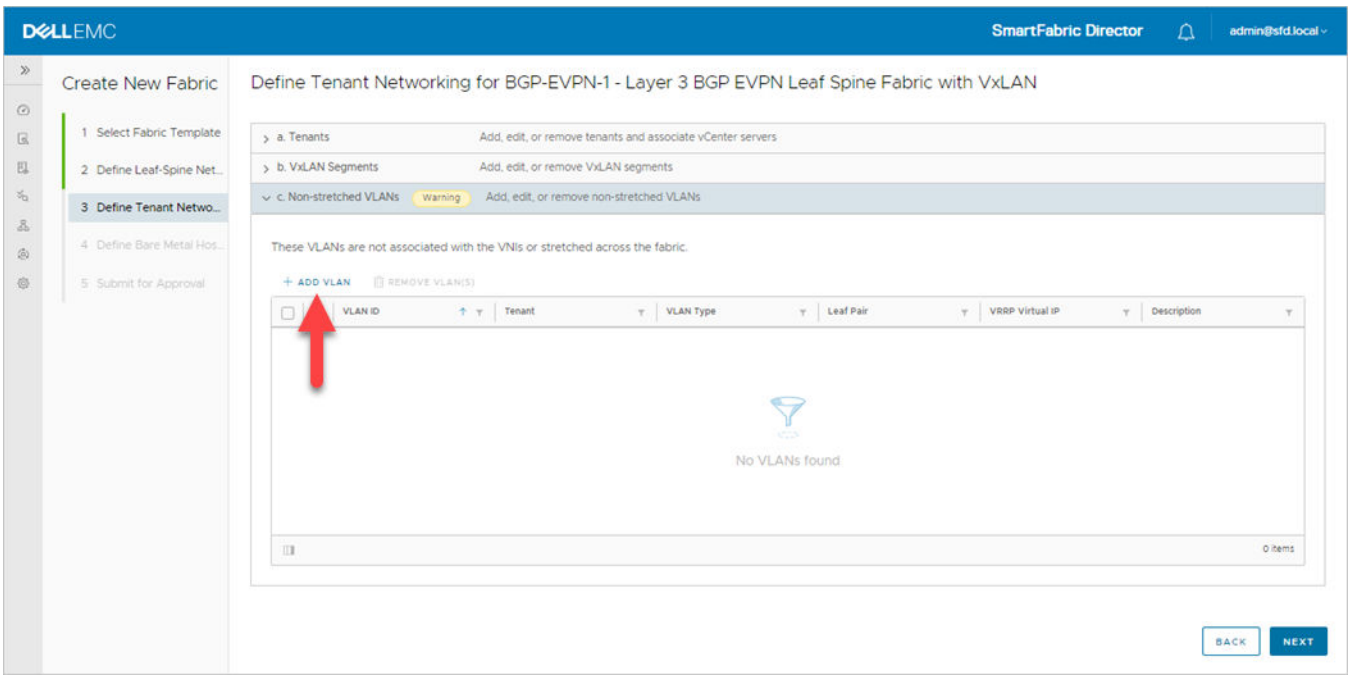
5. (Optional) Select multiple VxLAN segments to remove more than one, then select **Remove VxLAN segments**.
6. (Optional) All selected VxLAN segments are listed. Click **Remove** or **Cancel**.

Non-stretched VLANs

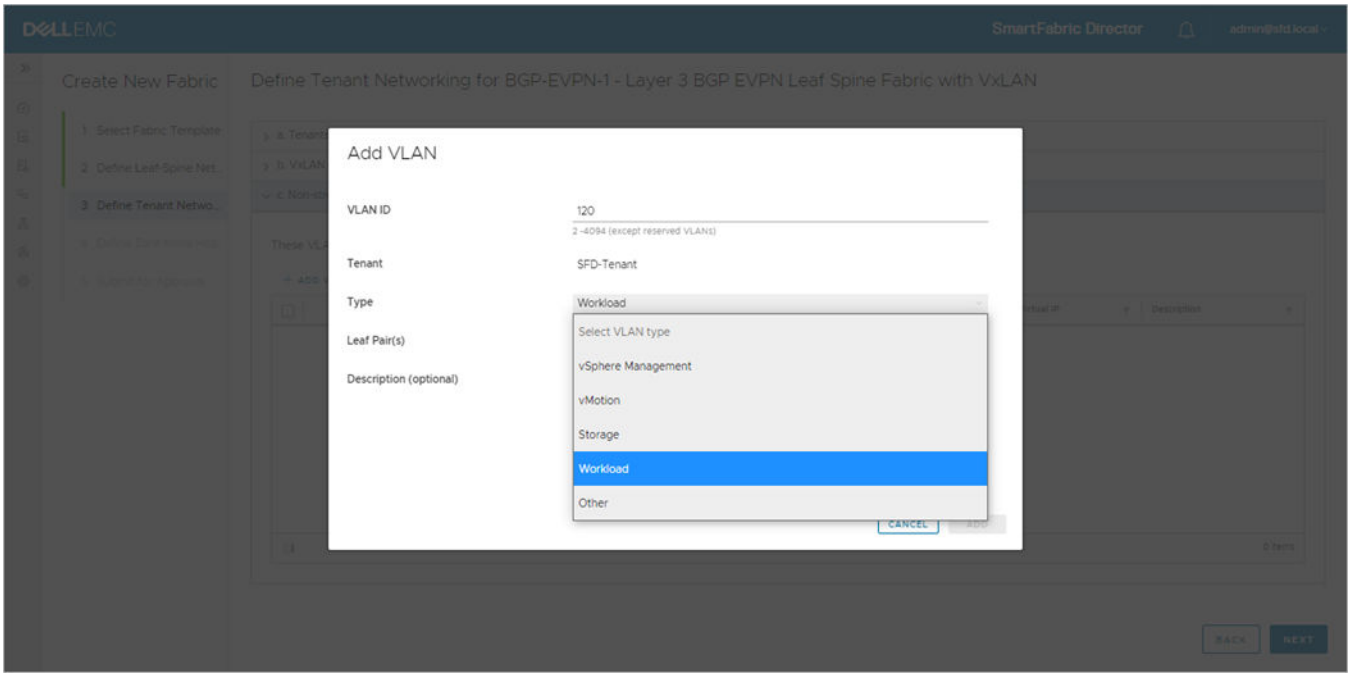
You may have workloads in more than one data center across Layer 3 boundaries. It does not need to be placed in a VxLAN segment, but you must define the VLAN. VLANs defined for these are local to a rack (leaf pair), and are not stretched across racks.

NOTE: If all workloads are placed in more than one rack, skip these steps and click **Next**.

1. Select **> c. Non-stretched VLANs**, then click **Add VLAN**.

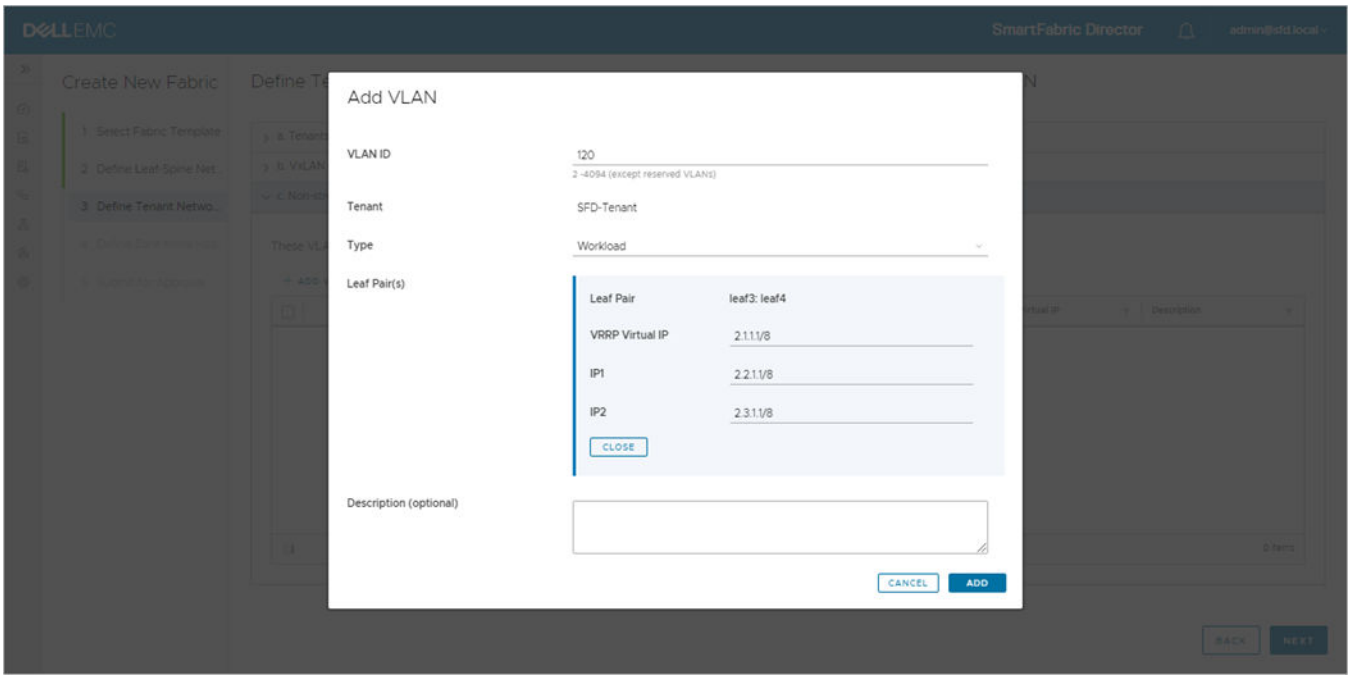


2. Specify a unique VLAN ID which belongs to a specific tenant. The VLAN ID cannot be used for any other VxLAN segment or other nonstretched VLANs.

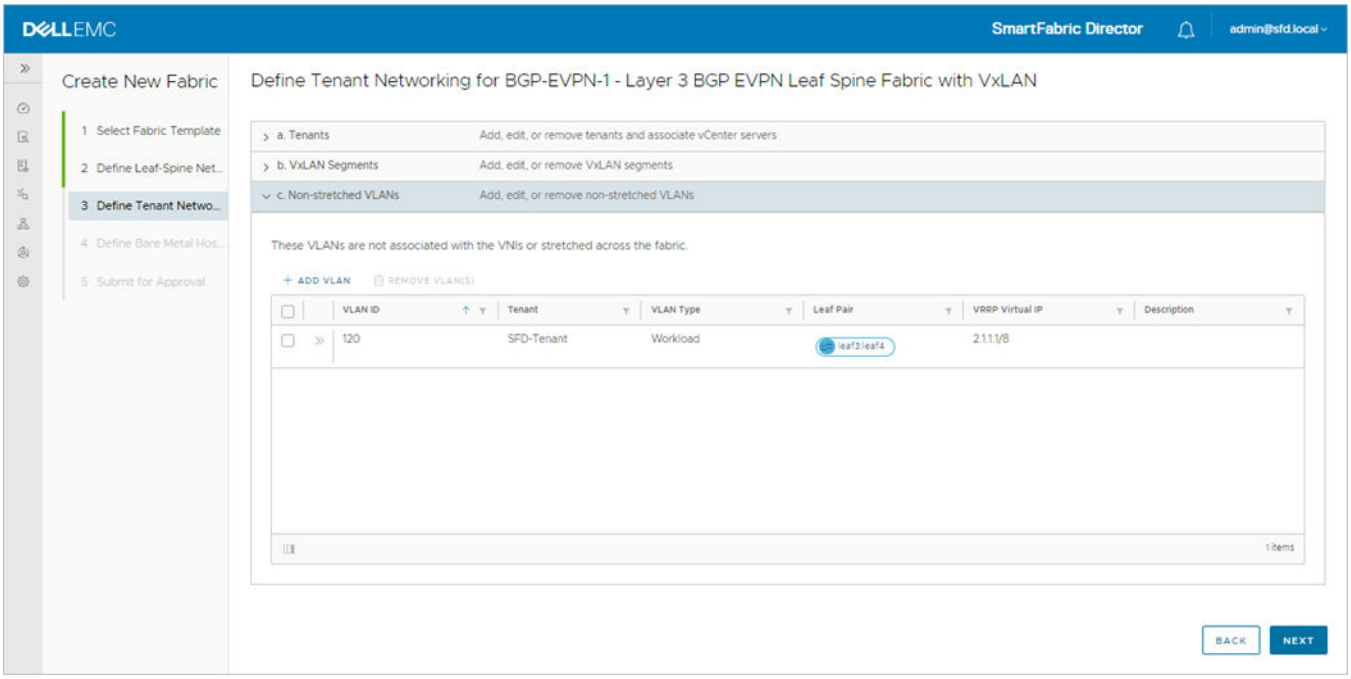


NOTE: SFD 2.0 only supports a single tenant. This field is automatically populated.

3. Select the leaf-pair (ToRs) of the rack where the workload are placed from the drop-down.
4. Specify the VLAN for the ToR pair, specify the two VIPs required, then click **Close**.



5. (Optional) Click **Add more pairs** if you have more hosts or workloads which are part of the same VLAN but in different racks. Configure the additional leaf pairs, then click **Close**.
6. (Optional) Click **Add**.
7. The added nonstretched VLANs display in the VLAN table. Click **>>** to view more information, then click **Next**.

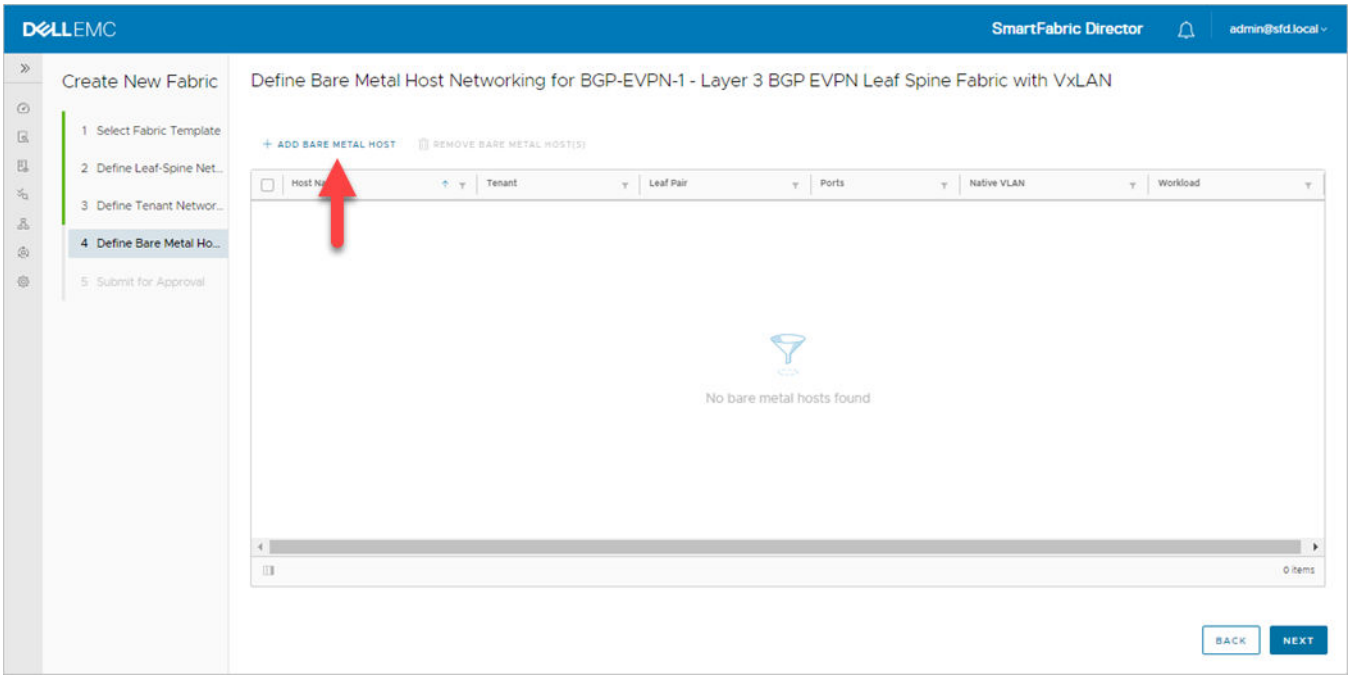


Define bare metal host networking

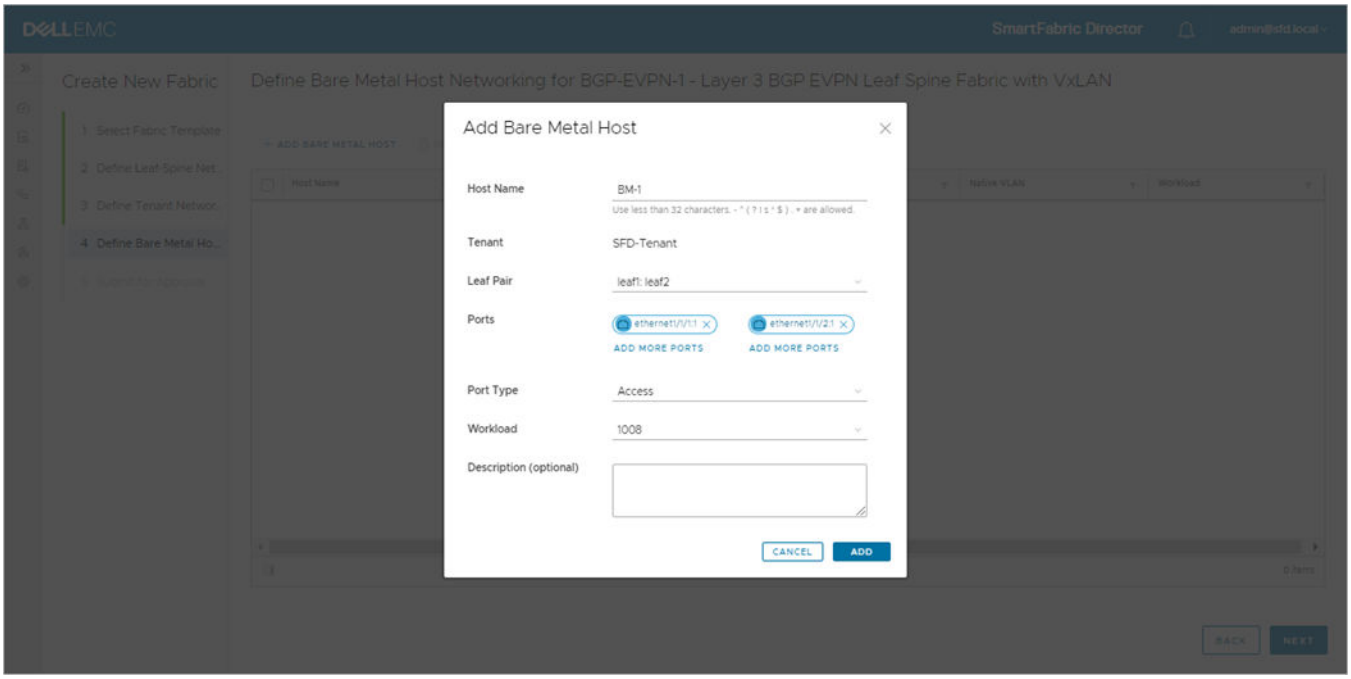
Not all applications can be virtualized, and you may need to deploy non-virtualized workloads. Hosts used to deplay non-virtualized workloads are called *bare metal hosts*. SFD 2.0 supports bare metal hosts.

NOTE: Define bare metal host networking is an optional step. Bare metal is required to add a VLAN in access or trunk mode. If there are no non-virtualized workloads (bare metal hosts), you can skip this step.

1. Click **Add bare metal host**.

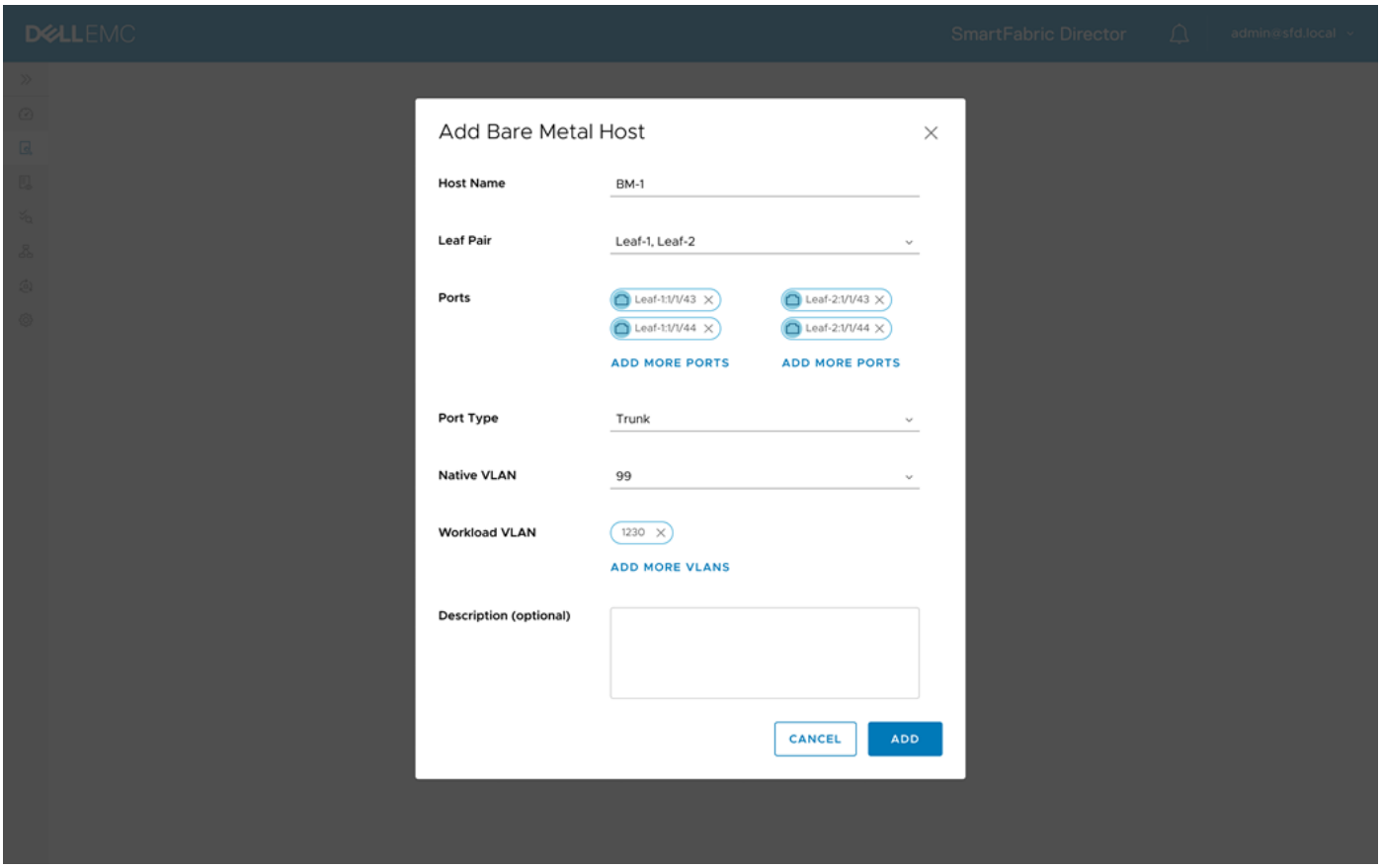


2. Enter the Host Name to identify the VLT pair to which the host is connected to, then select the Leaf Pair.

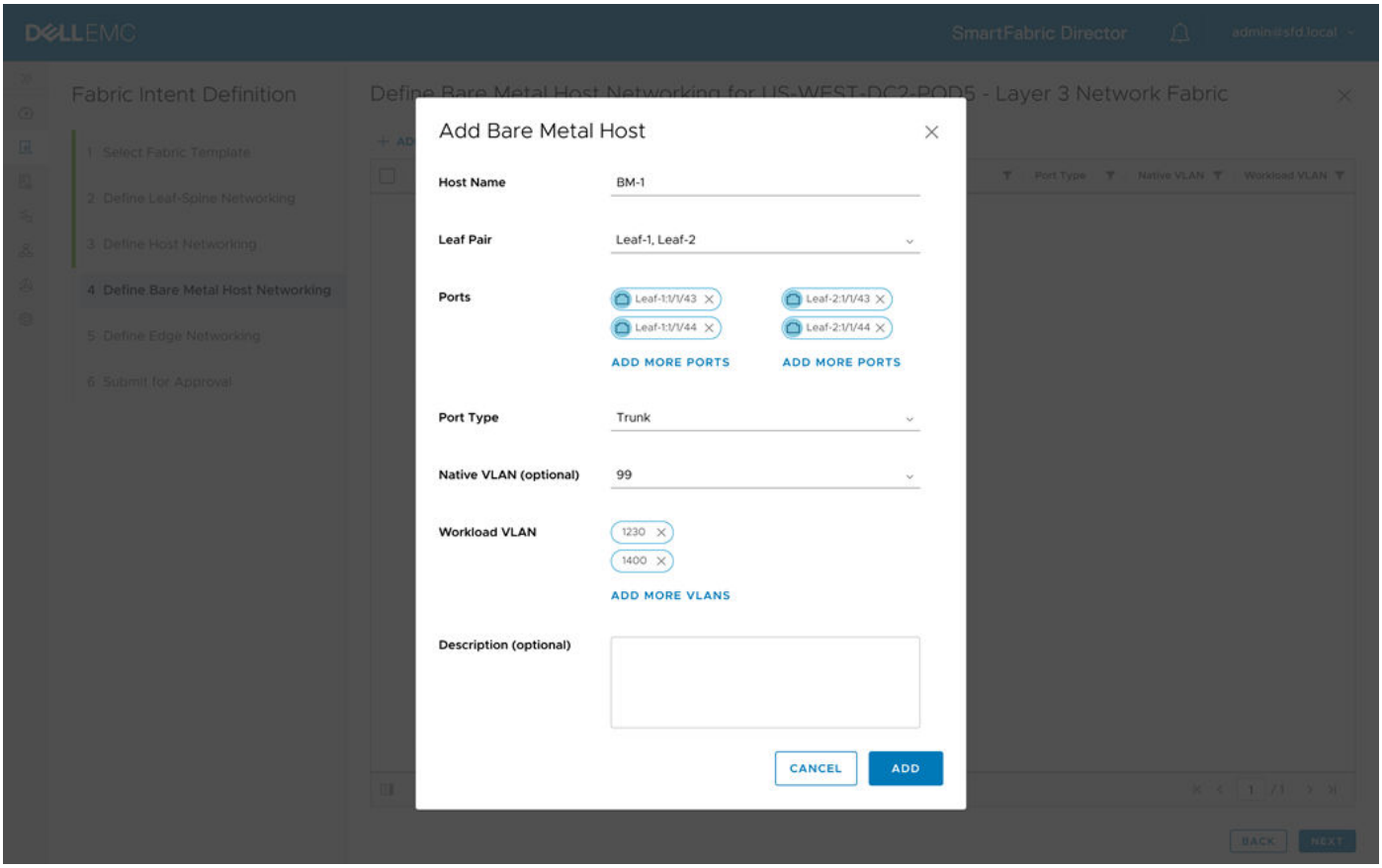


3. Specify one or more switch ports that the server is connected to, select Access or Trunk for the port type, select the workload VLAN, an optional description, then click **Add**.

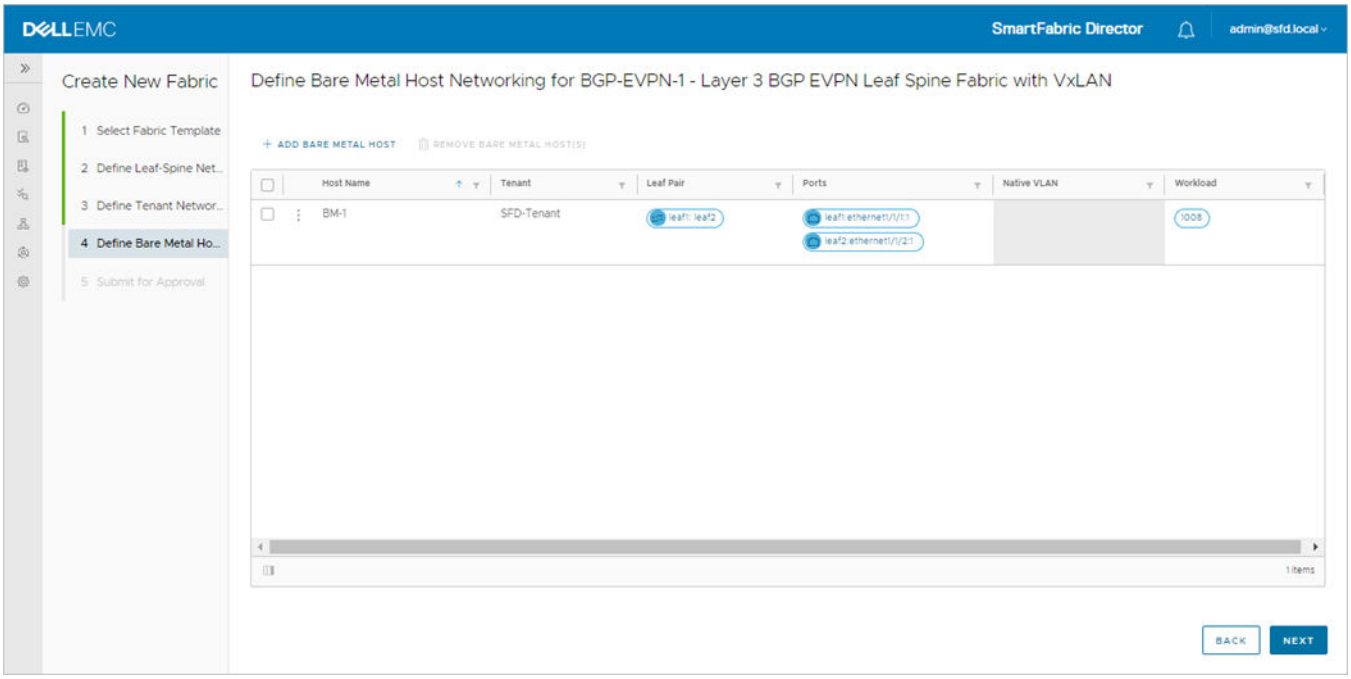
   A trunk port type requires a native VLAN in addition to the workload VLAN. The switch default configuration has a native VLAN, and the switch native VLAN option is prepopulated. If you select trunk as the port type and would like to specify the native VLAN explicitly, enter a VLAN number. Similar to an access port type, a workload VLAN needs to be specified.



4. With a trunk port, the host can have more than one workload VLAN. Click **Add more VLANs** to add additional workload VLANs, then click **Add**.



5. The configured bare metal host displays in the bare metal host table. Click **Next** to proceed to edge networking.

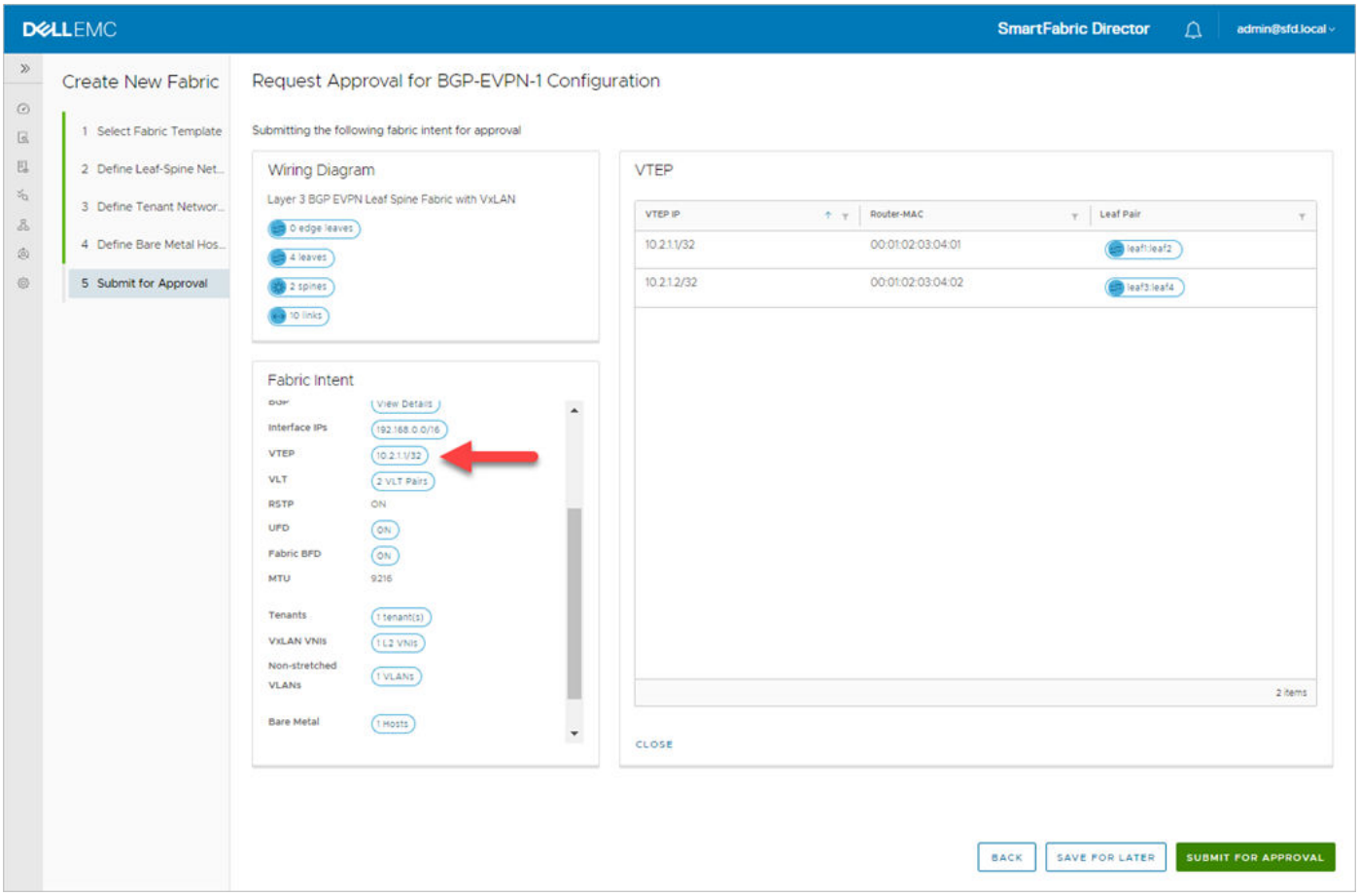


6. (Optional) Select the bare metal host, click the three dots, then select **Edit** to modify the configuration.

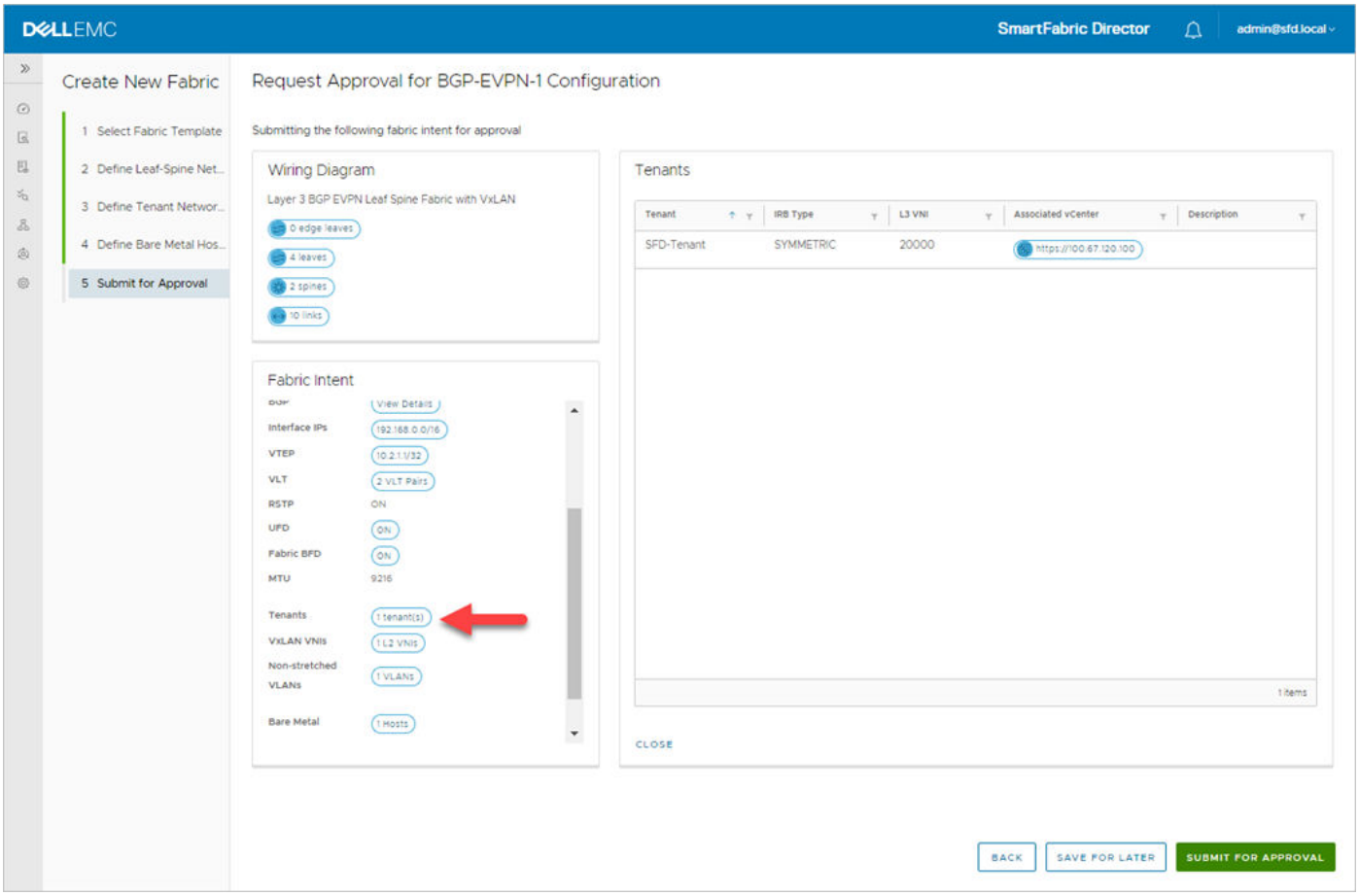
Submit for approval

Once the fabric intent is complete, you can then submit it for approval. A summary of the wiring diagram and the fabric intent displays. Select on the tiles provides details of that specific parameter.

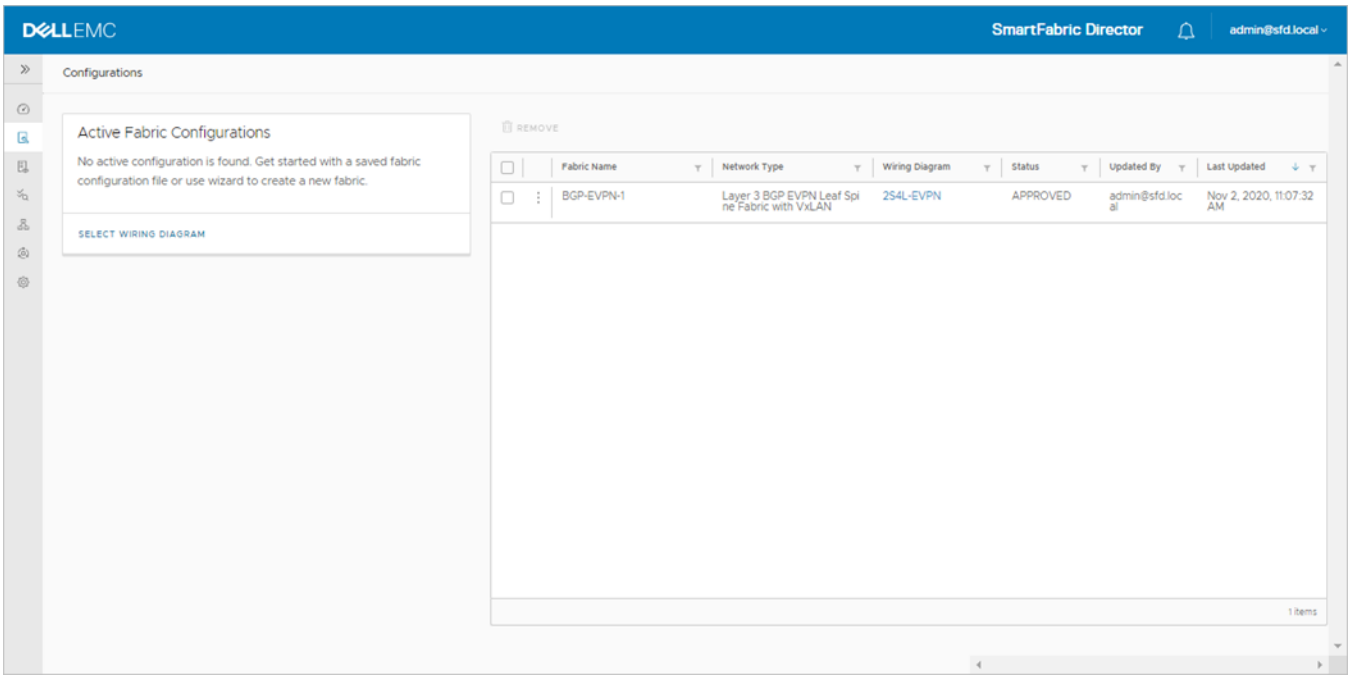
1. Click **VTEP** within the fabric intent to view VTEP intent details.



2. Click **Tenants** to view tenant intent details.

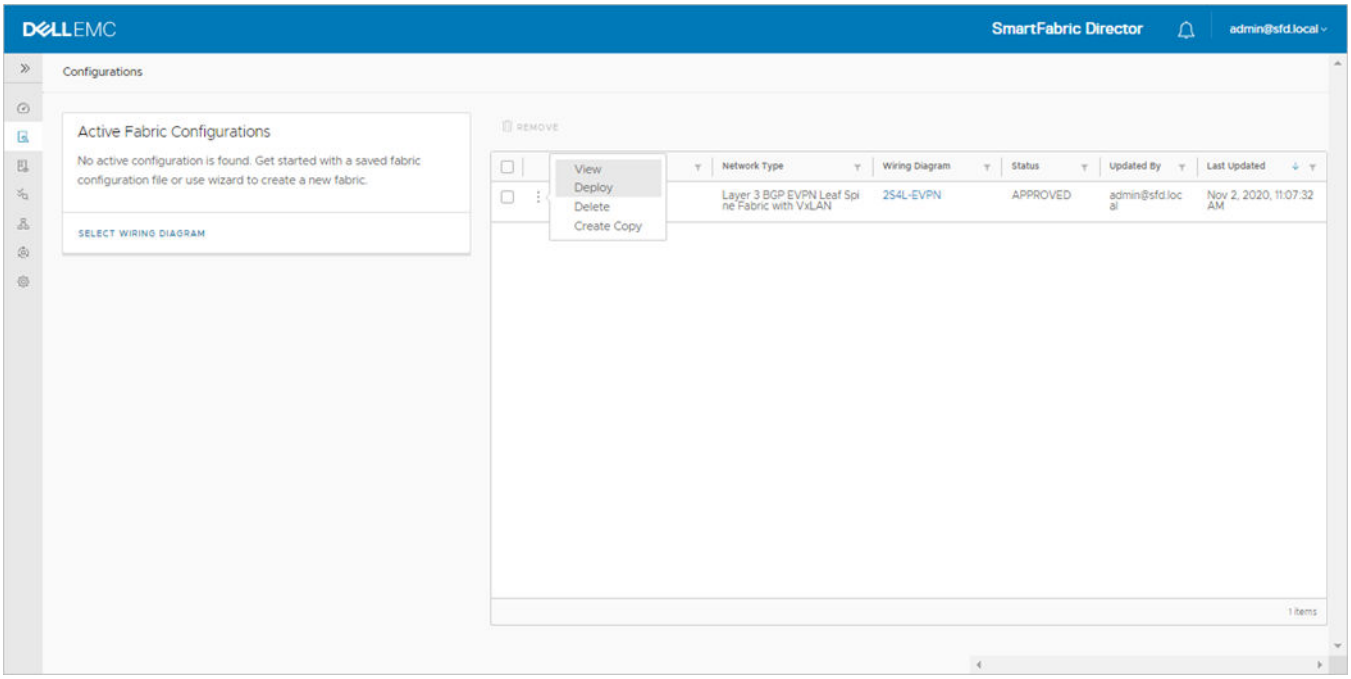


3. Click **Submit for approval** to submit the fabric intent. Click **Back** to return to the previous step, or click **Save for later**.

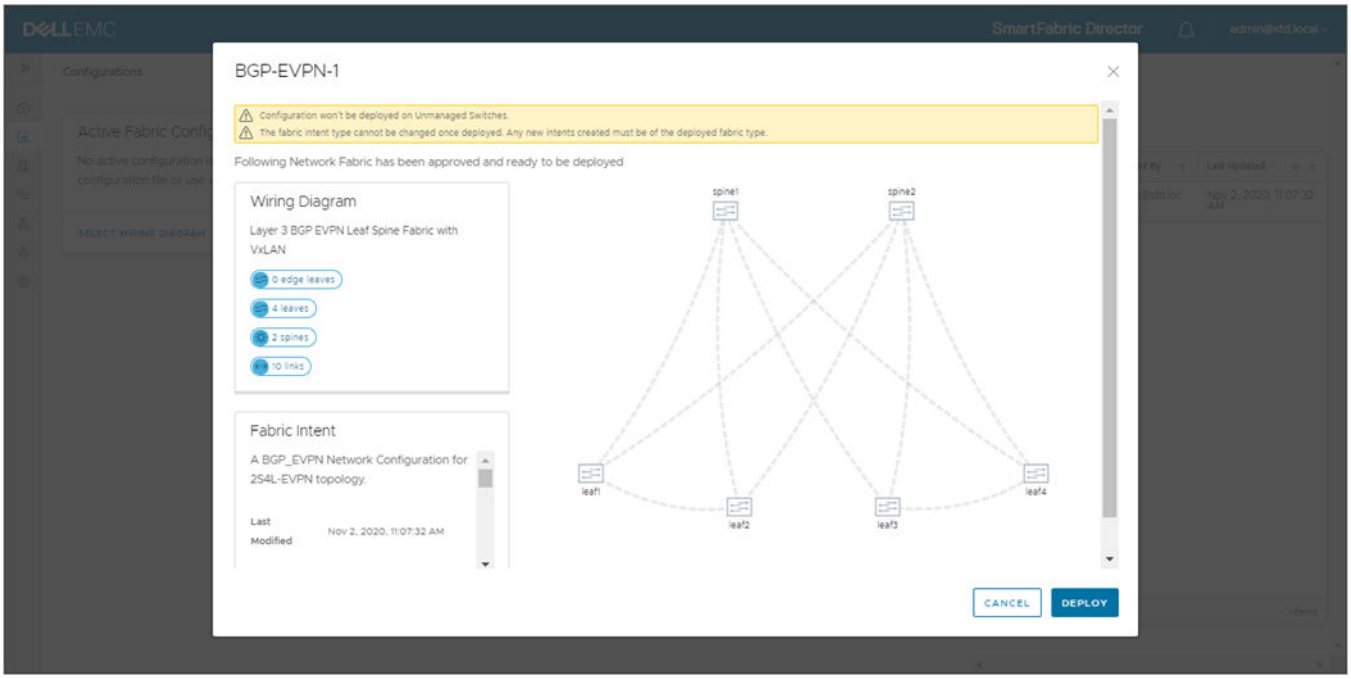


Deploy an approved fabric intent

1. Once the fabric intent is approved, you are ready to deploy the fabric so SFD can configure each switch based on the intent. Select the fabric intent, click the three dots, then select **Deploy**.

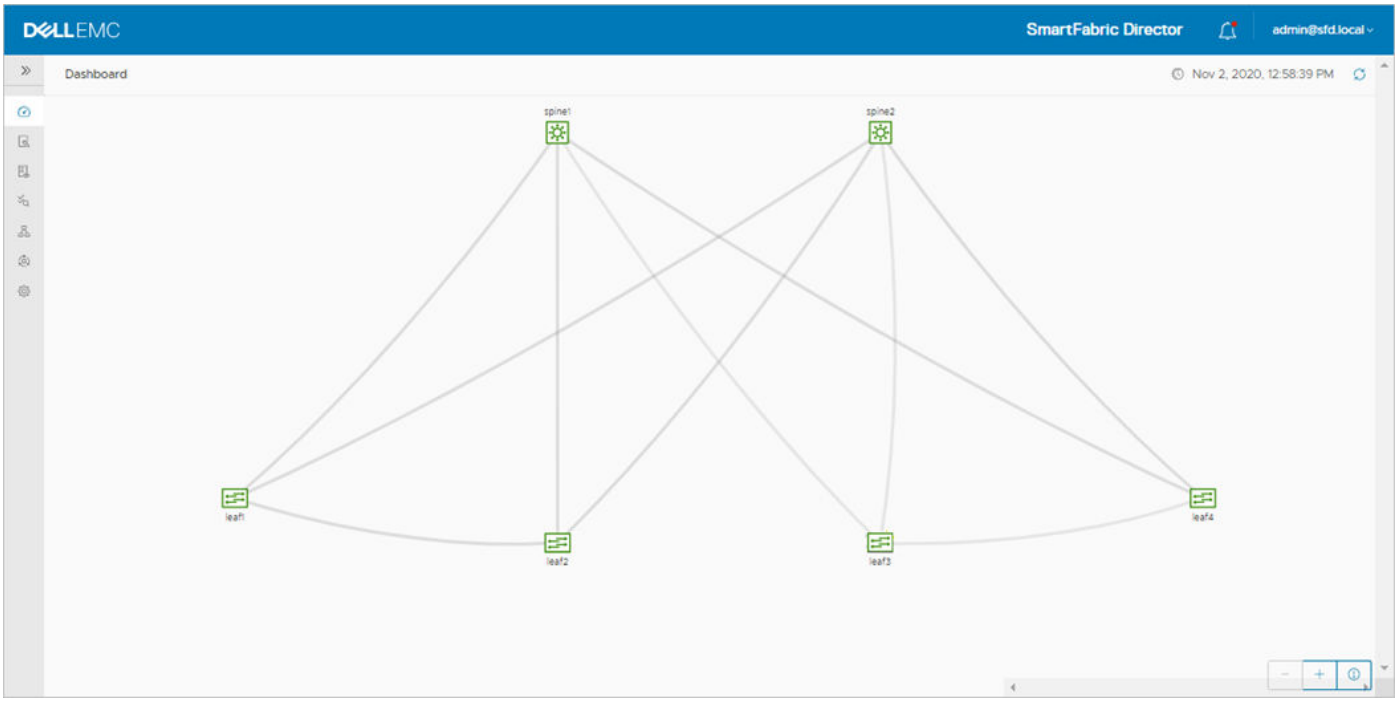


2. Once the fabric intent is approved, you are ready to deploy the fabric so SFD can configure each switch based on the intent. Select the fabric intent, click the three dots, then select **Deploy**.



NOTE: You can optional select View prior to Deploy.

SFD starts configuring each switch, and the progress displays on the dashboard. As each switch is successfully configured, the switch turns green.

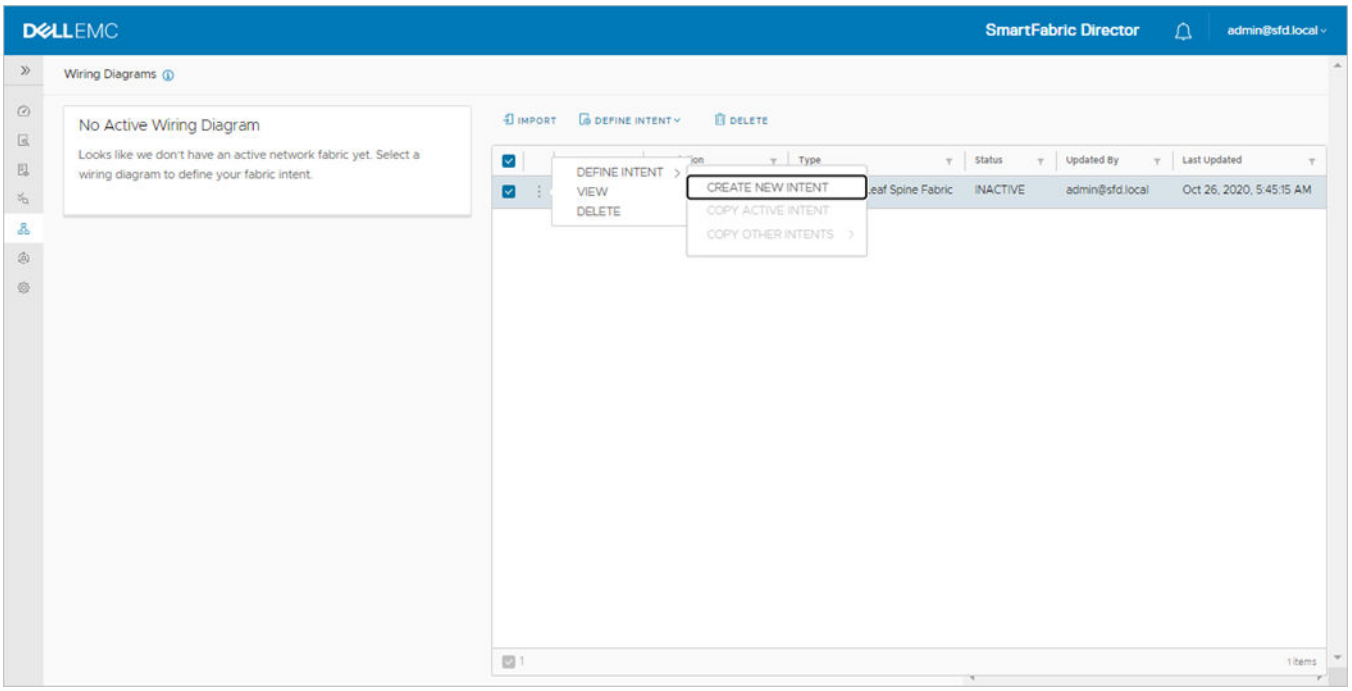


Details of the deployment can be viewed in the SFD notifications page.

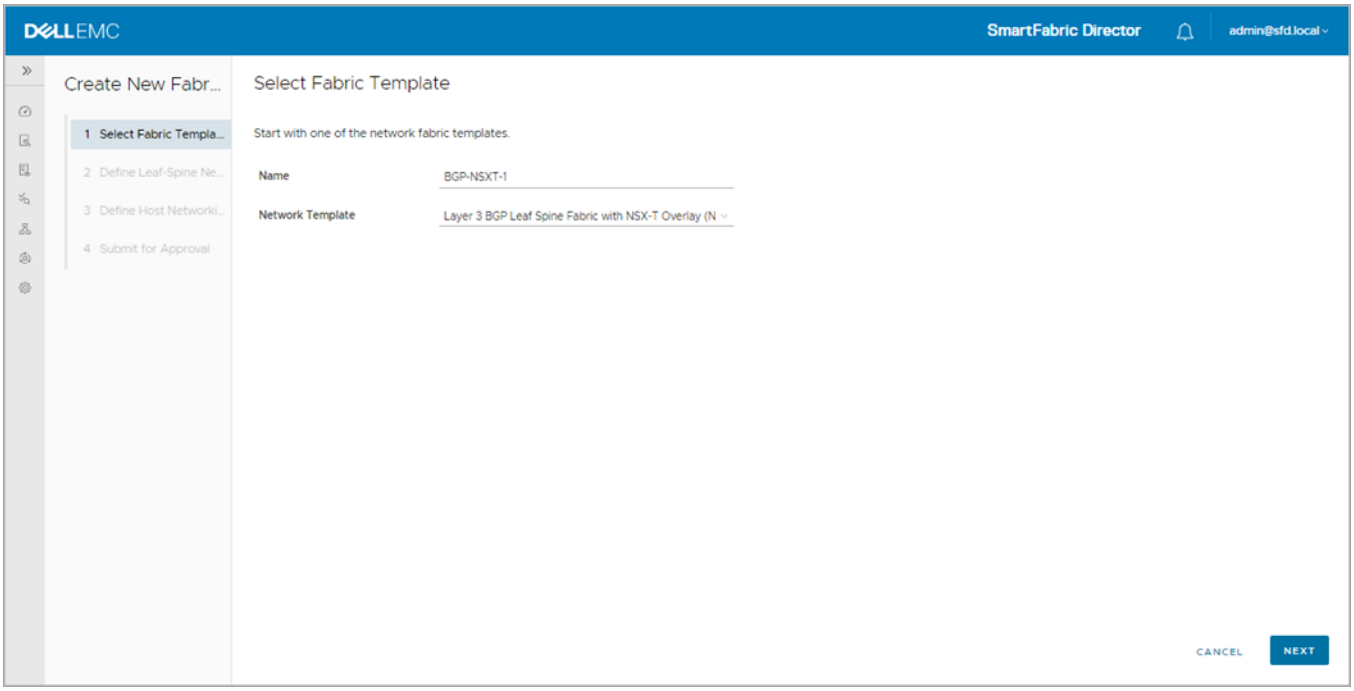
Layer 3 BGP leaf spine fabric with NSX-T overlay

Select fabric template

1. Select the fabric, then **Define intent** > **Create new intent**. If modifying an active intent, make a copy of an intent from the table of intents (active or otherwise), then make the necessary changes.

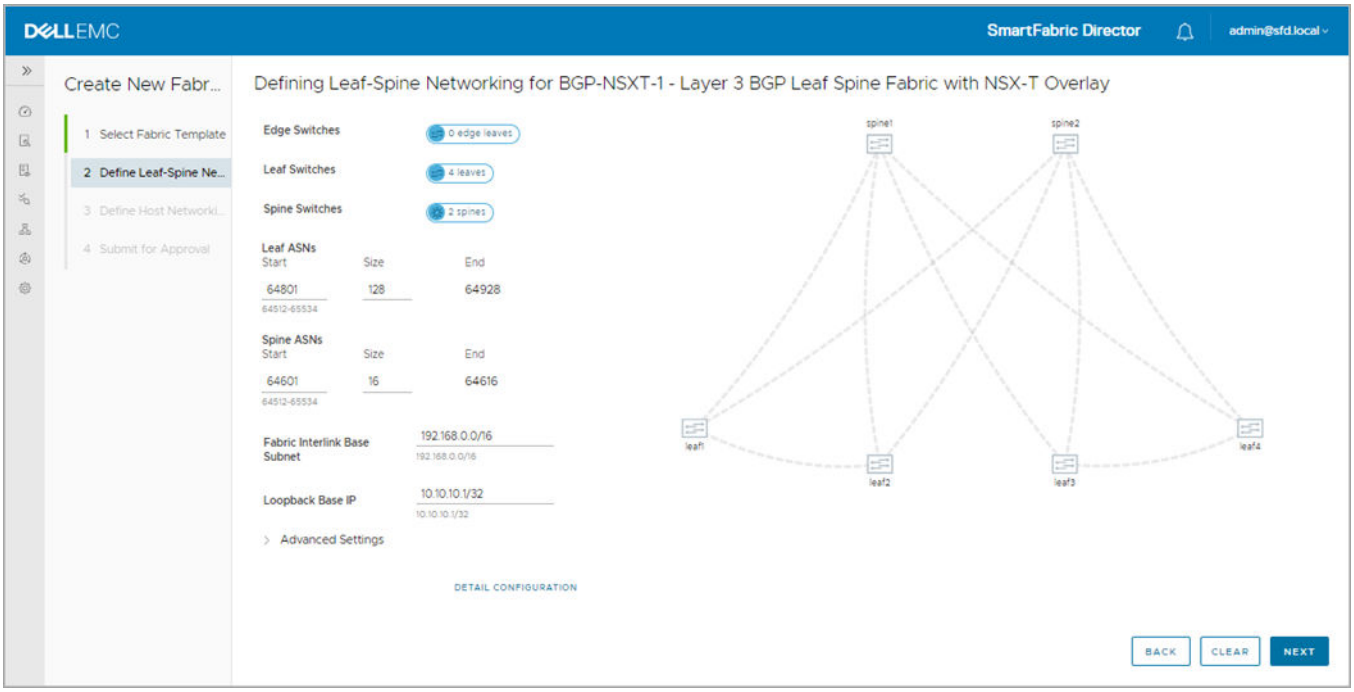


2. Select **Layer 3 BGP leaf spine fabric with NSX-T Overlay**, then click **Next**.



Define leaf spine networking

1. It is recommended to keep the default values for the leaf and spine ASNs to allow for future expansion. If the size is made restrictive, adding spine or leaf pair switches could result in failure due to nonavailability of ASNs. Click **Advanced settings**.

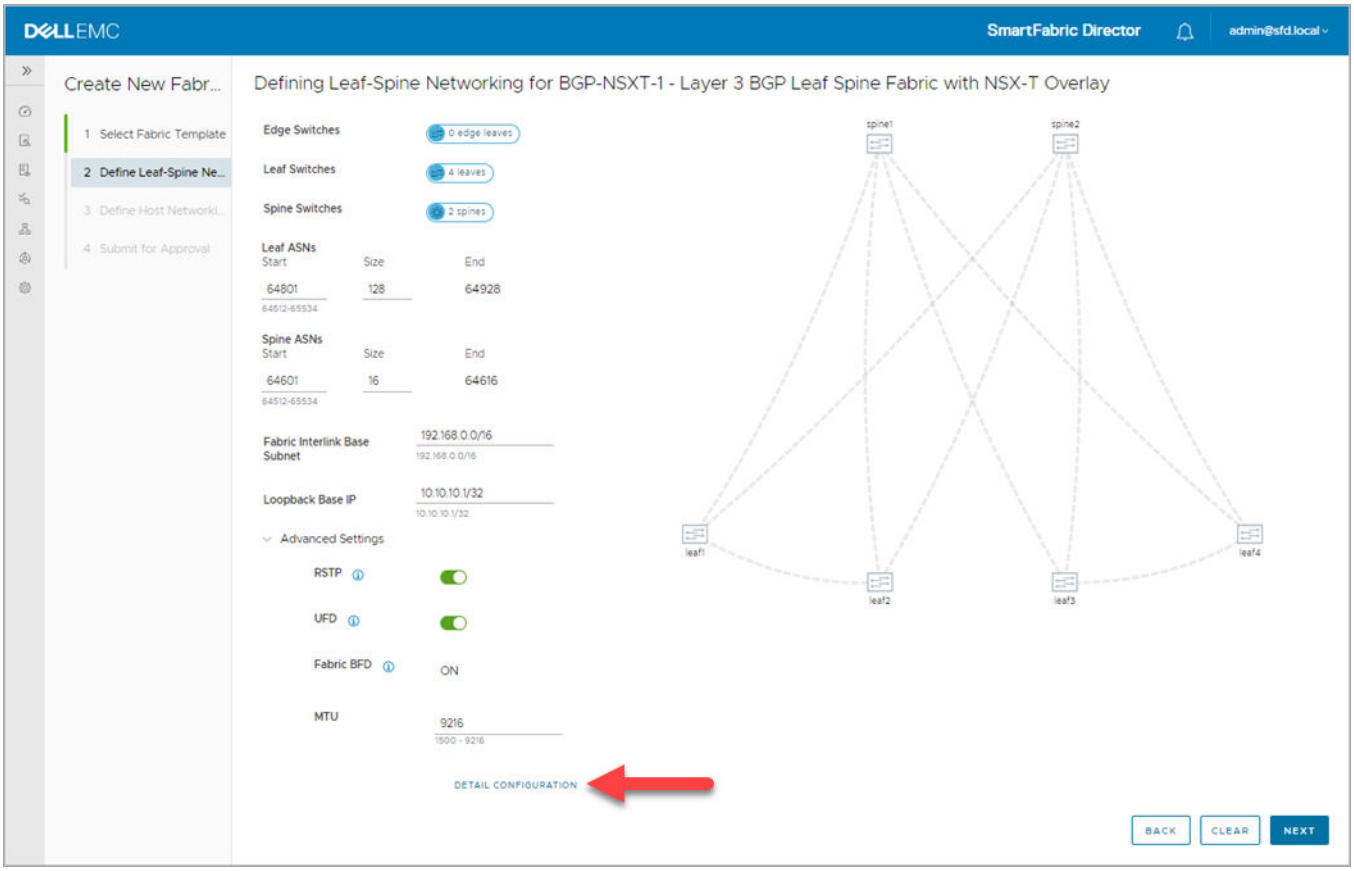


2. Specify the base addresses to be used as the starting point for allocation. SFD allocates the interlink subnets, IP address to the loopback interfaces, and the VTEP IP address for each switch. These addresses are used within the fabric.

   If switches are removed and added back, the individual IP addresses assigned to the newly added switch may not be in monotonically increasing order and it is not guaranteed that a previously allocated IP address is reused.

   The functionality of the fabric is not dependent on any specific order that the addresses are allocated by SFD. There cannot be duplicate IP addresses within the fabric, and the addresses must be within range starting with the specified base value.

3. Enable rapid spanning-tree protocol (**RSTP**) to ensure a loop-free topology. Disabling STP would disable the functionality on all switches in the fabric.



4. Enable uplink failure detection (**UFD**) to detect the loss of upstream connectivity. An uplink state group is configured on each leaf switch, creating an association between the uplinks to the spins and the downlink interfaces.

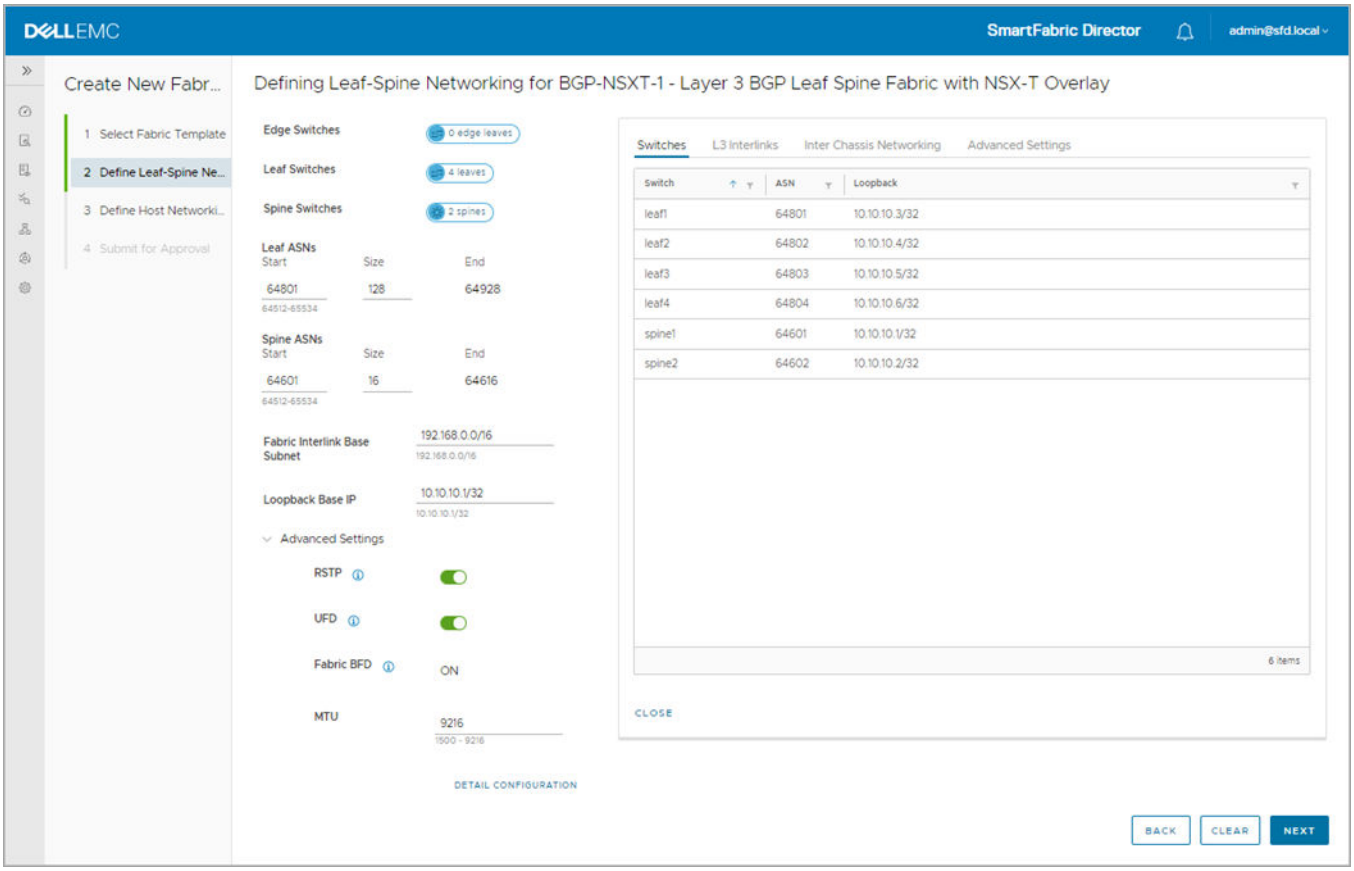
   If all uplinks fail on a switch, UFD automatically shuts down the downstream interfaces. This propagates to the hosts attached to the leaf switch. The host then uses its link to the remaining switch to continue sending traffic across the leaf-spine network. Disabling UFD disables the functionality on all switches in the fabric.

   Bi-directional forwarding detection (BFD) is a network protocol that is used to detect faults between two forwarding engines connected by a link. It provides low-overhead detection of faults, even on physical media that does not support failure detection of any kind (such as Ethernet). BFD is enabled by default on all switches in a fabric and cannot be modified.

5. Specify the maximum transmission unit (**MTU**) for the fabric (default 9216).

   SFD ensures that the MTU is set to the specified value on all switches in the fabric. VxLAN is an overlay technology that has an overhead due to the VxLAN header. A lower MTU value could result in slower throughput.

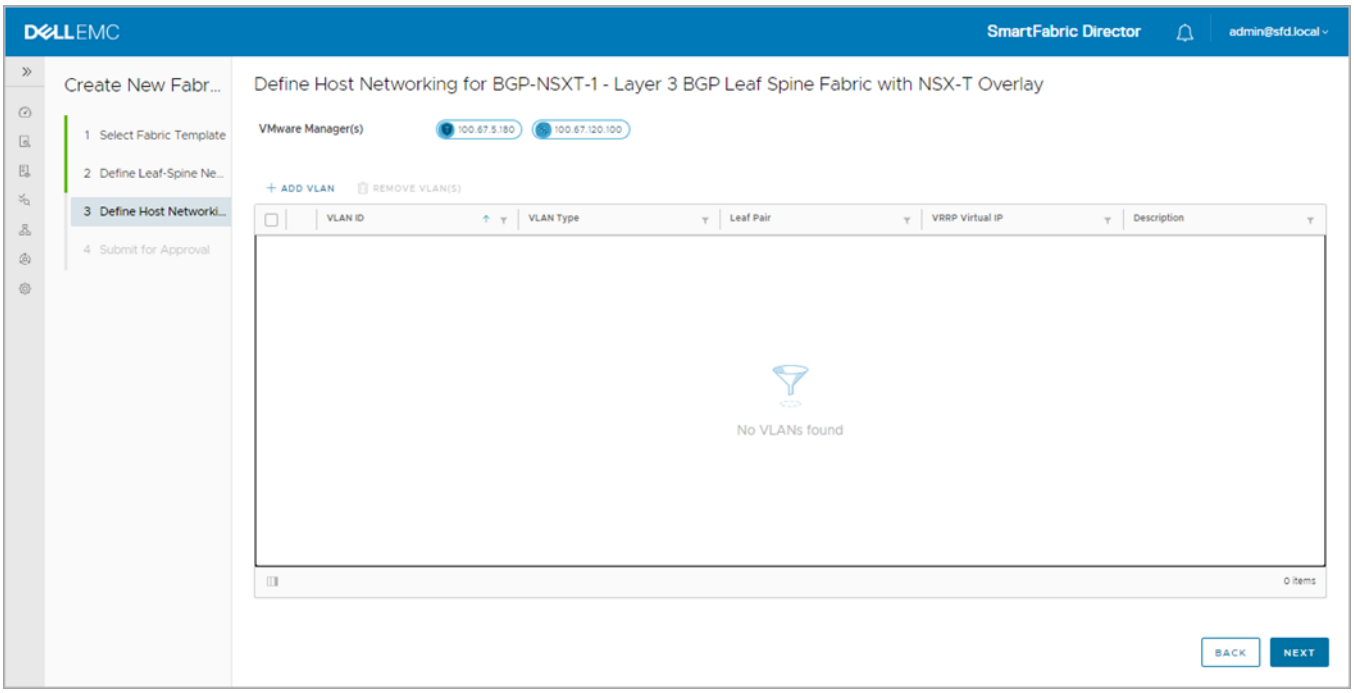
6. Click **Detail configuration** to view the per switch configuration parameters allocated by SFD, then click **Next**.



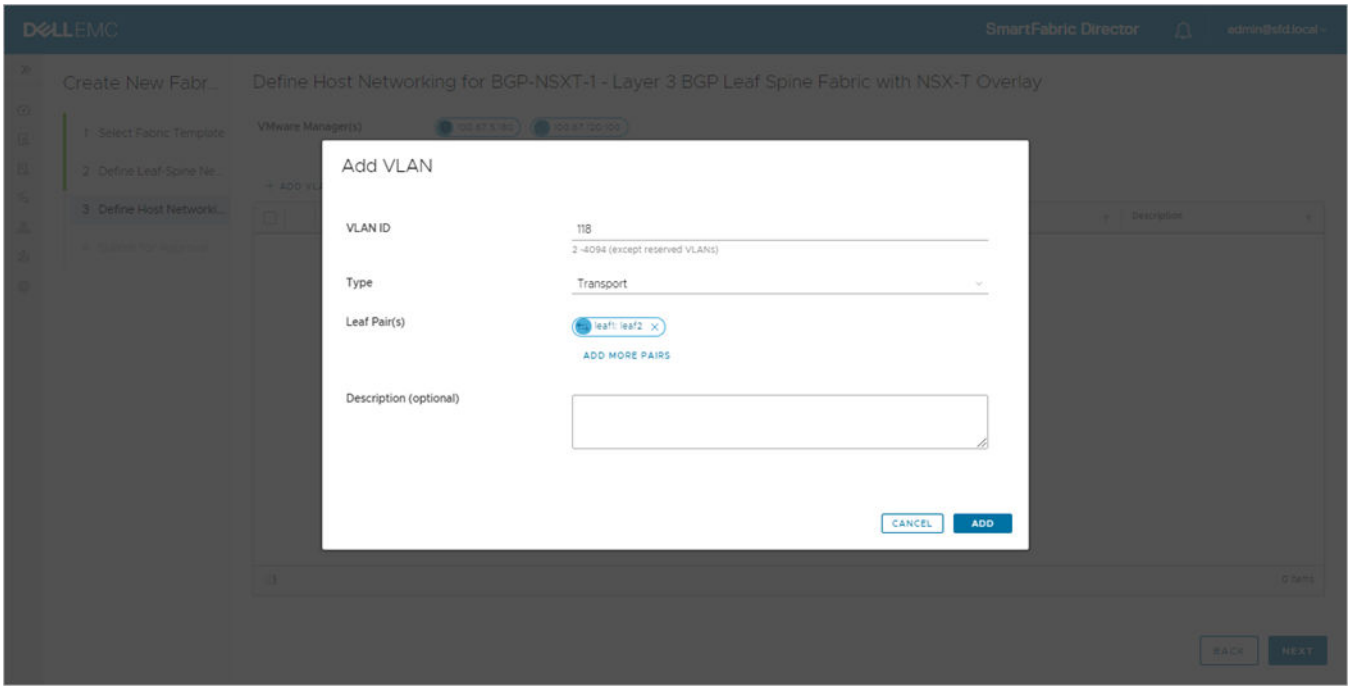
Define host networking

You can specify configuration to support servers carrying virtualized workloads, which are managed by NSX-T Manager. SFD interfaces with NSX-T Manager to retrieve the port group information when a workload (VM) is deployed. It uses the workload to configure the switch to bind the port to the VLAN.

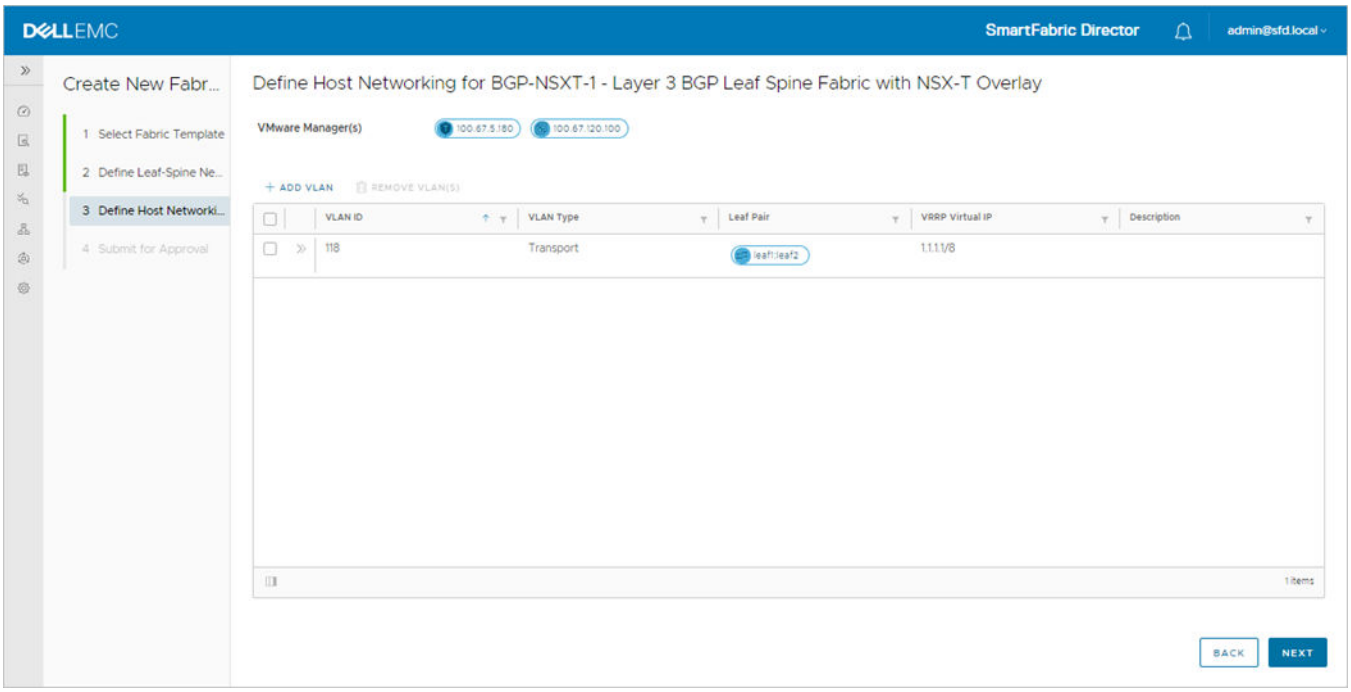
1. Click **Add VLAN** to add the configuration for each port group for the NSX-T Manager, then click **Next**.



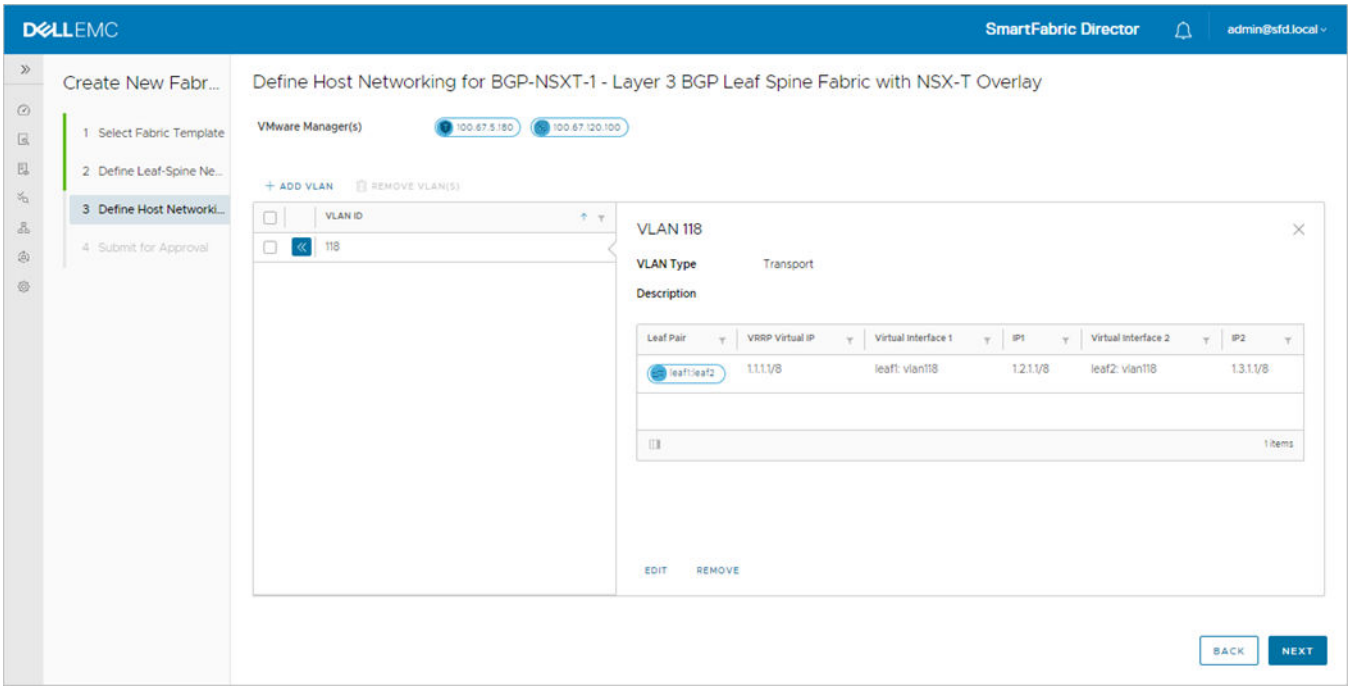
2. Enter the VLAN ID corresponding to the port group, select the Type, then associate one or more VLT pairs to a VLAN ID from the list of available VLT pairs (from the wiring diagram).



3. (Optional) Click **Add more pairs** and repeat the steps.
4. Enter an optional description, then click **Add**. Each leaf in the VLT pair has its own SVI IP, and each VLAN in the VLT pair has a VRRP virtual IP in the same subnet as the VLAN.

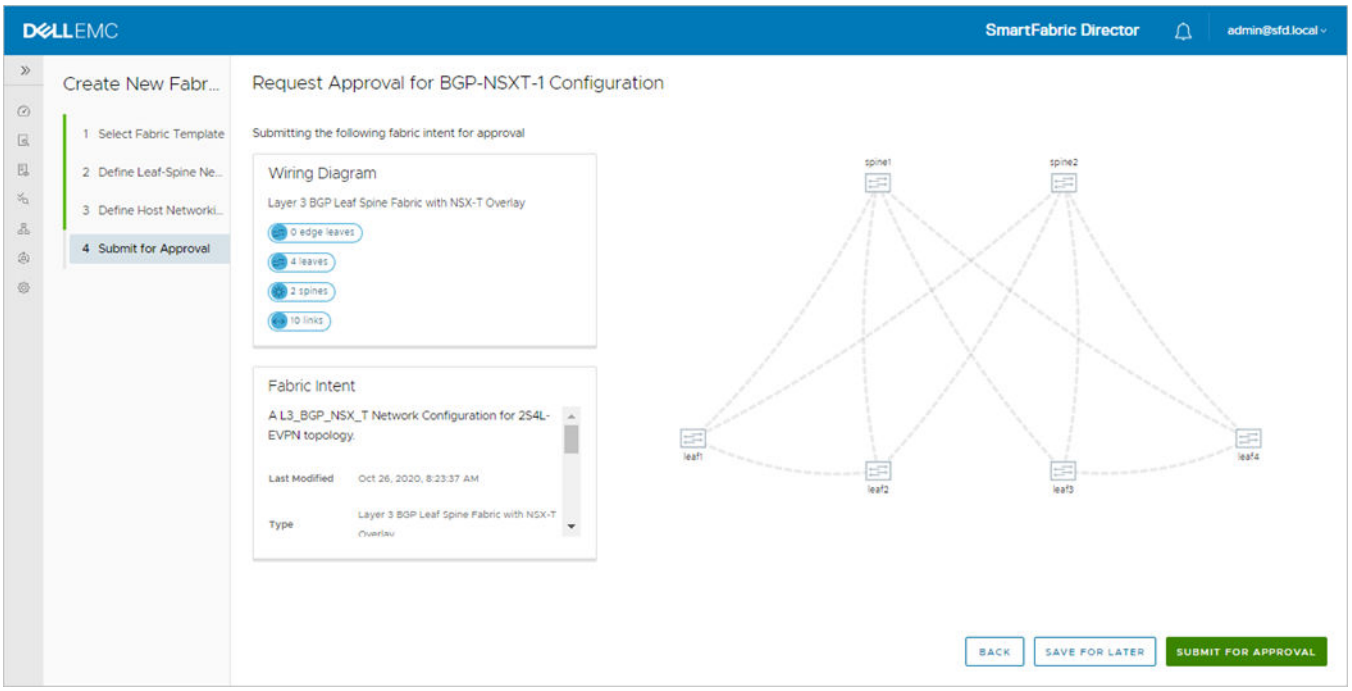


5. Click **>>** to provide more details, then click **Next**.



Submit for approval

Once the fabric intent is complete, you can then submit it for approval. A summary of the wiring diagram and the fabric intent displays. Select on the tiles provides details of that specific parameter.

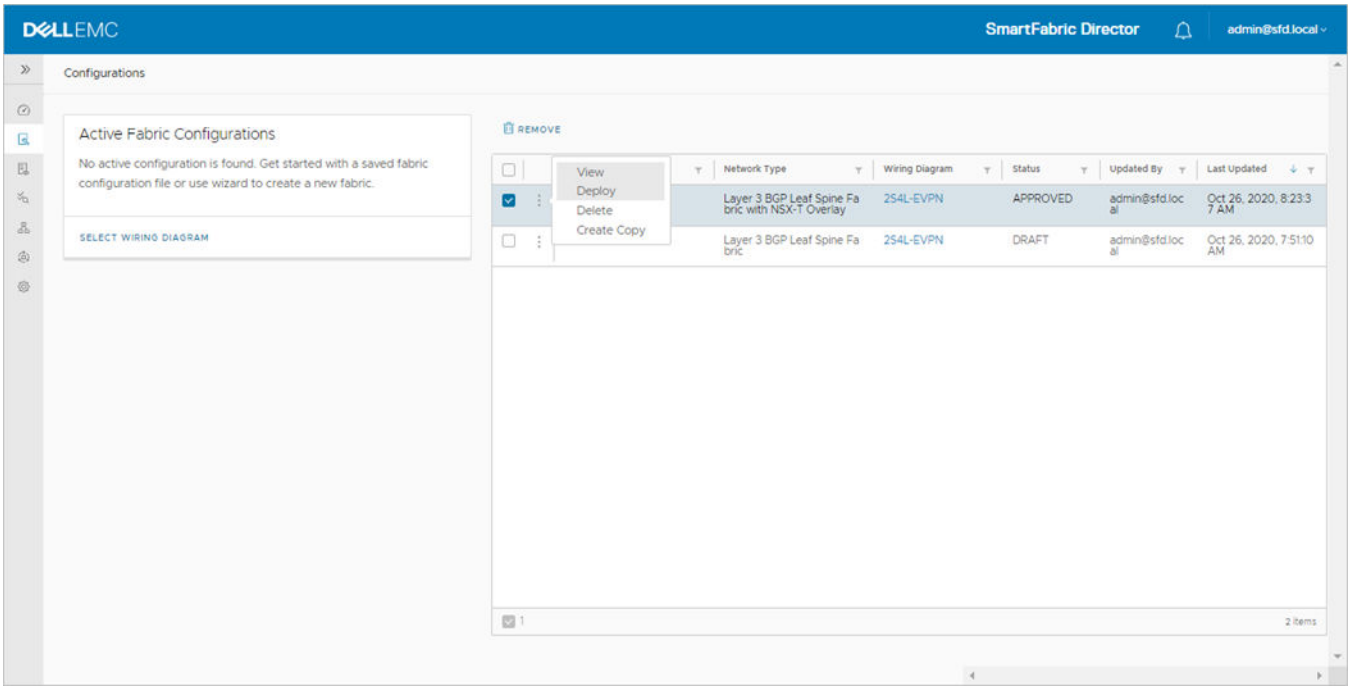


Deploy an approved fabric intent

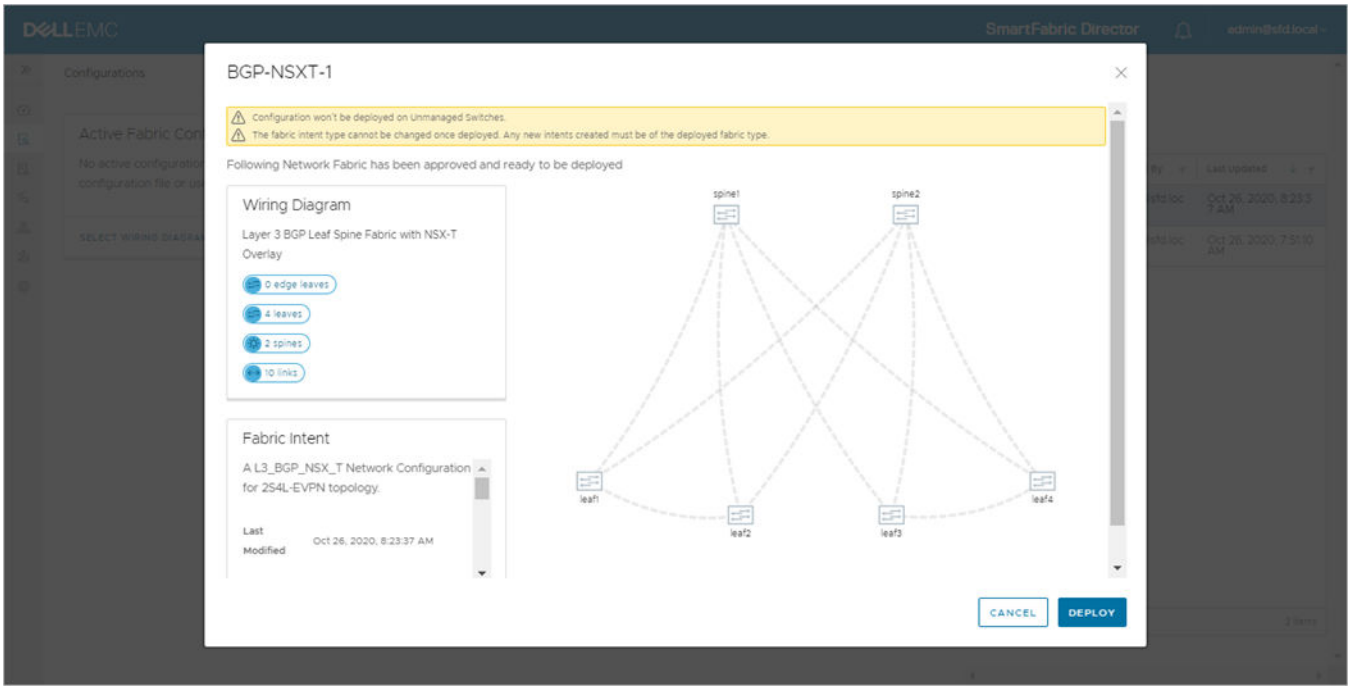
Once the fabric intent is approved, you are ready to deploy the fabric so SFD can configure each switch based on the intent.

1. Select the fabric intent, click the three dots, then select **Deploy**.

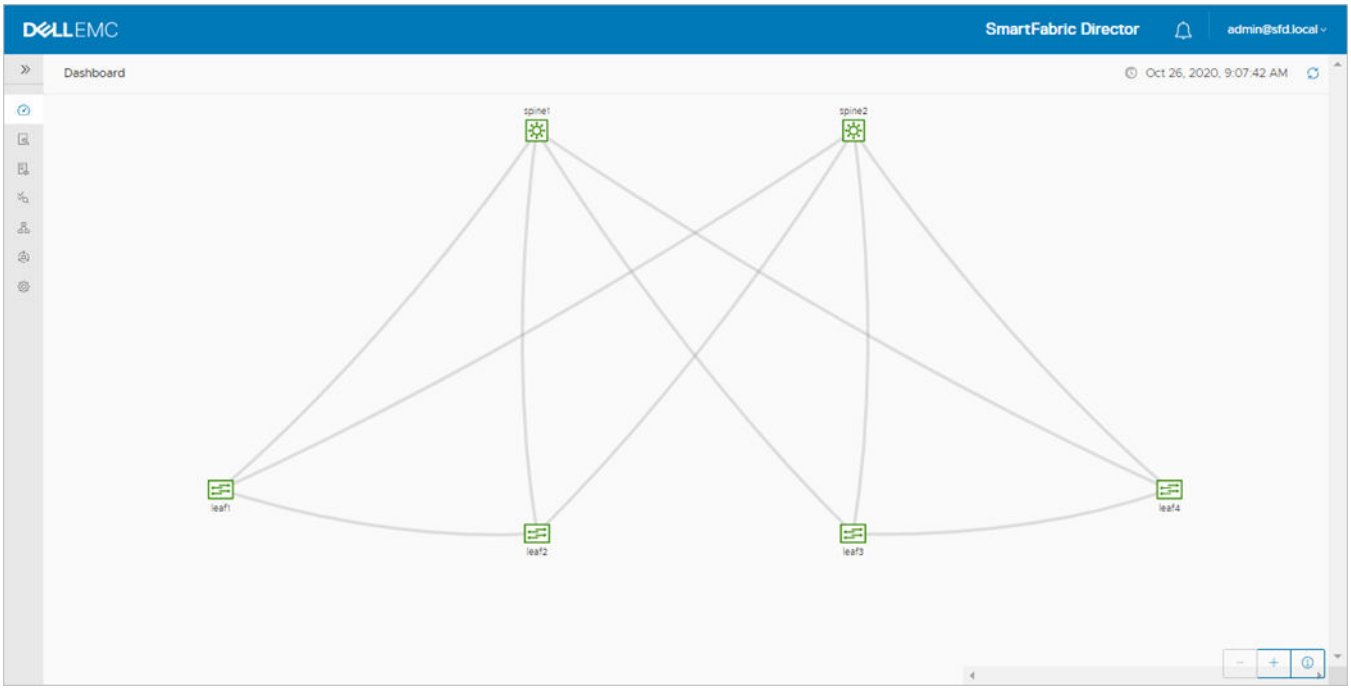
   NOTE: You can optional select View prior to Deploy.



2. Click **Deploy**.



SFD starts configuring each switch, and the progress displays on the dashboard. As each switch is successfully configured, the switch turns green.



Details of the deployment can be viewed in the SFD notifications page.

Layer 2 VLT fabric

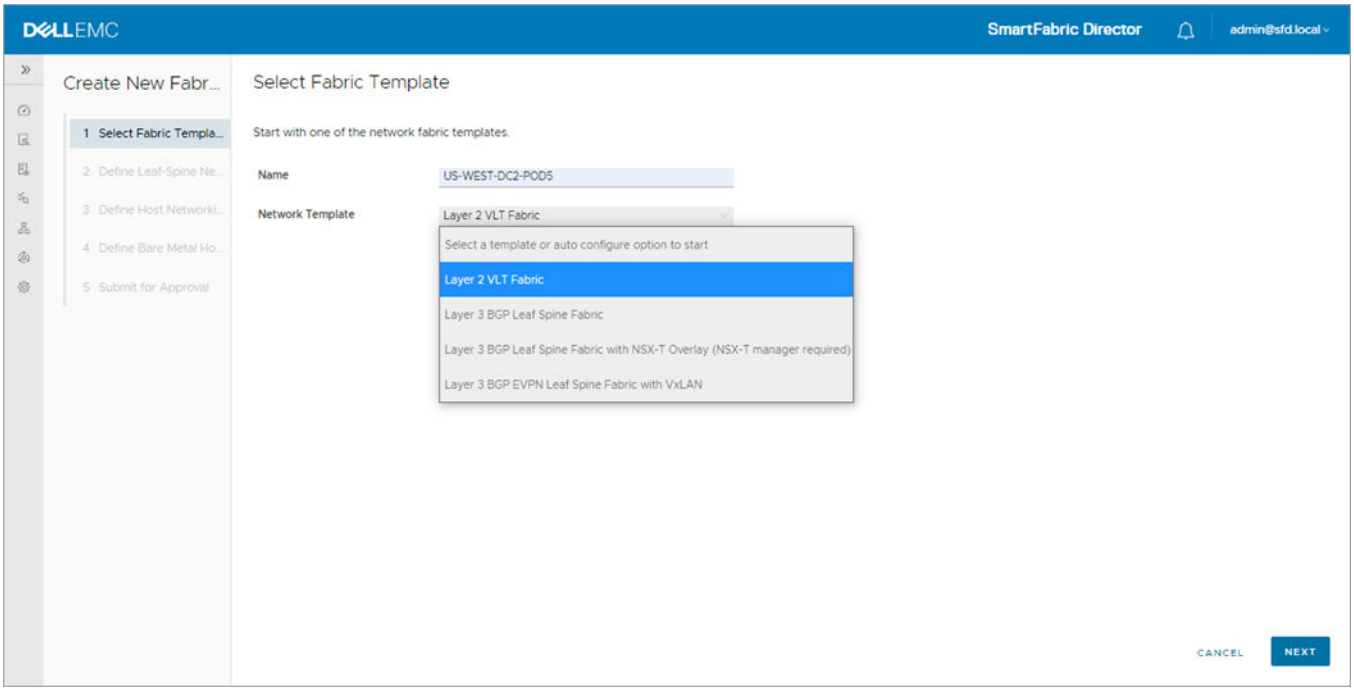
This information explains the Layer 2 fabric. The leaf spine networking template for a Layer 2 fabric is different from that for a Layer 3 fabric.

NOTE: You can only use a vCenter Server to configure a Layer 2 fabric intent. NSX-T Manager is only used for Layer 3 fabric intents.

Select fabric template

For Layer 2 leaf spine fabric, you do not specify any parameters. SFD generates a per-switch configuration for the interlinks between the leaf and spine switches.

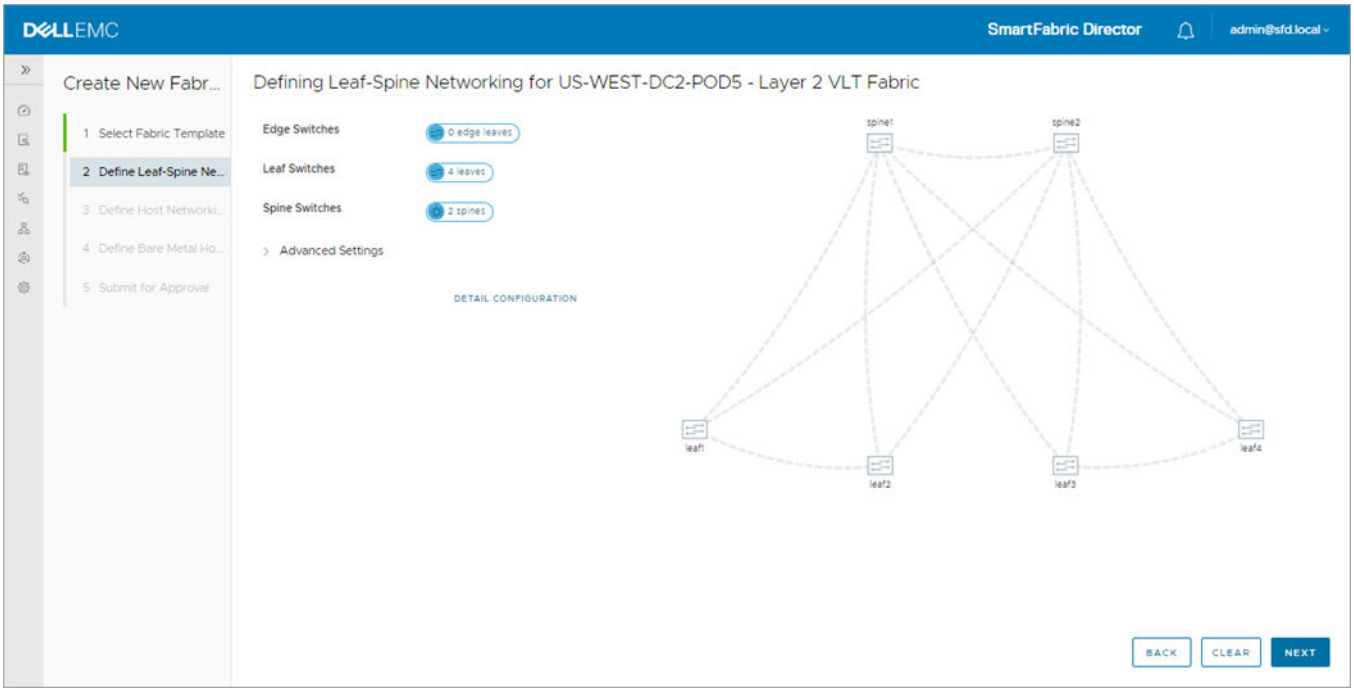
1. Select **Configurations** from the left column to view and define fabric intents, then click **Get Started**. If there are no existing fabric intents, you can use the user interface to specify the fabric intent. Any such file can be used as a seed and edited.
2. Enter the **Fabric Name**, select **Layer 2 VLT fabric**, then click **Next**.



Define leaf-spine networking

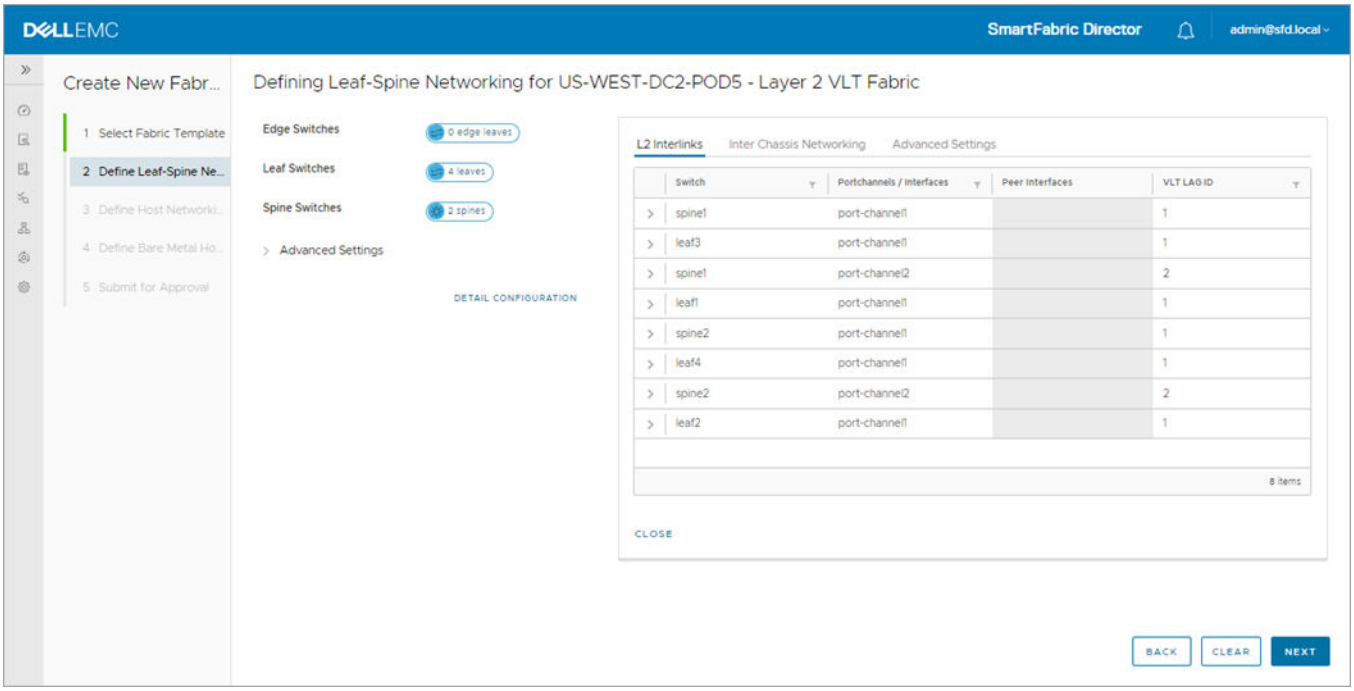
You are now ready to specify the parameters to generate configuration for the host facing ports, inter-VLAN routing, and host dual-homing. This screen also indicates the IP or DNS address of the vCenter (VMware Manager) used to manage the VMs on the hosts that are connected to this fabric.

1. For Layer 2 leaf spine fabric, SFD generates a per switch configuration for interlinks between the leaf and the spine switches. Click **Next** to continue.

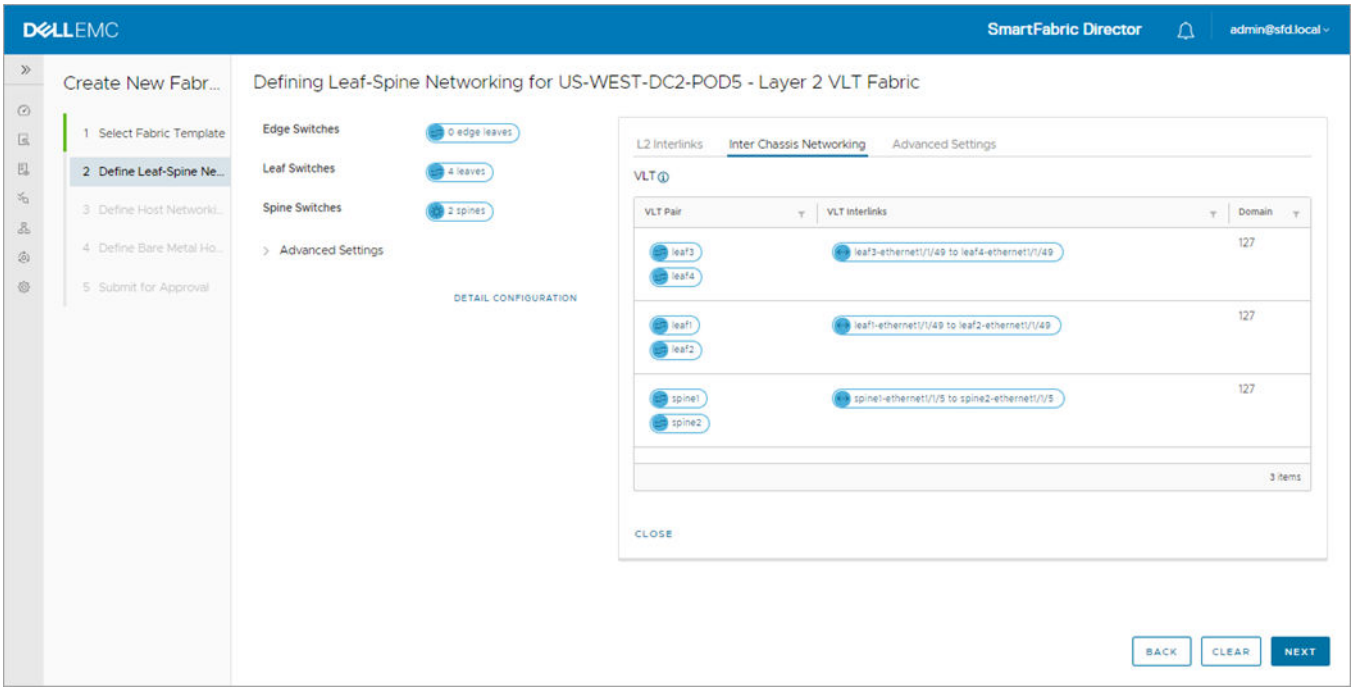


2. (Optional) Click **Detail Configuration** to view the per switch configuration, click **Clear** to clear the specified intent, along with the detailed (per switch) configuration for the interlinks. Click **Back** to return, or click **Next** to continue.

NOTE: Fields cannot be edited.

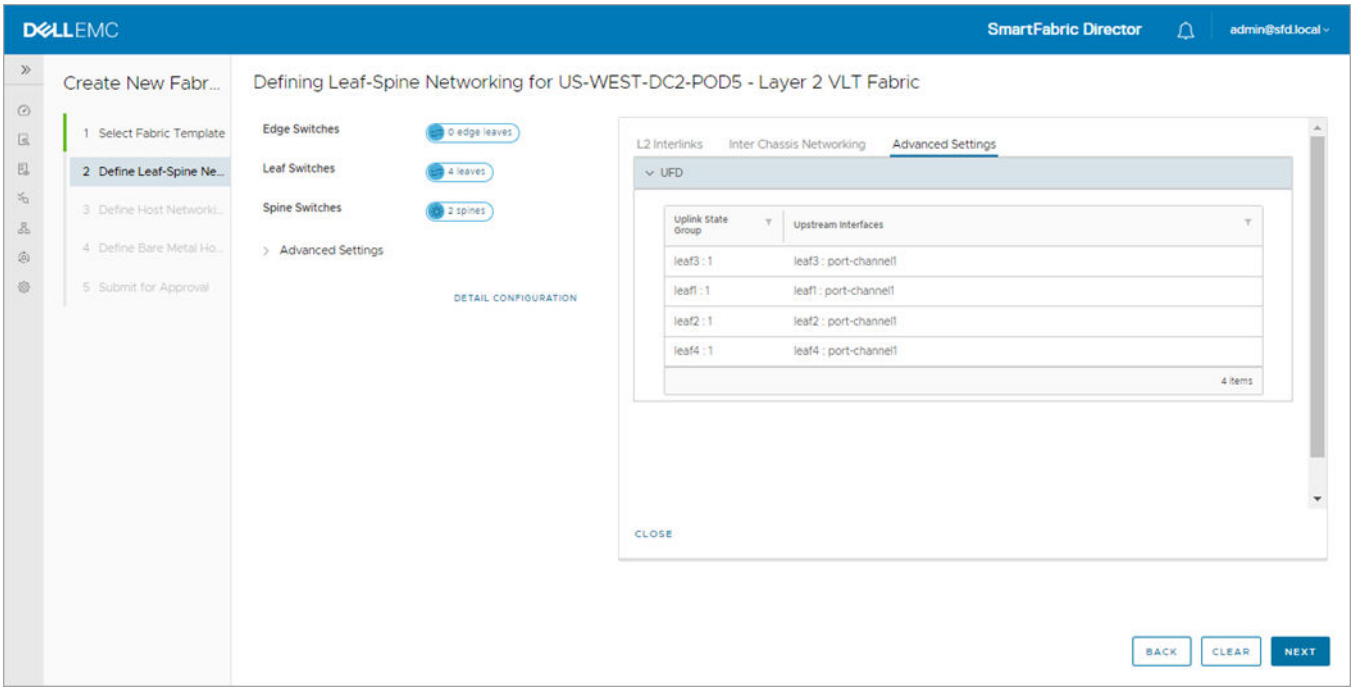


Details of inter chassis networking configuration for Layer 2 fabric.



Details of advanced settings for Layer 2 fabric.

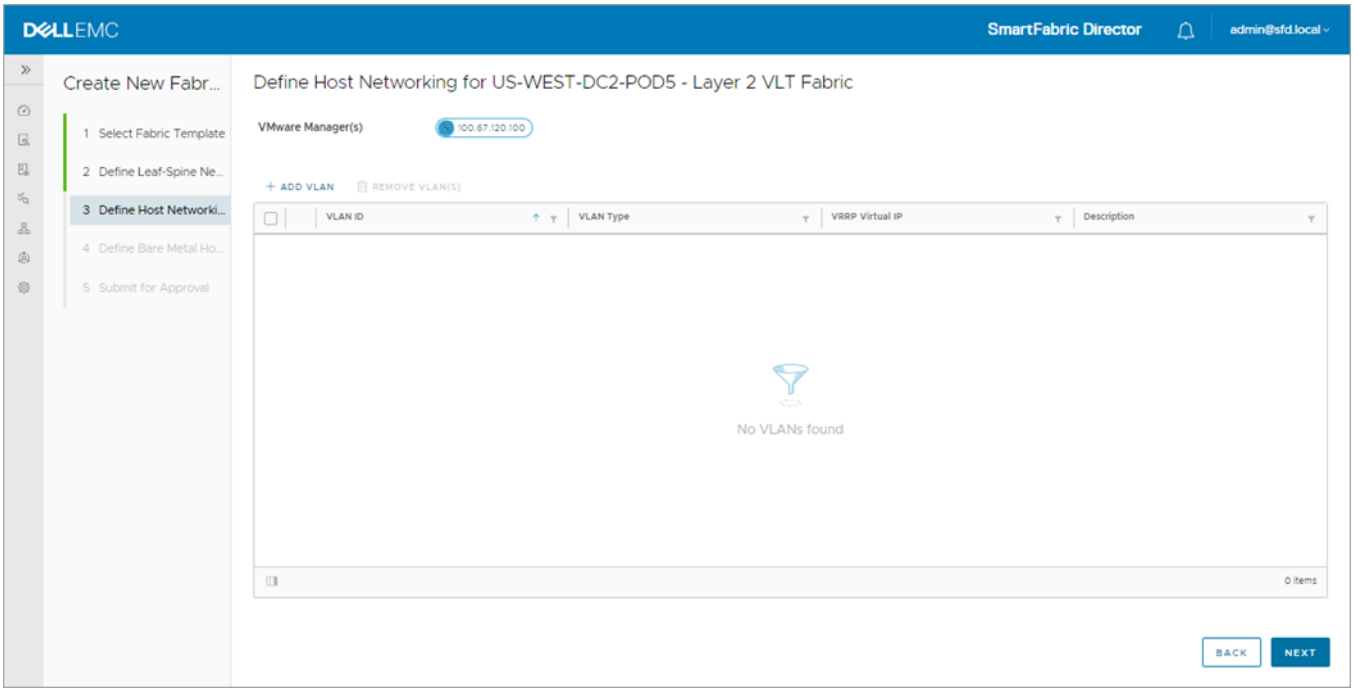
NOTE: RSTP is enabled by default and cannot be disabled.



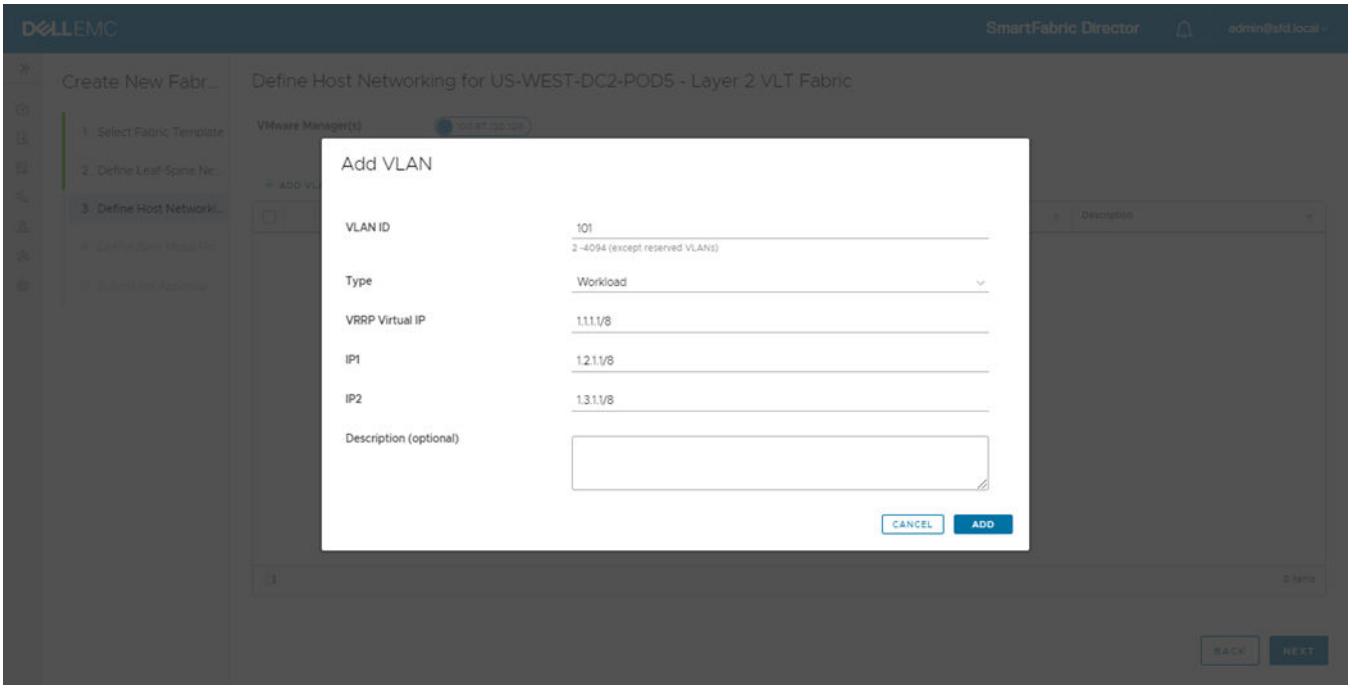
Define host networking

You are now ready to specify the parameters to be used by SFD to generate the configuration for host facing ports, inter-VLAN routing, and host dual-homing. This screen also indicates the IP or DNS address of the vCenter (VMware Manager) used to manage the VMs on the hosts that are connected to this fabric.

1. Select **System Settings** from the left column, then select **VMware Manager Integration**. A list of vCenter Server connections previously configured display. If there are no existing vCenter Server connections, this table is blank.

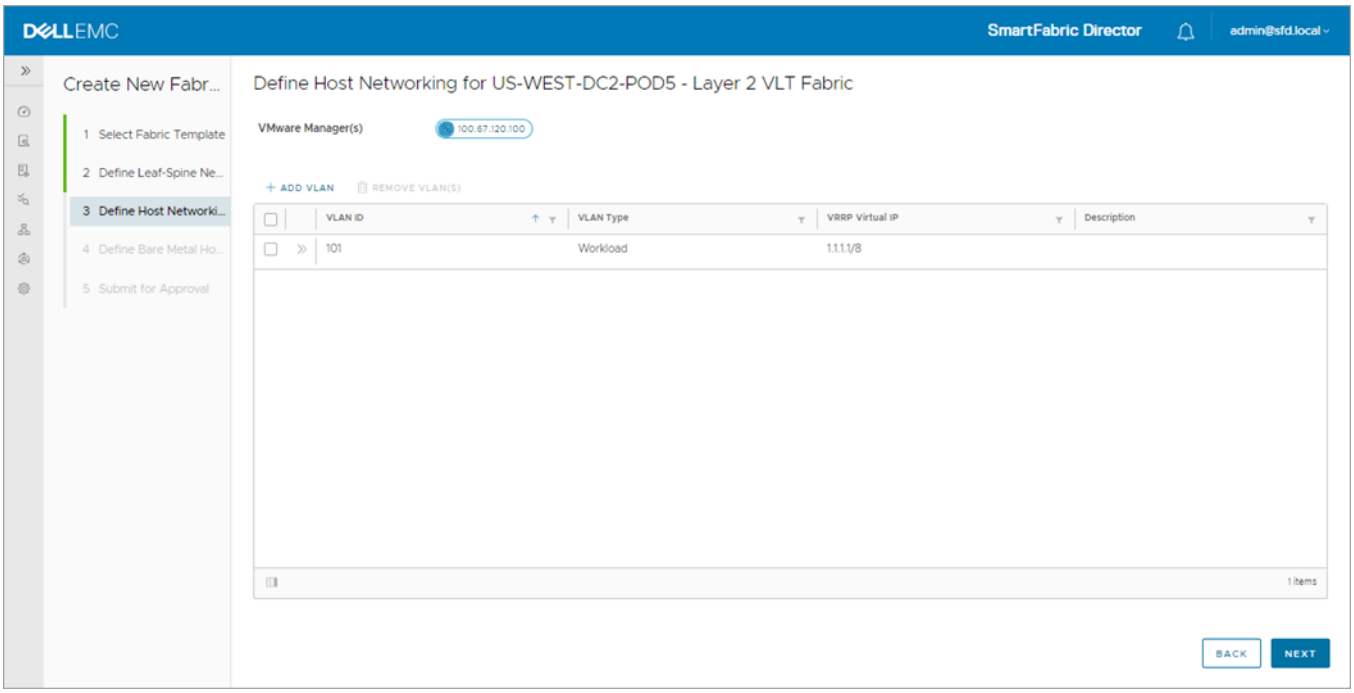


2. Click **Add VLAN** to add the configuration for each port group used by the vCenter, select the VLAN type, select the leaf pairs, enter an optional description, then click **Add**.

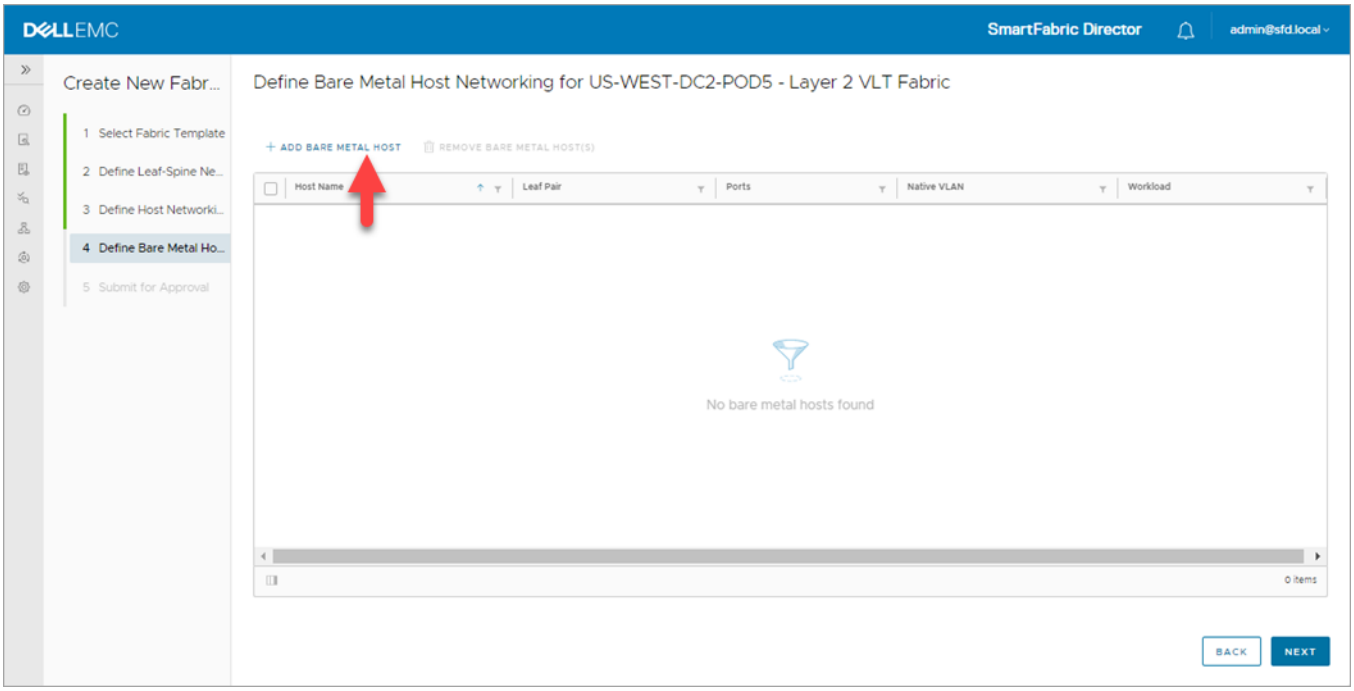


SFD creates a virtual interface on each spine, and associates it to the VLAN ID. Each virtual interface obtains an SVI IP, and each VLAN in the VLT pair obtains a VRRP virtual ip in the same subnet as the VLAN.

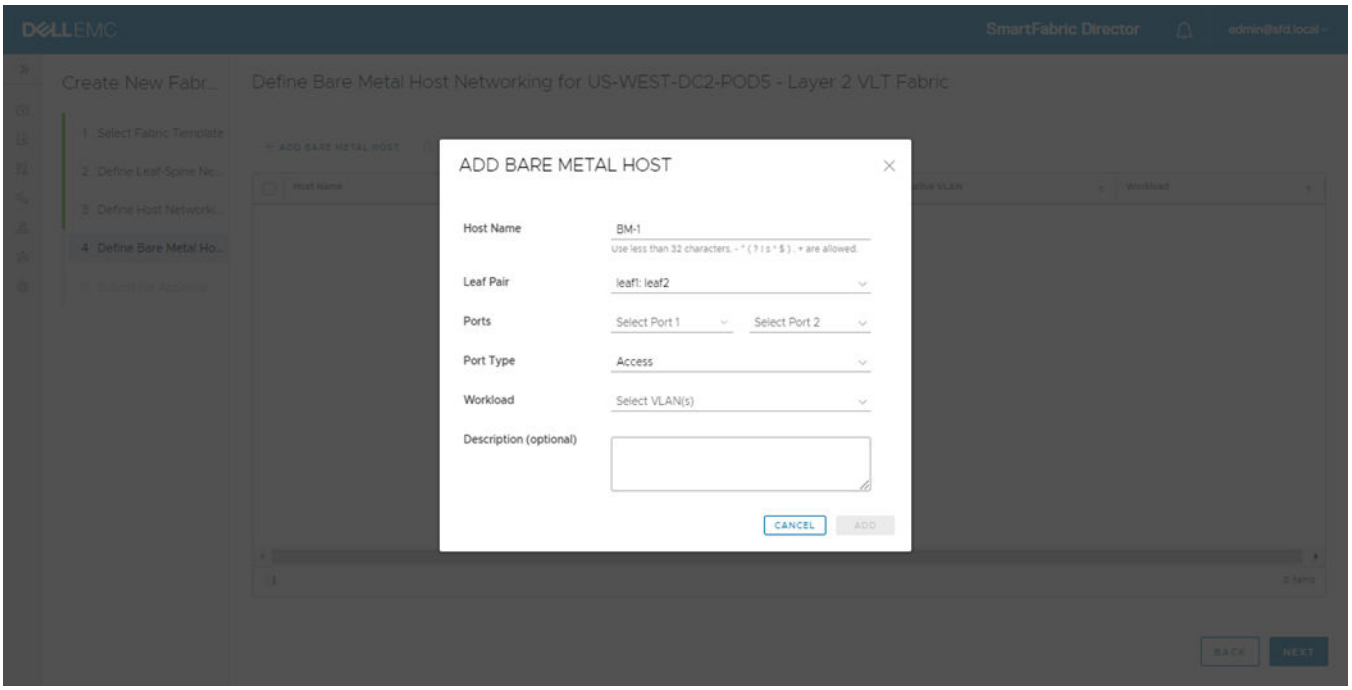
3. (Optional) Delete any VLAN ID row by selecting the checkbox to the left of each row.



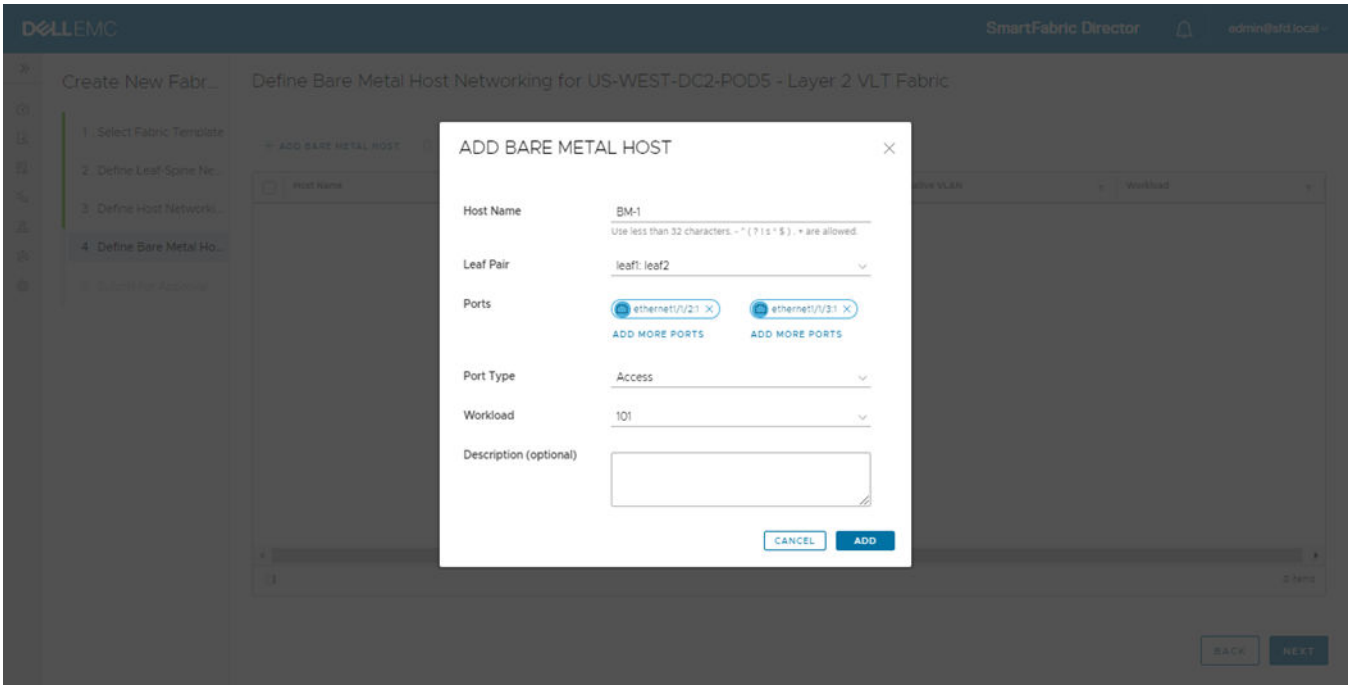
4. Navigate between pages by using the arrows; click **Back** to go to the previous step, or click **Next**.
5. Select **Add bare metal host**.



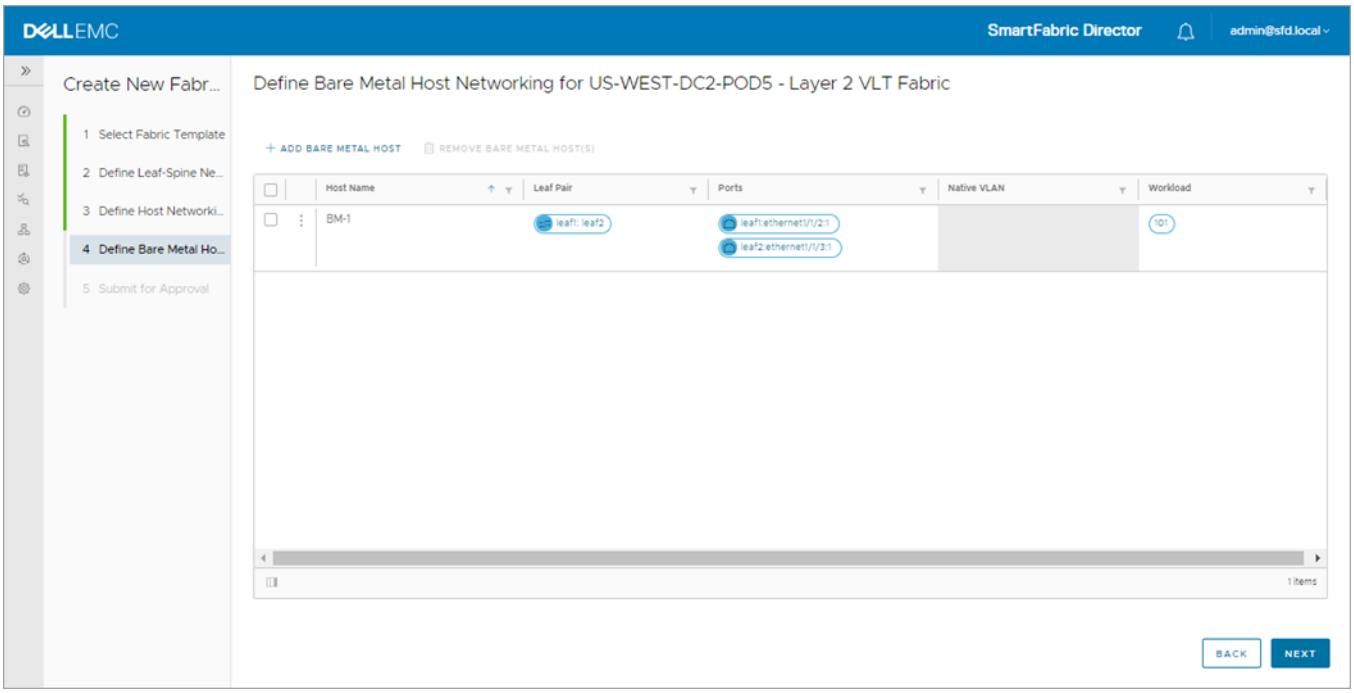
6. Enter the Host Name to identify the VLT pair to which the host is connected to, then select the Leaf Pair.



7. Specify one or more switch ports that the server is connected to, select Access or Trunk for the port type, select the workload VLAN, an optional description, then click **Add**.



The bare metal host configuration displays; click **Next**.



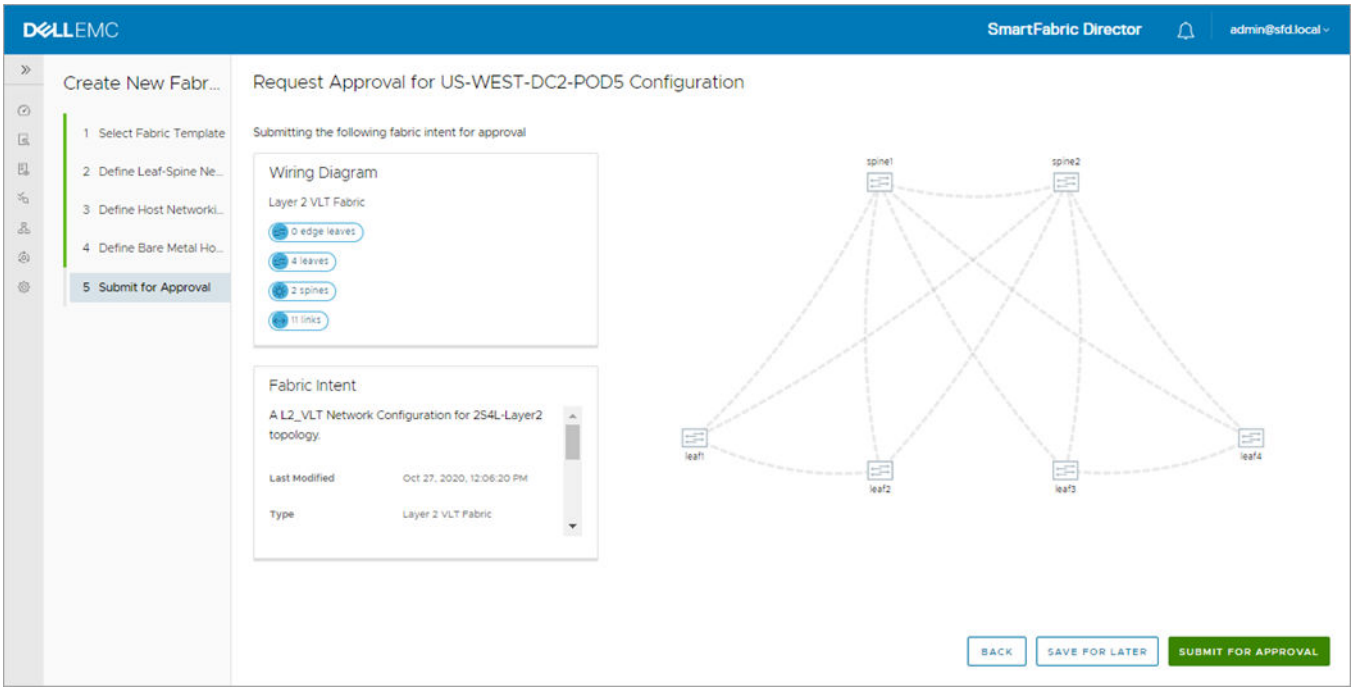
Submit for approval

You are now ready to submit your L2 fabric intent for approval. The fabric intent must be approved before it can be deployed on the physical switches by SFD. Each fabric intent is associated with a wiring diagram.

1. The wiring diagram summary displays, along with a topology graph which corresponds to the wiring diagram. Click **Save for Later** to save the specified fabric intent as a draft in the SFD data store, or click **Back** to return to Define overlay networking.

   The summary displays different depending on the type of fabric configured. The example shows a Layer 3 fabric intent.

   NOTE: BFD is disabled by default on links from Edge ports to the external peer router. You can enable Edge ports if the external router has BFD enabled.



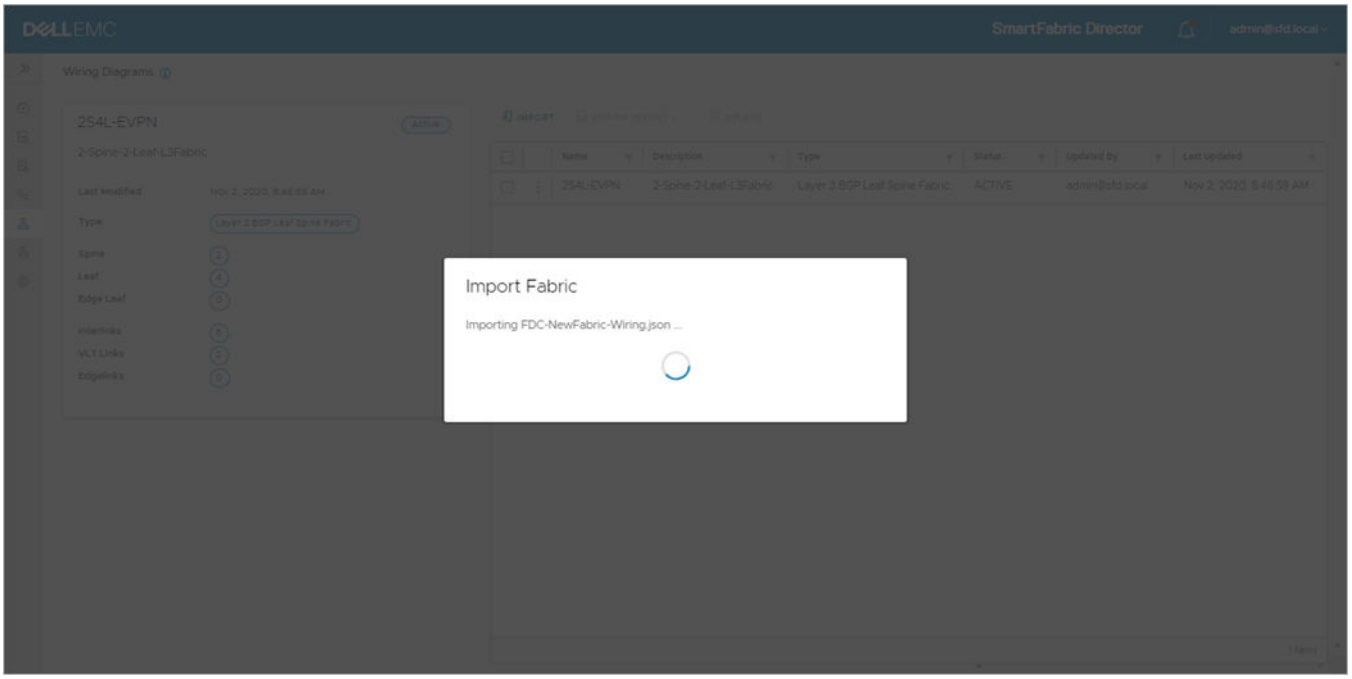
2. Click **Submit for Approval** to submit the fabric intent, along with the associated wiring diagram for approval by the authorized approver.
3. (Optional) Click **Back** to go to the previous step, or click **Save For Later** to save the specified fabric intent as a draft. All drafts are saved in the SFD data store.

Any fabric intent pending approvals are listed in the fabric intent list which can be viewed by selecting the Intent icon on the left.

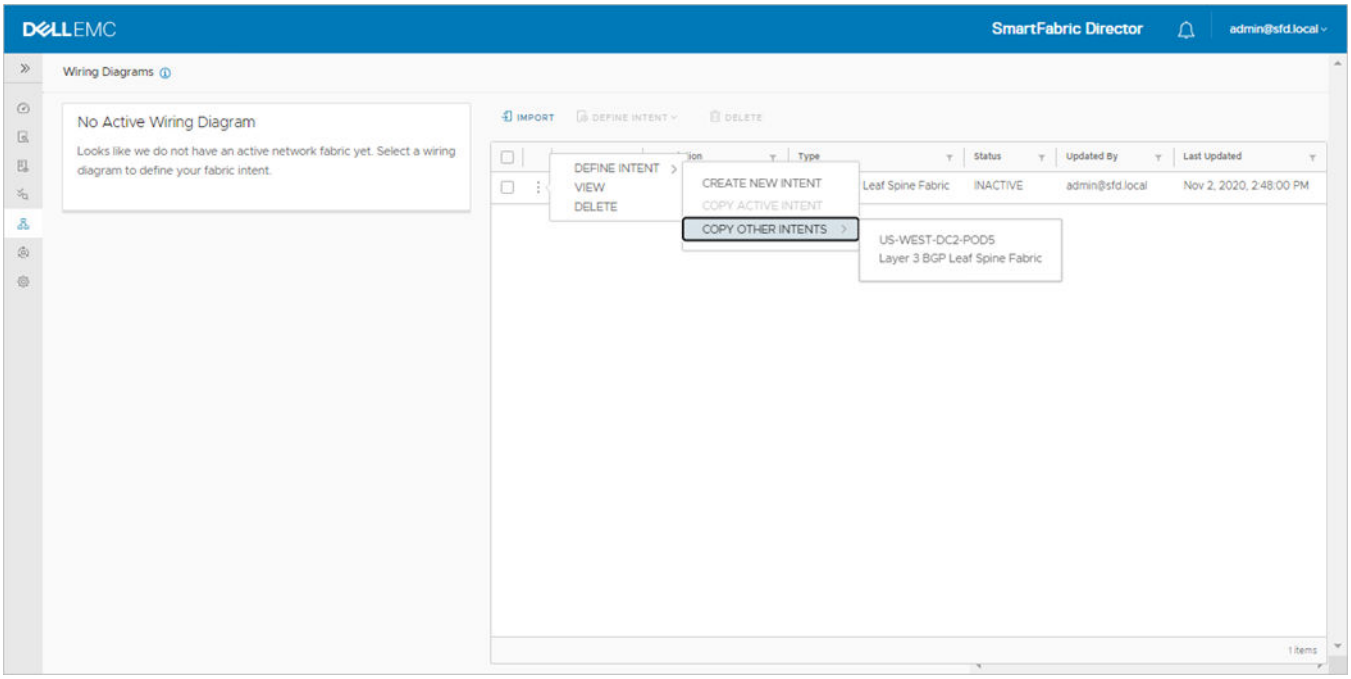
Importing a new wiring diagram

This information explains how to import a new wiring diagram. You may update the fabric to add or remove switches, or add or remove links.

1. Select **Wiring Diagrams > Import**.



2. Define and associate a Fabric Intent. You can also clone or copy an existing Fabric Intent, then make any necessary changes by going through the Fabric Intent Wizard.



3. See Approve fabric Intent and Deploy fabric intent.

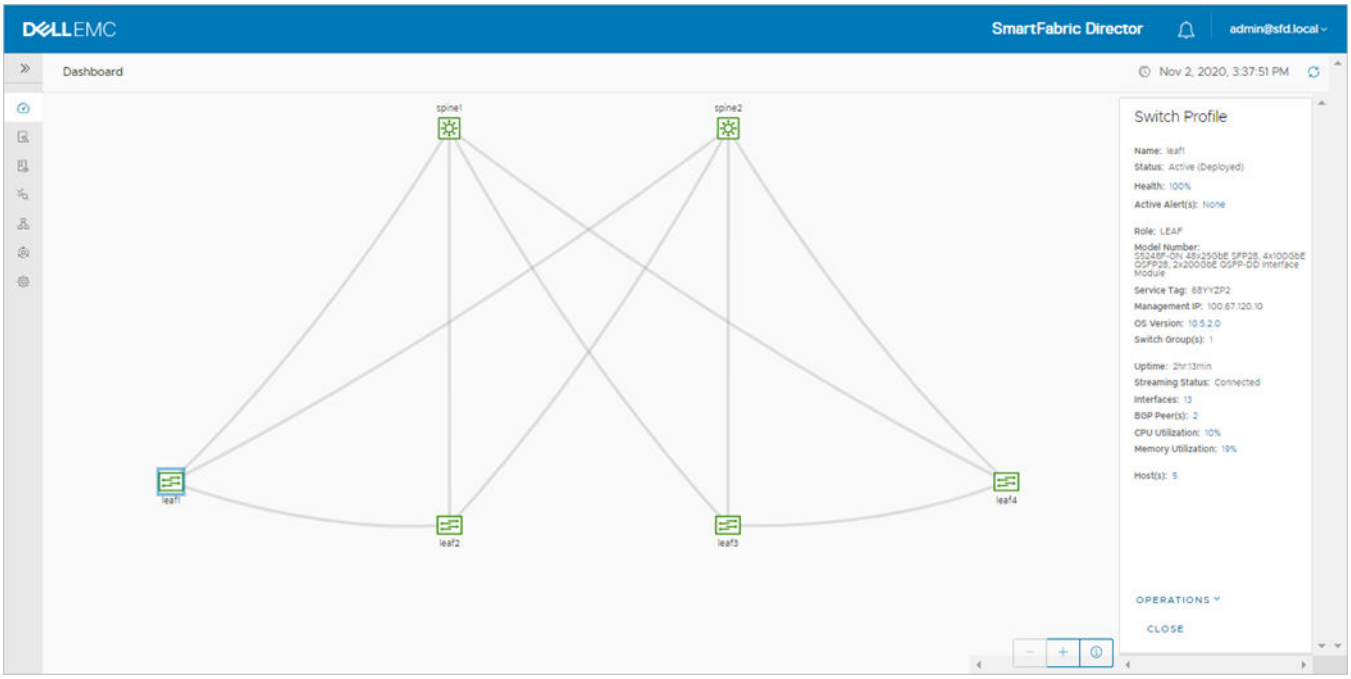
8

Monitoring

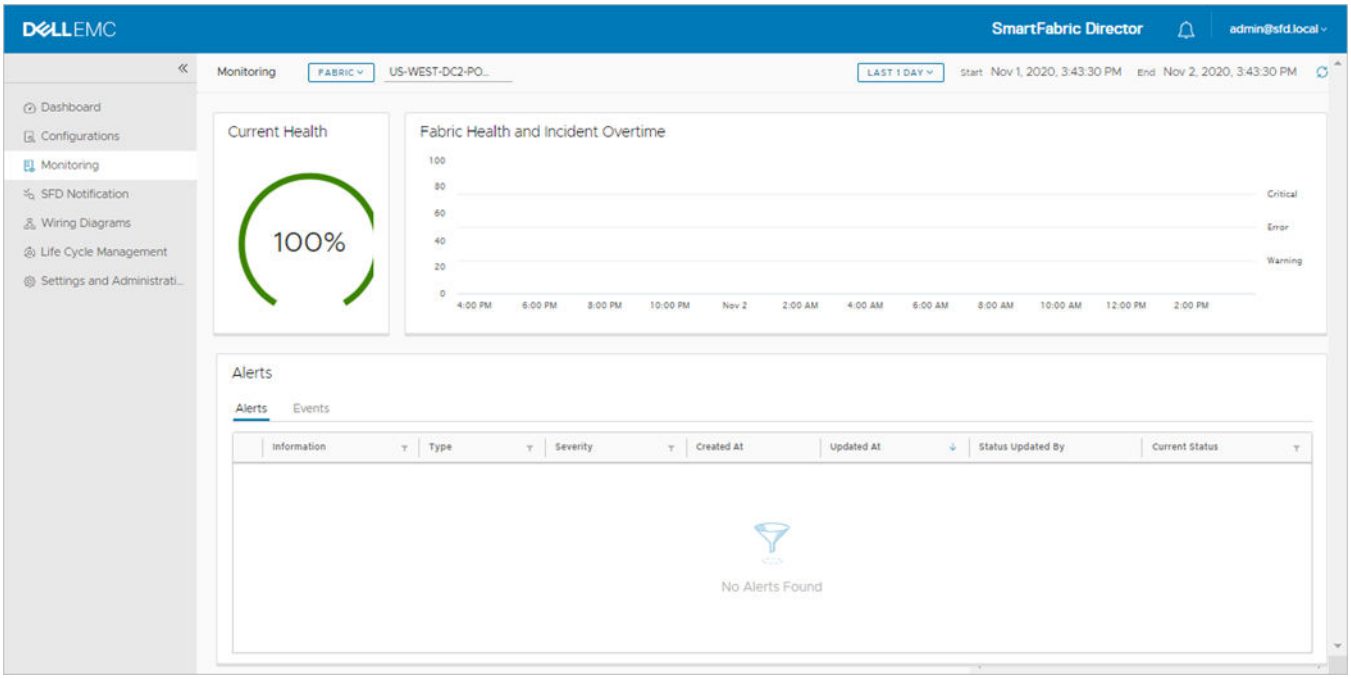
This information explains how to monitor the fabric, viewing switch level details. Monitoring data is the last information streamed by the switch to SFD. The switch streams telemetry information to SFD every 60 seconds. The streaming status of a network device is available in the switch profile under monitoring.

1. From the SmartFabric Director dashboard, select a switch to open up the switch profile panel to view a summary of the switch.

   NOTE: When viewing CPU data over a large time window, the graph displays peak CPU data. This time window can be adjusted or lowered to get a granular view of the CPU data.



2. Select the **Monitoring** icon from the left to view the fabric health.



3. Select any interface to view the switch profile and details.
4. Scroll down to view additional details.

Topics:

- Notifications, events, alerts, and activities

Notifications, events, alerts, and activities

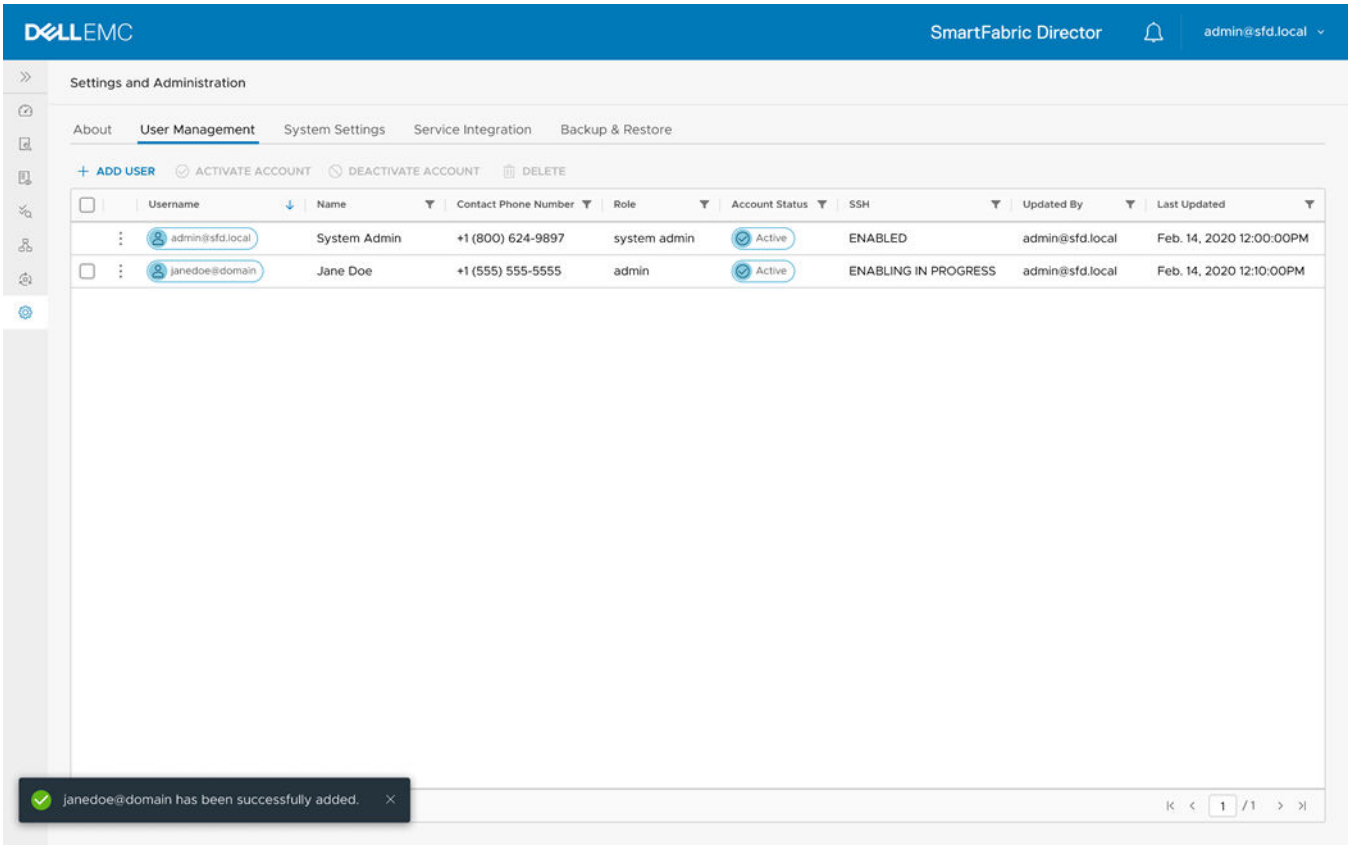
This release has made enhancements and now displays notifications, alerts, and activities. In additional, two types of message types for notifications are introduced.

Toast message

Toast messages provide information and medium priority events to reference later. Toast messages when they are not dismissed should live in a notifications panel until they are dismissed or the notification expires. The notification expiration default is six seconds, unless the notification is acknowledged or the condition is cleared.

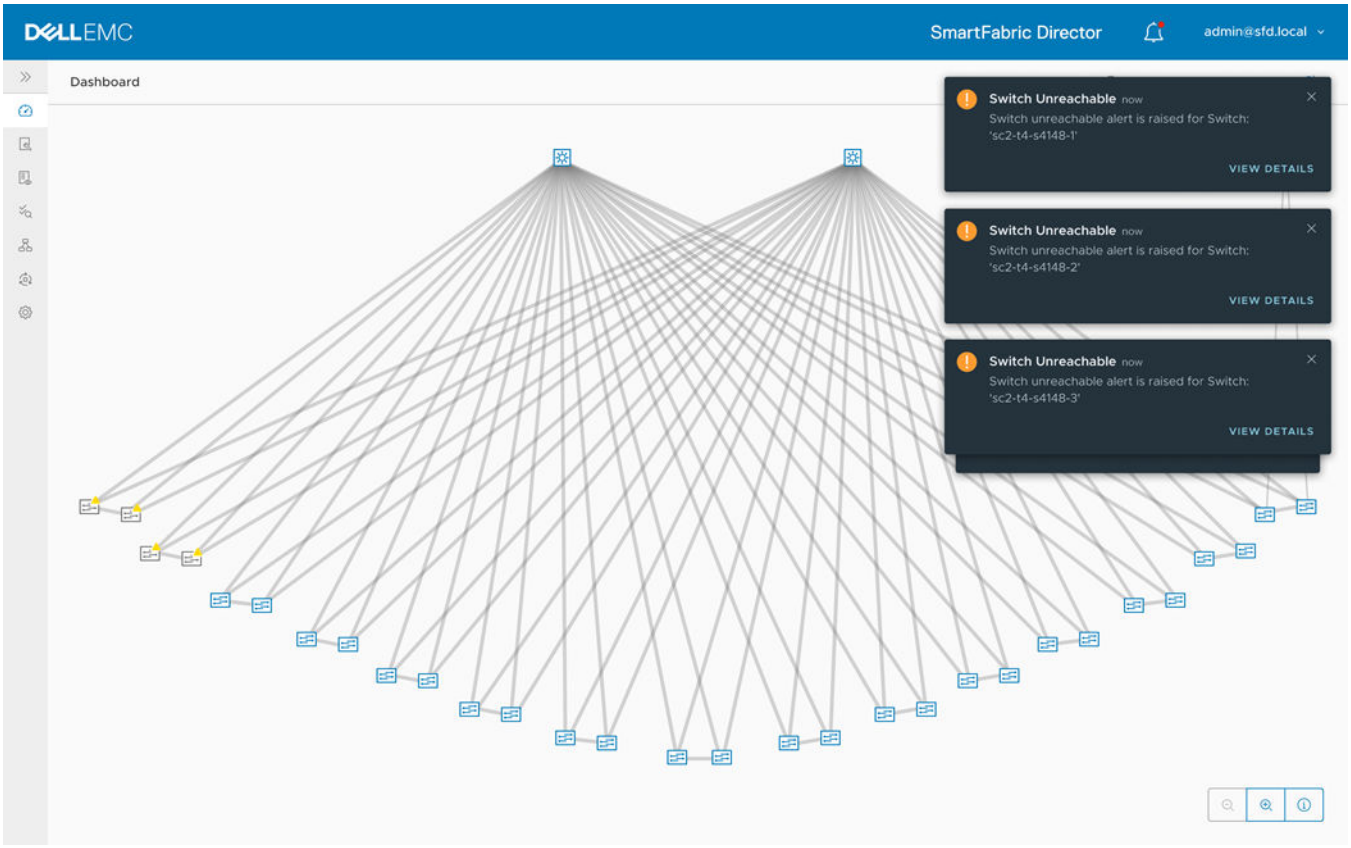
Snackbars

Snackbars are a quick configuration of a successful action. It displays in the current user view only, and displays for up to six seconds, or until dismissed or the page is navigated away from.



Snackbars display along the bottom of the screen. This notification is used for these confirmations:

- Successful SFD service tag upload
- Switch operating system support matrix file upload
- VM manager addition
- Active Directory (AD) server addition or removal
- Switch image server addition or removal
- Backup server addition or removal
- Lifecycle management (LCM) job completion
- Backup job completion
- Wiring diagram import
- Fabric intent (configuration) deployment

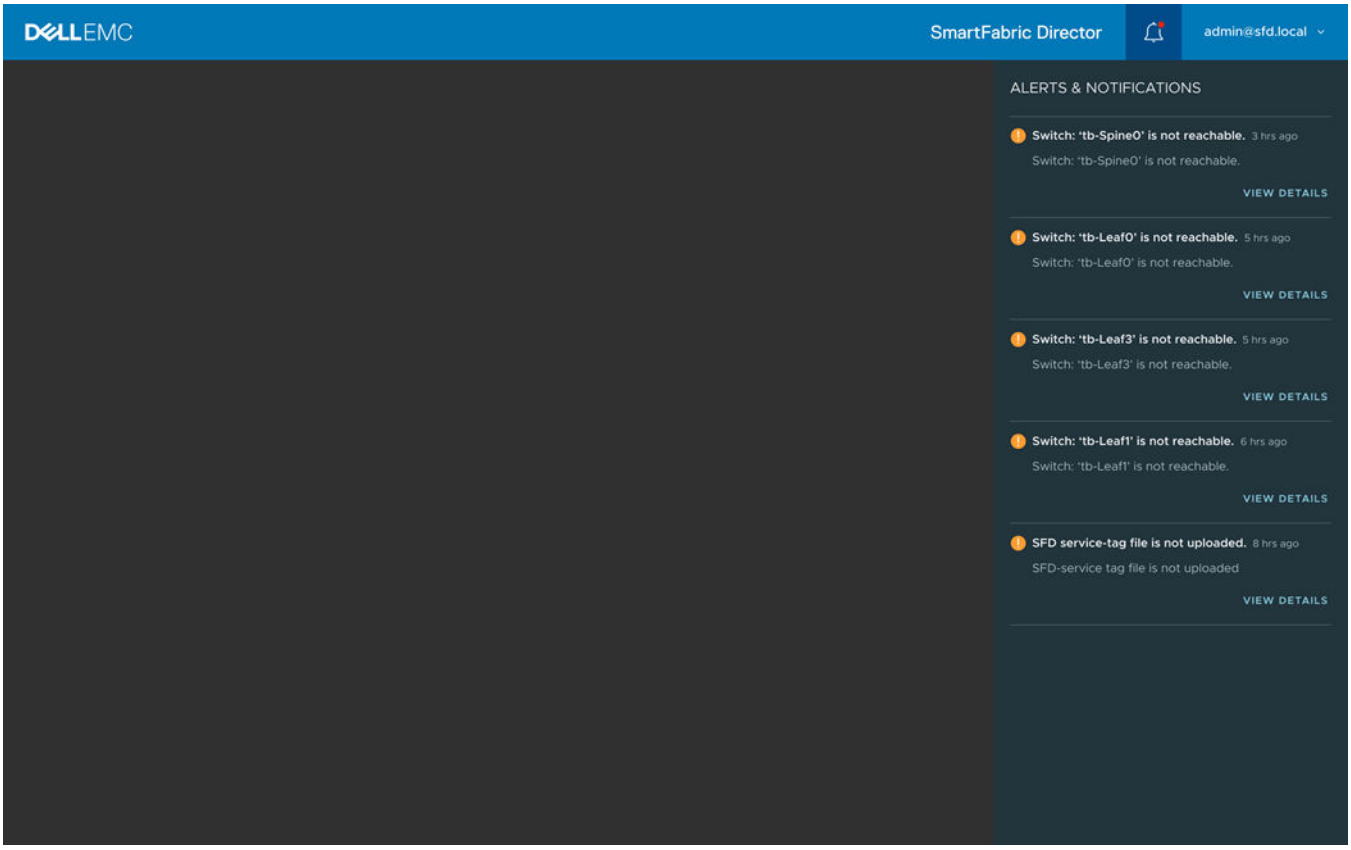


Toast notifications display at the upper right of the screen. If multiple toast messages display simultaneously, they are placed along the right edge of the screen.

Alerts and notifications

You can view job activity details, events, alerts, and switch logs with SFD 2.0. Alerts and notifications appear at the bell icon at the top of the screen.

1. Click the **bell icon** to list all notifications which have not been acknowledged.

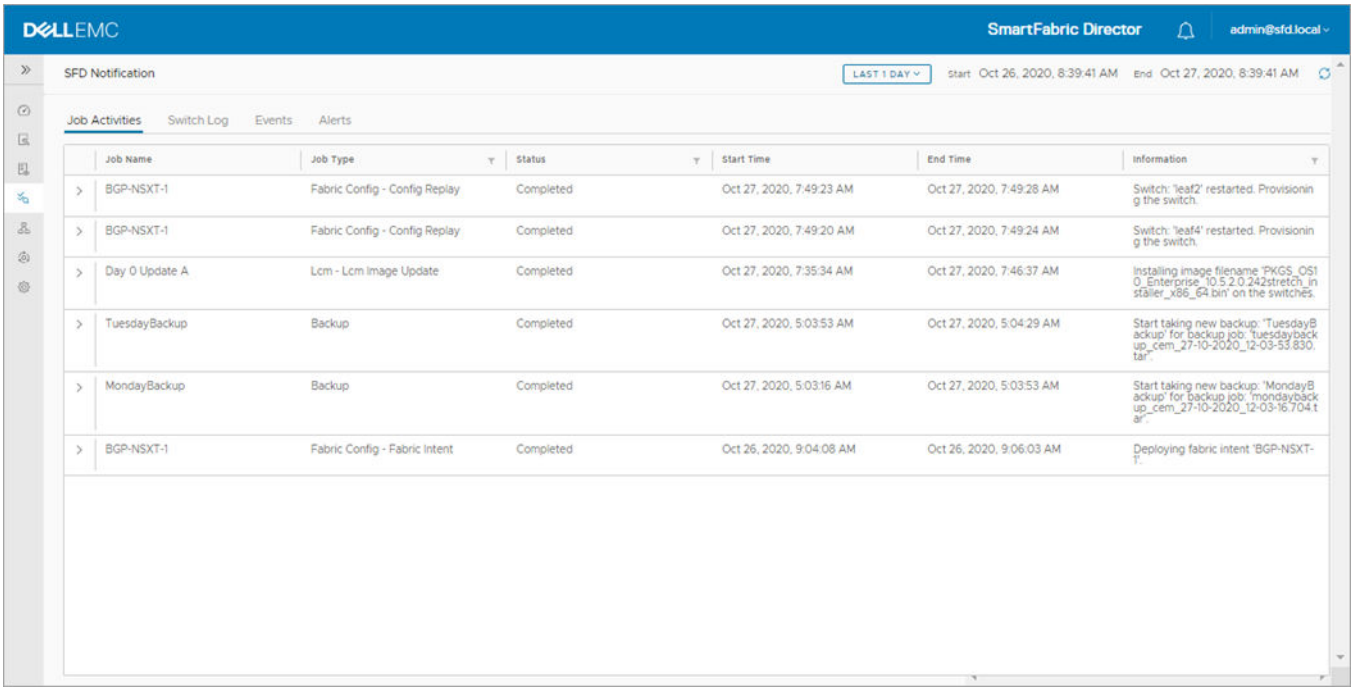


Events which need attention display as alerts and notifications.

2. Click **View details** to view more information.

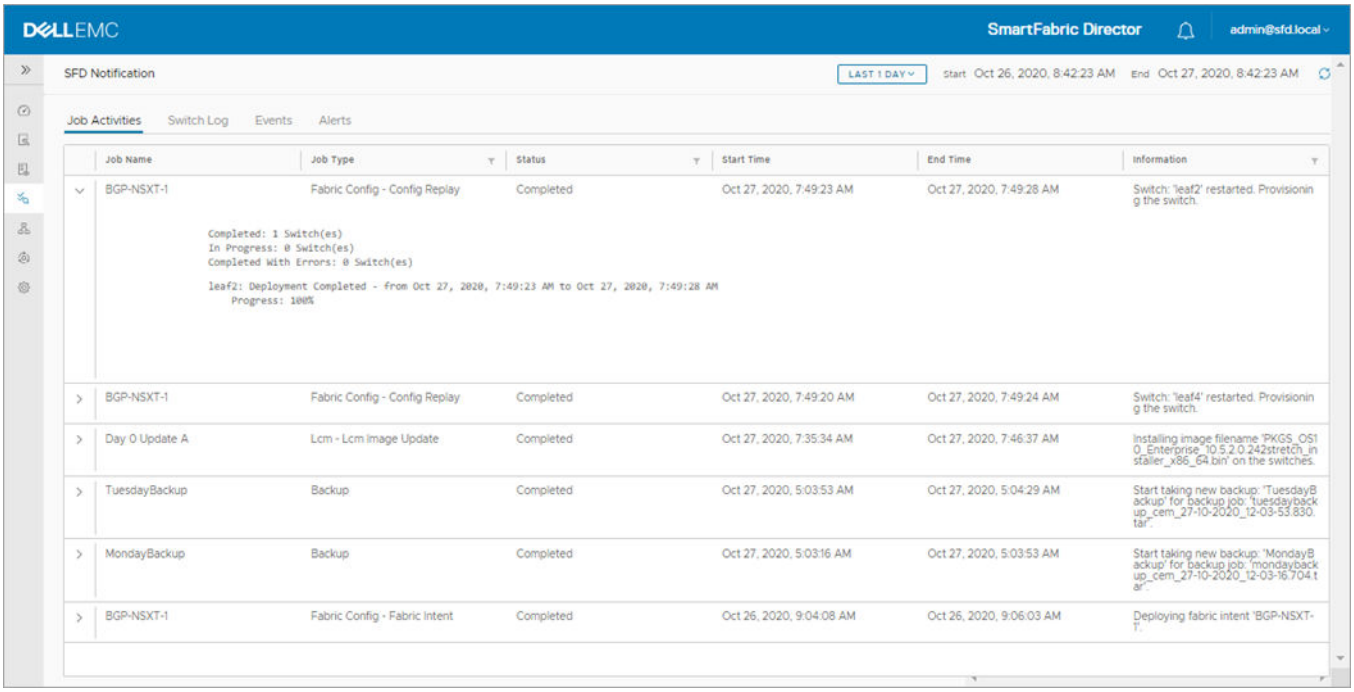
SFD job activities

For long running SFD job activities such as fabric intent deployment (fabric configuration), you can view the lifecycle management (LCM) progress using the job activities tab. You can view the job type, status, start and end time, and summary information for each job.



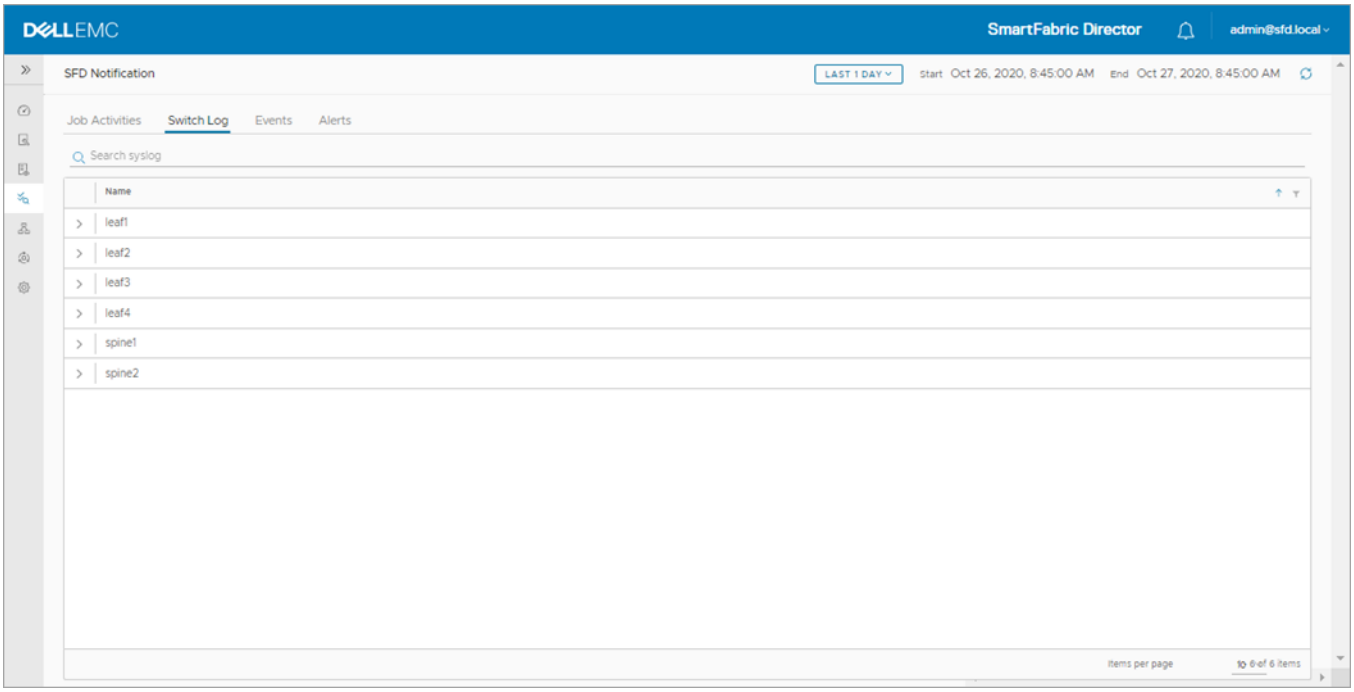
NOTE: If the job is in progress, the end time is disabled and unavailable.

Click **>** to view details.

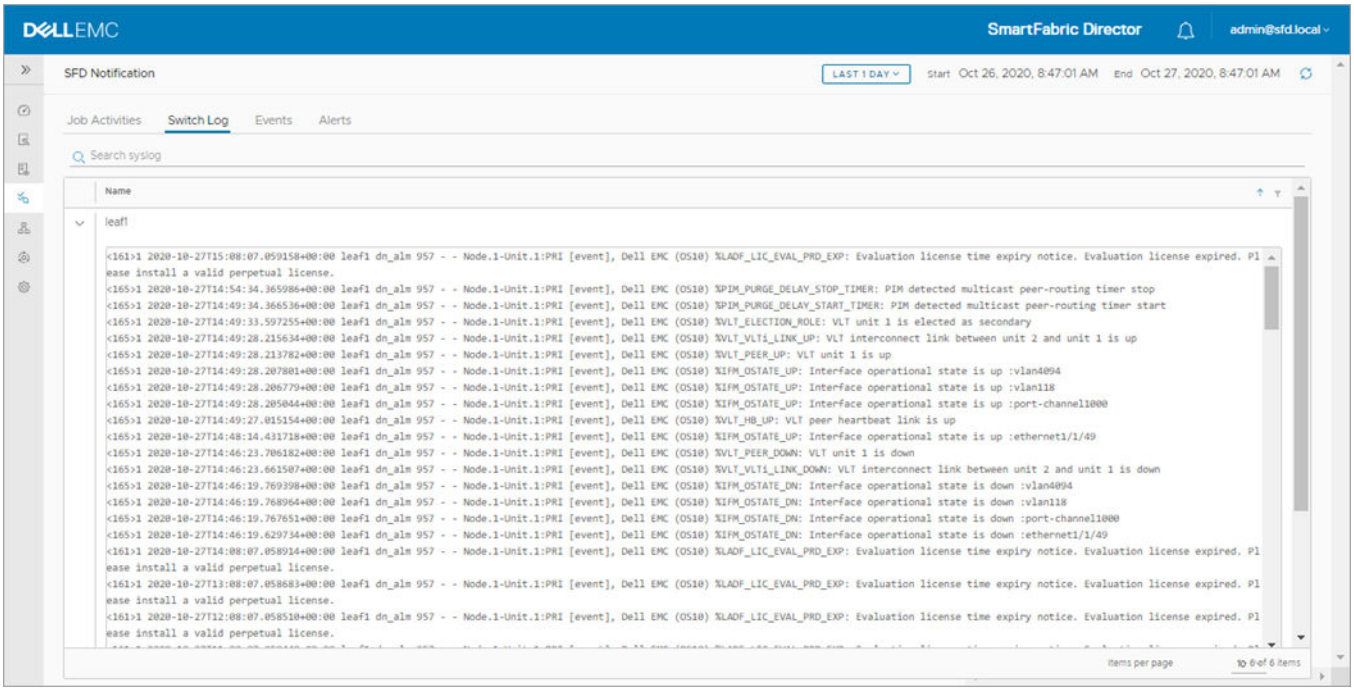


Switch log

SFD acts as a destination for switch logs. Select **Switch log** to view the switch logs that are organized on a per-switch level.

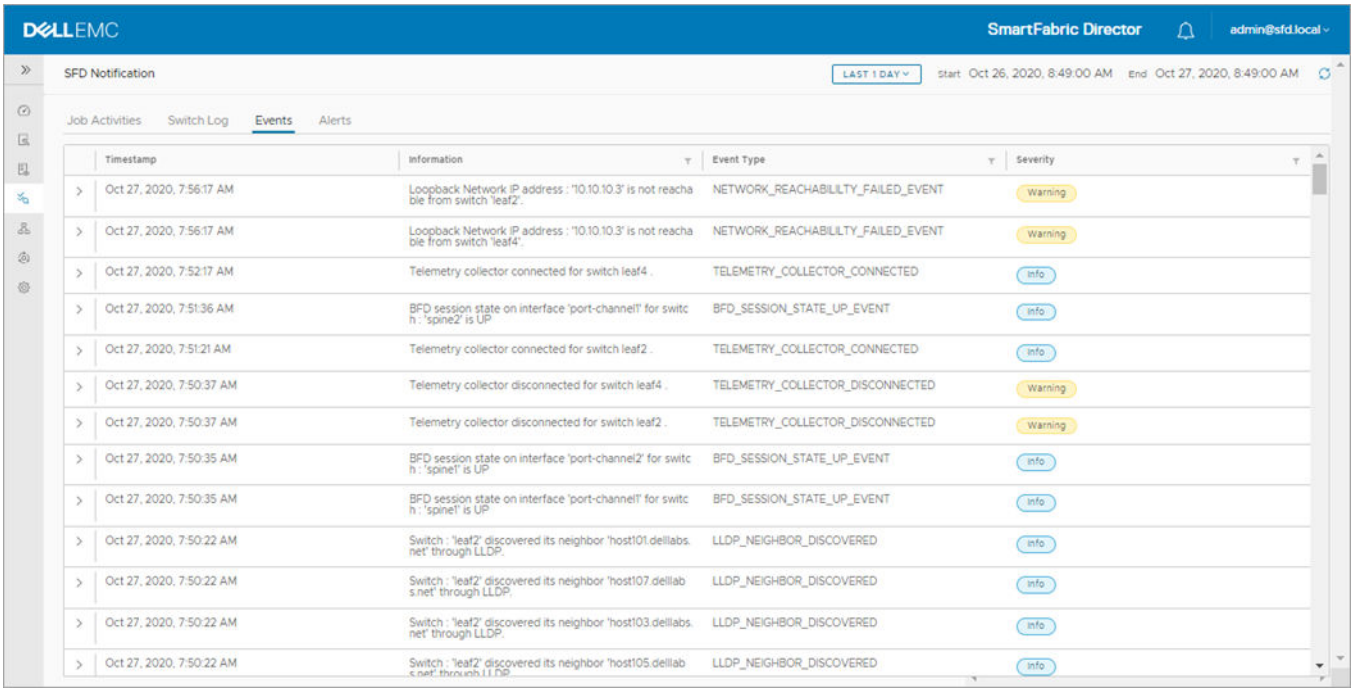


Click **>** to view details.

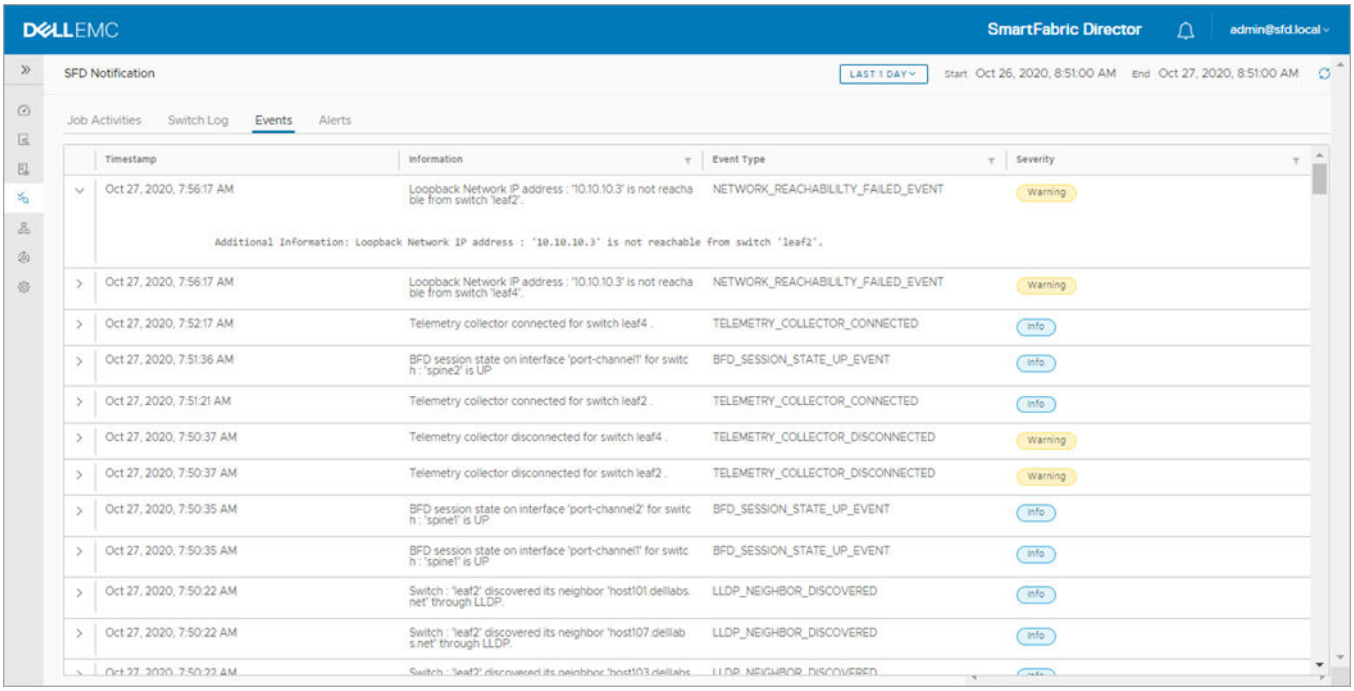


Events

You can view all SFD events using the Events tab. Events are classified as critical, warning, and info severity levels. Event type, timestamp, and summary information display.



Click **>** to view details.



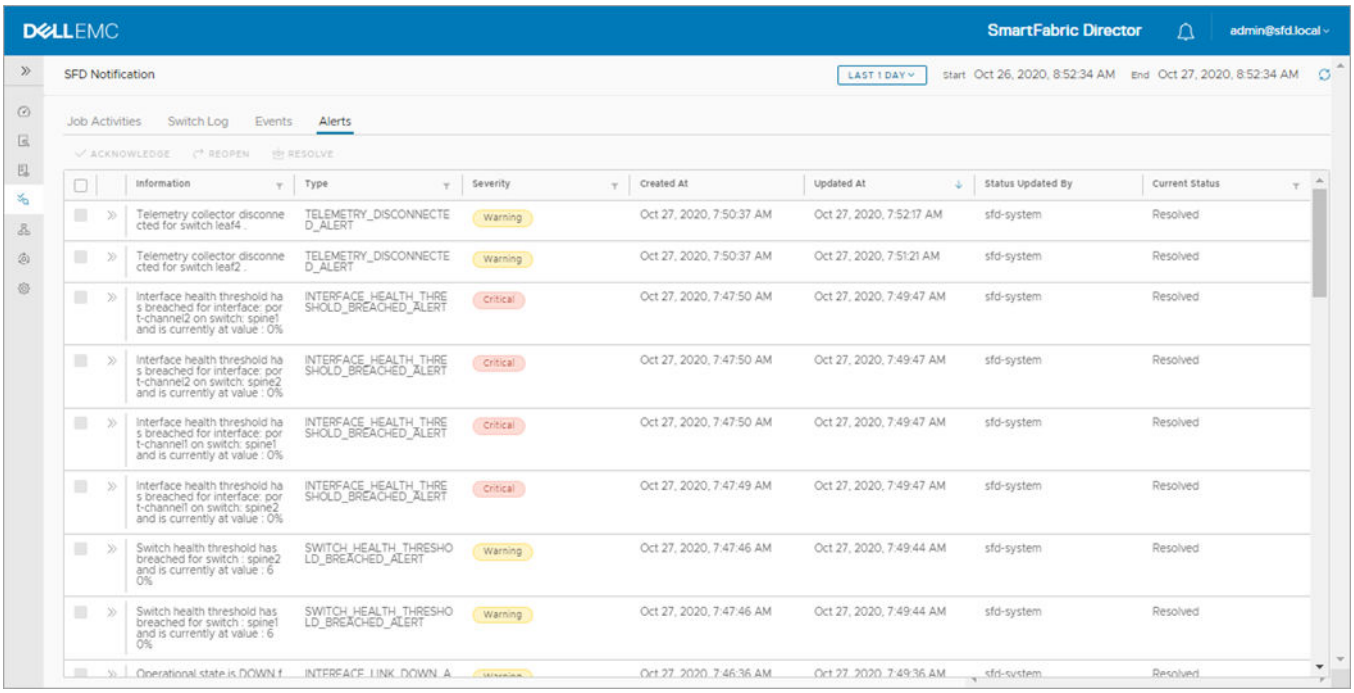
Alerts

SFD alerts are events with demand attention. Alerts are shown as toast messages and available at the Bell icon. You can take action on an alert (acknowledge), and also view a list of alerts using the Alerts tab.

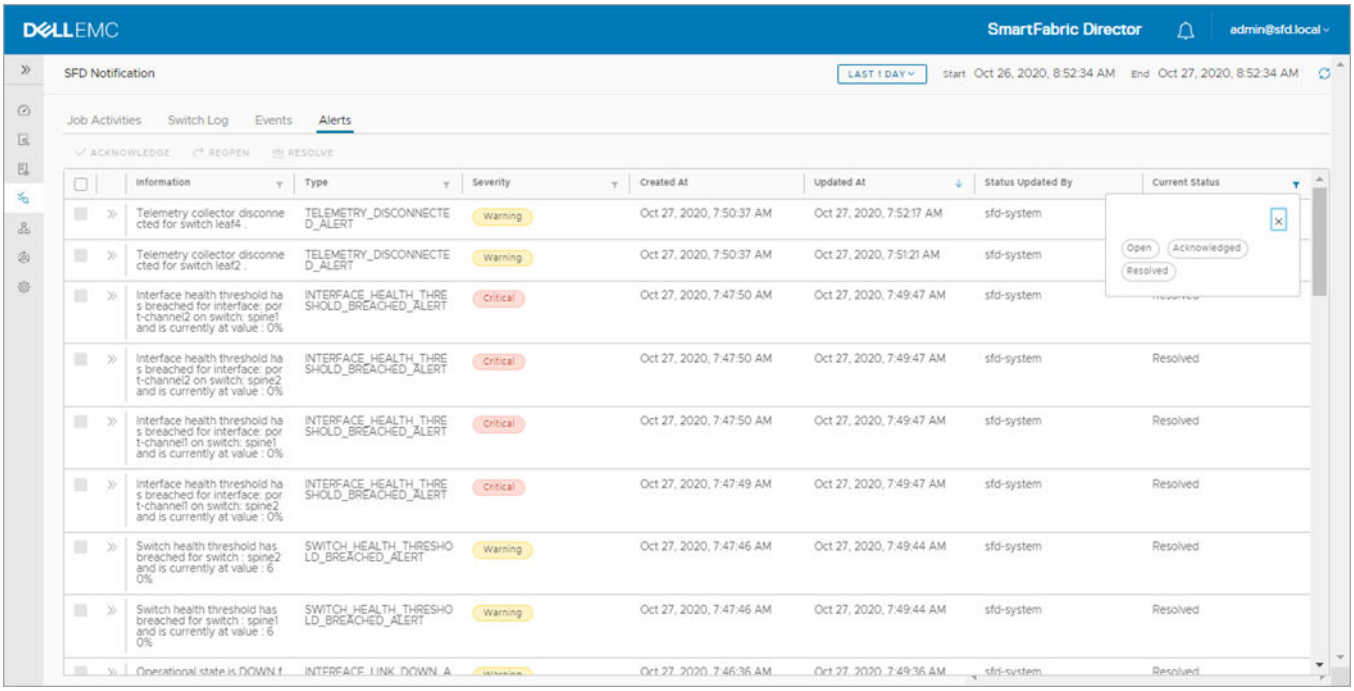
Alert display descriptions:

- *Created at column* displays the time when the alert was created
- *Updated at* column displays the timestamp when the last action was taken
- *Status updated by* field displays the user who last performed the action

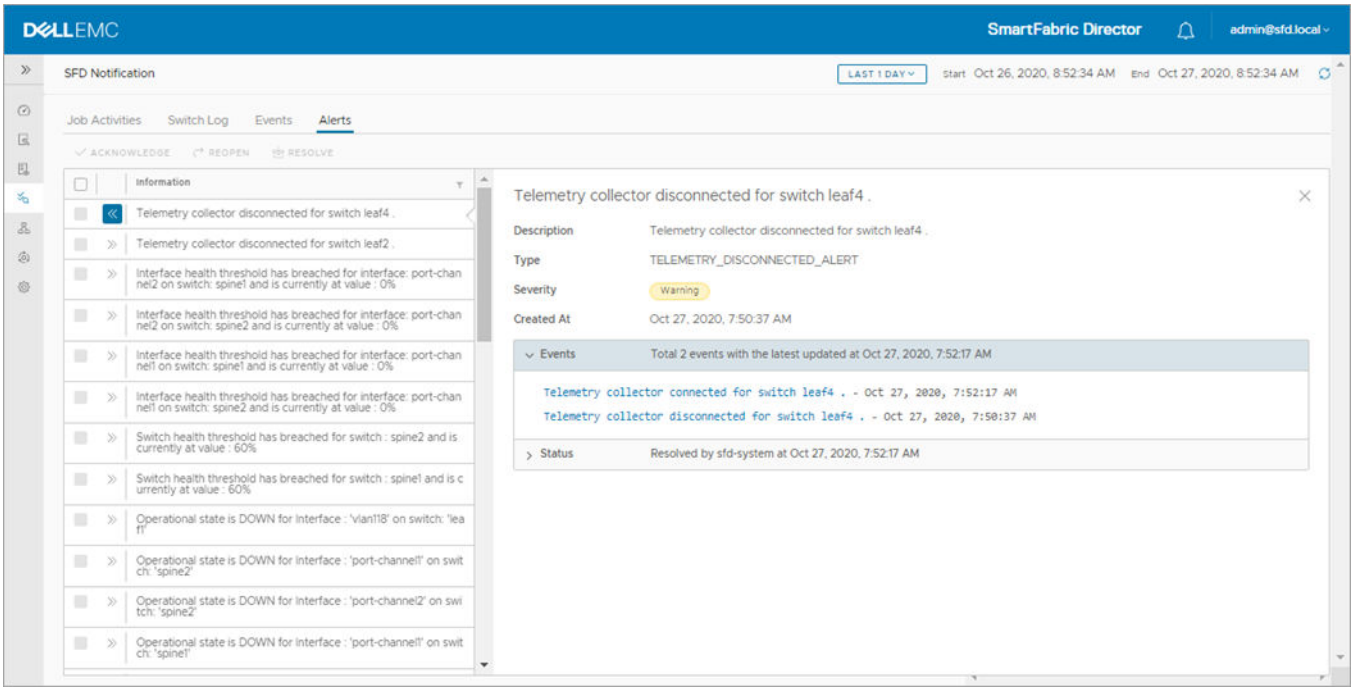
Alerts can also be cleared if the event triggering that alert goes away. In such cases, the *Status updated by* field displays as *SFD system*.



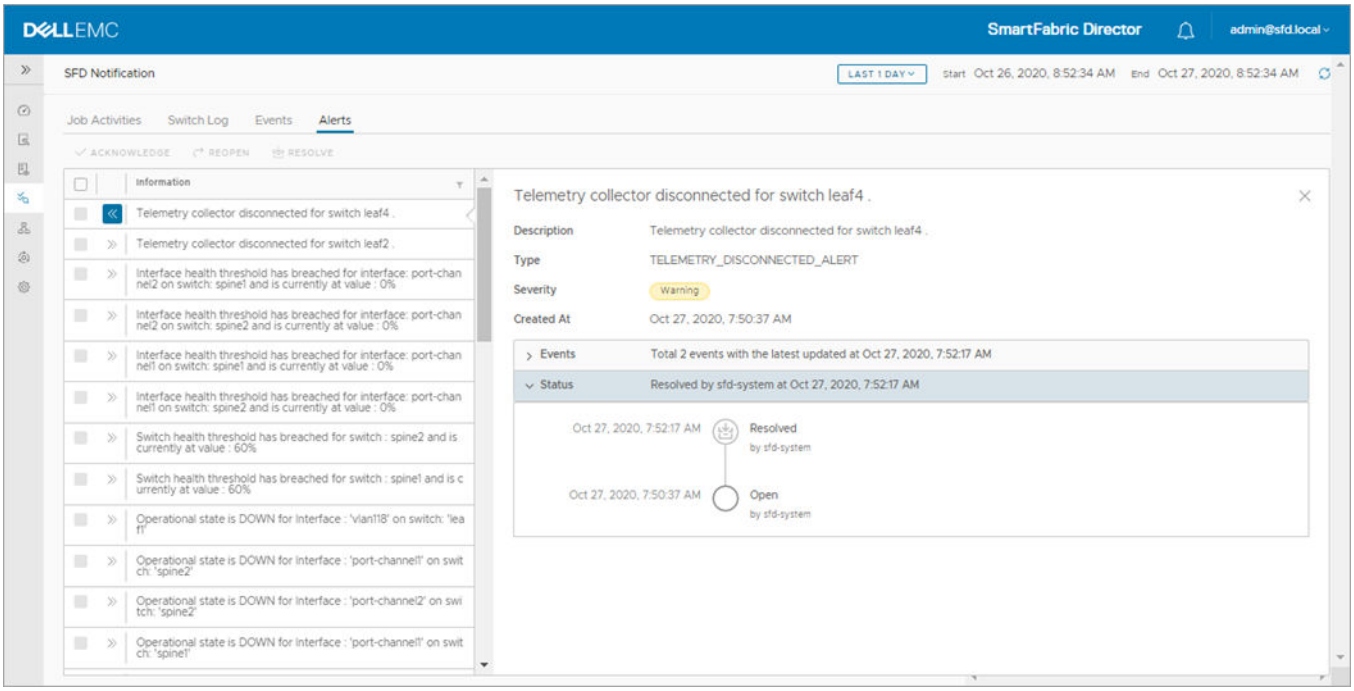
By default, the table is filtered to display Open and Acknowledged alerts. The Current status filter can be used to view any combination of open, acknowledged, or resolved alerts.



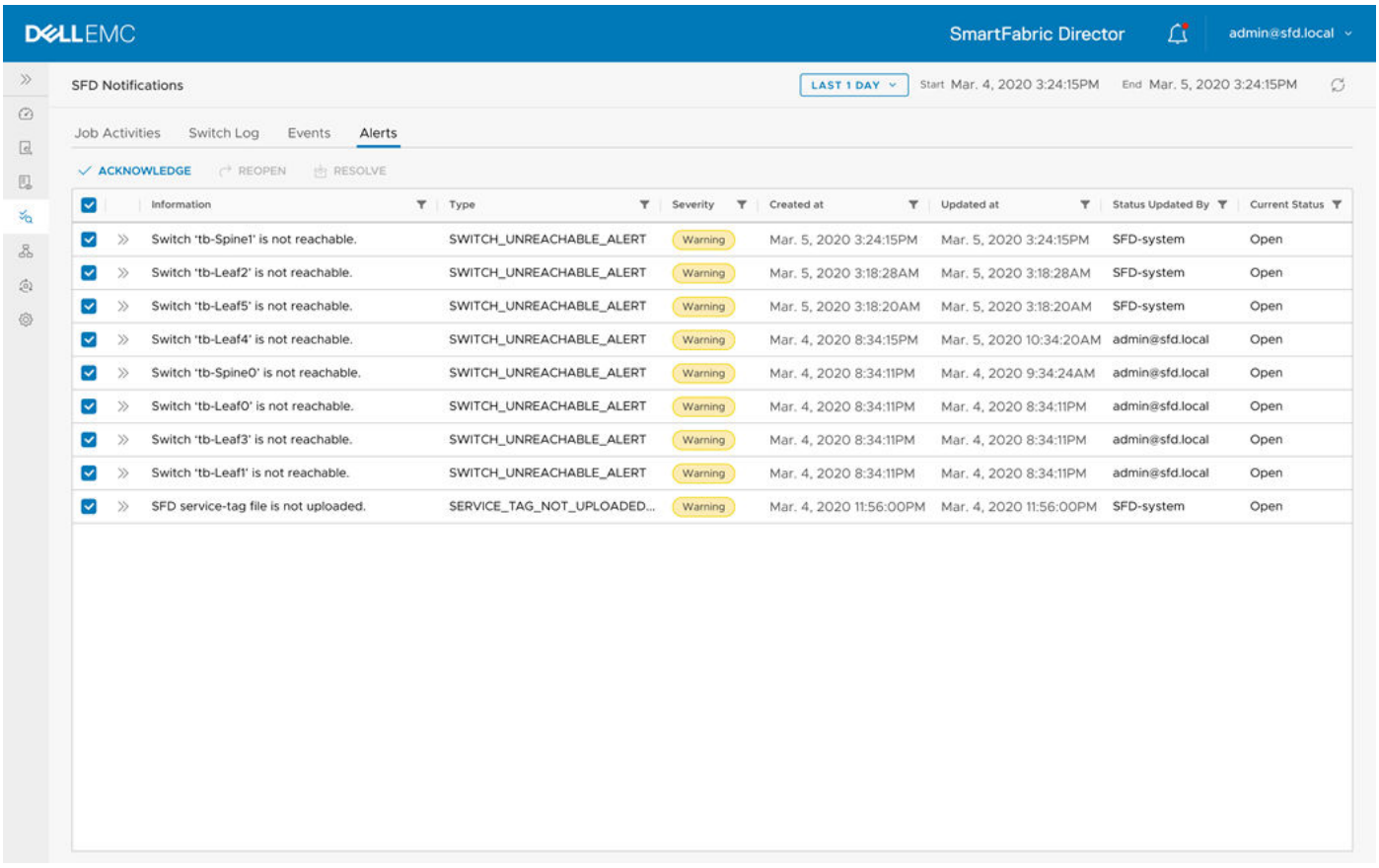
Click **>>** to view details.



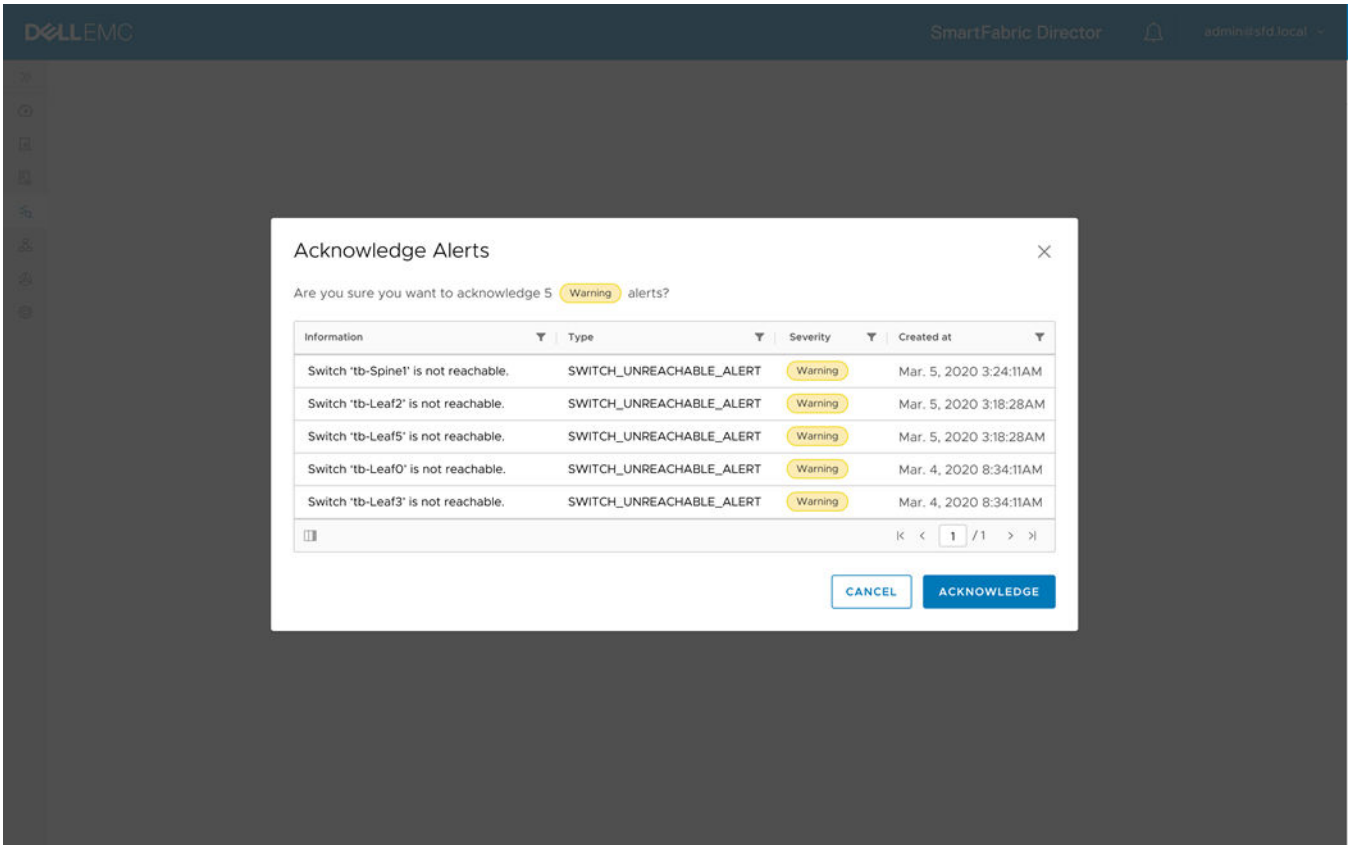
Alert detail includes a list of events that lead to the alert and status which display details on updates and the status of the alert.



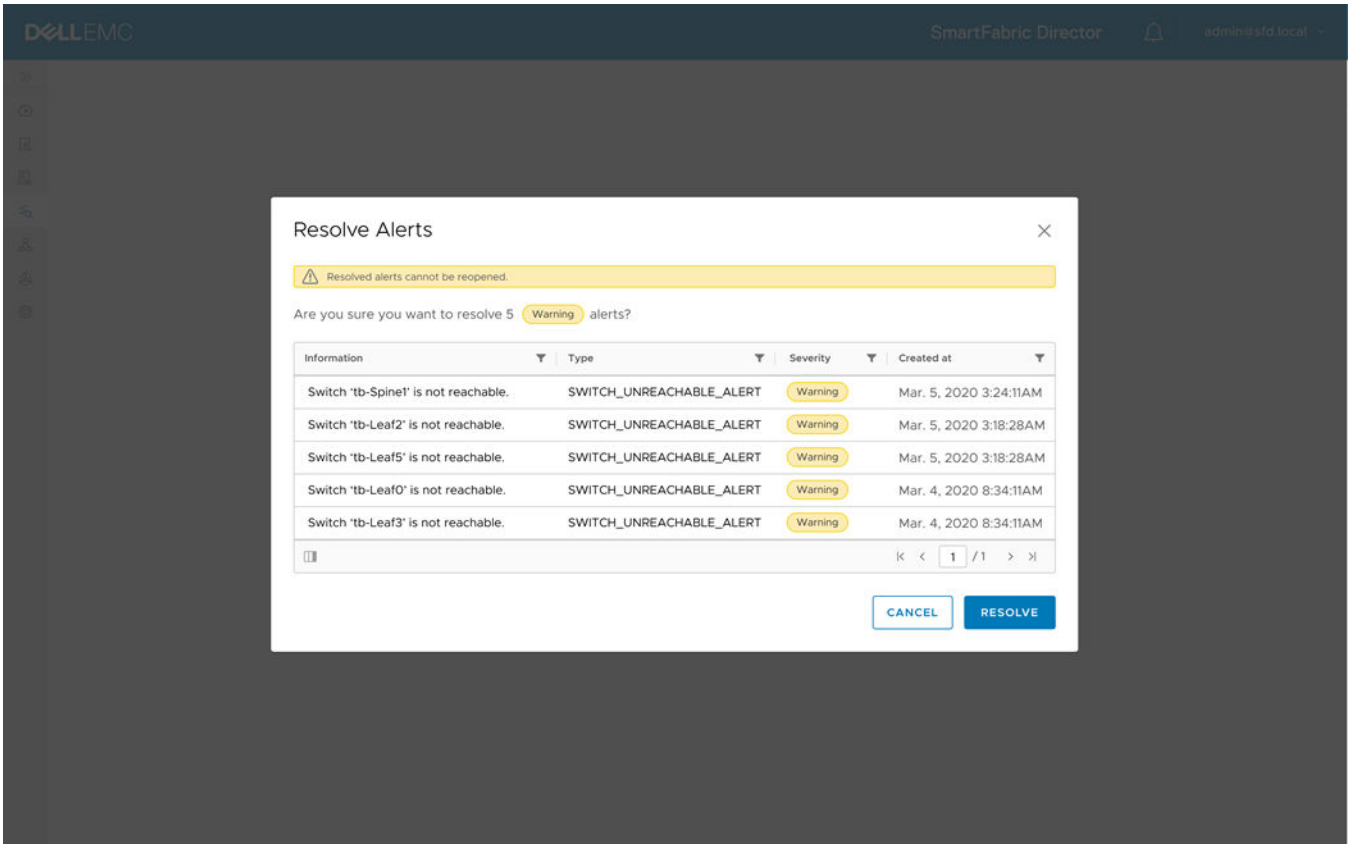
Bulk actions are available such as acknowledge an open alert, reopen, or resolve an acknowledged alert by selecting more than one alert.



Click **Acknowledge** to confirm the action when selecting more than one alert.

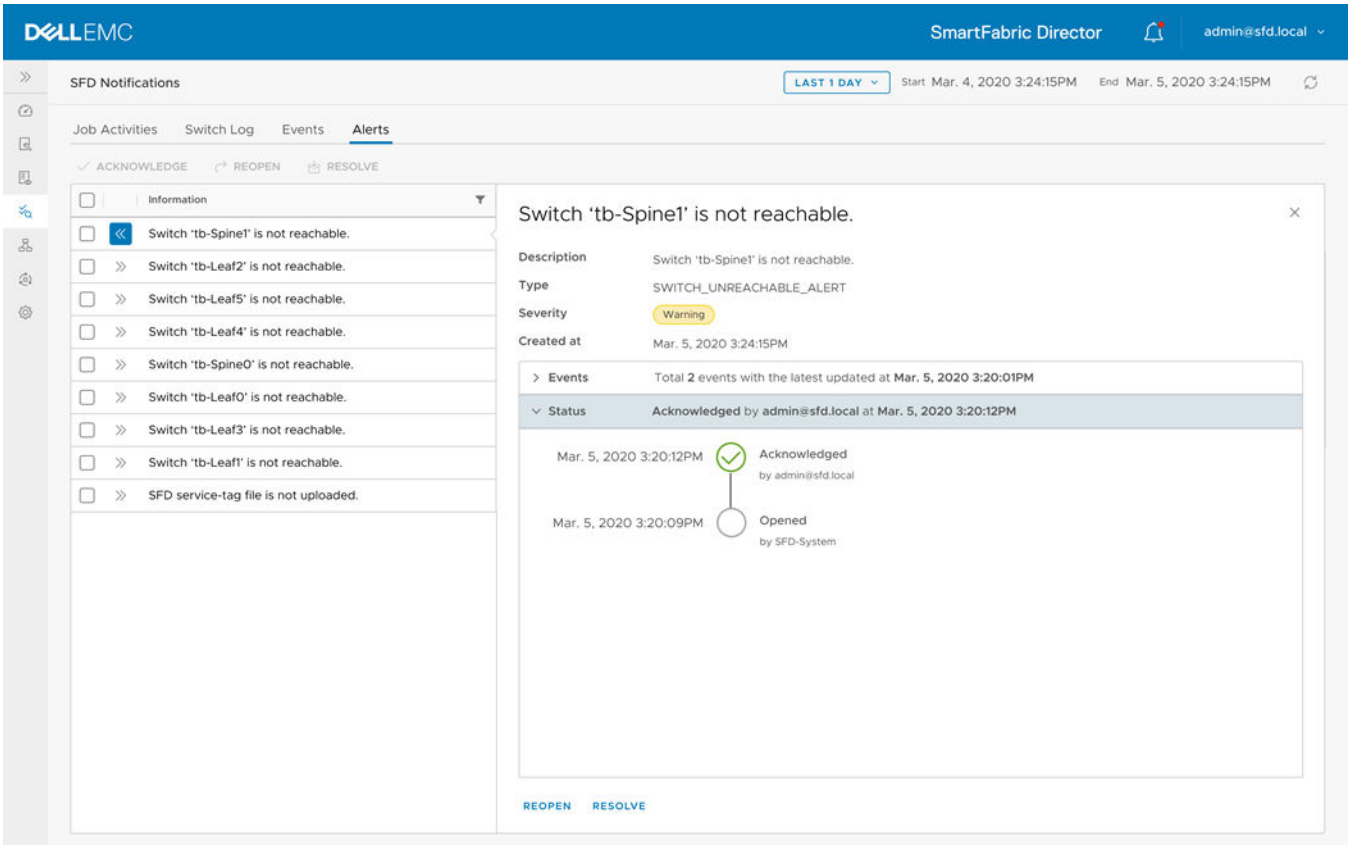


Click **Resolve** to confirm the action when selecting more than one alert.

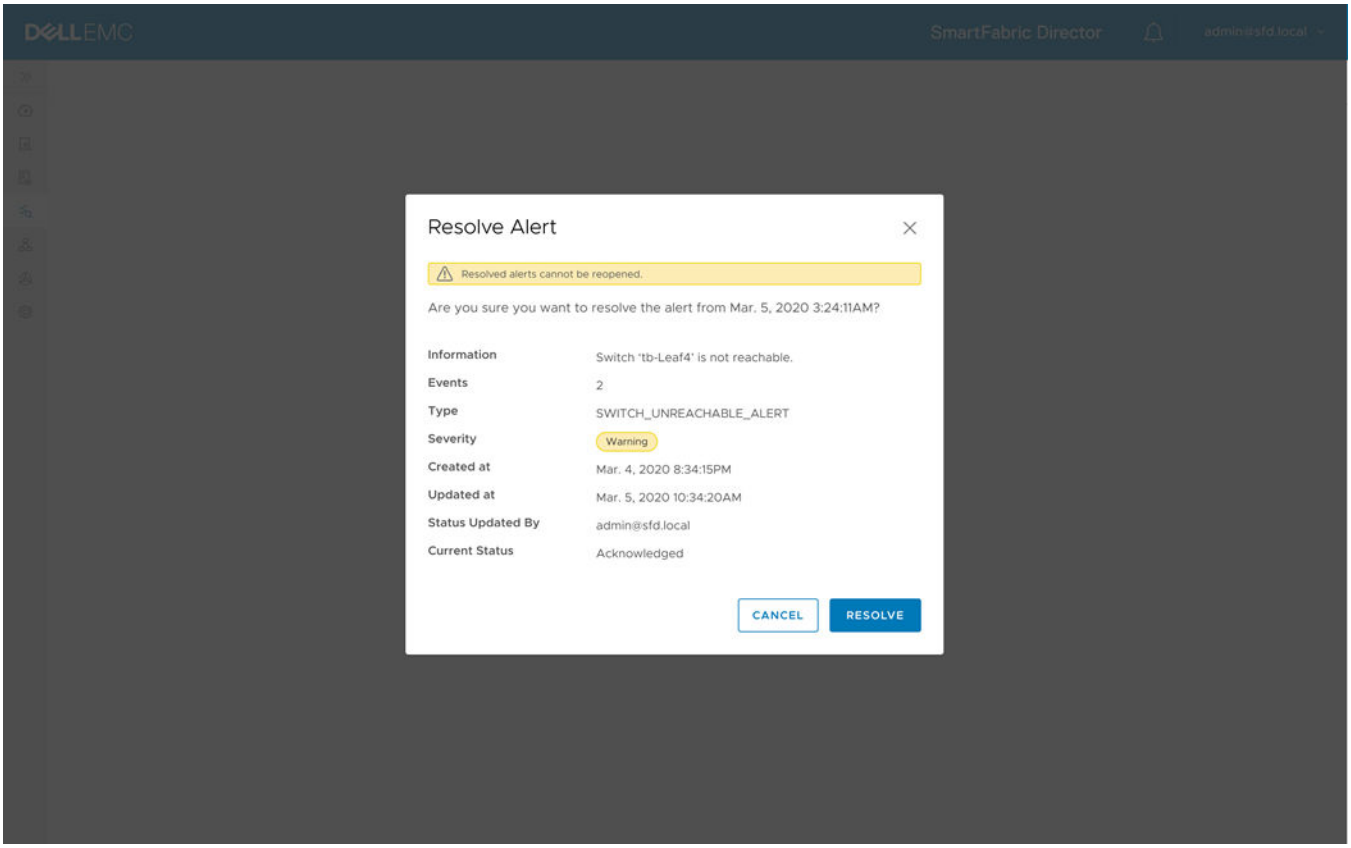


NOTE: Resolving an alert disables any additional actions such as reopen.

You can also acknowledge or resolve an individual alert.



Select the action and click **Reopen** or **Resolve**.



9

Backup and restore

Proper backup of SFD is crucial to restore the system to its working state in the event of failure. This feature ensures that all configuration data is backed up. We recommend regular backups — backup frequency and schedule depend on your business needs and operational requirements.

At a bare minimum, it is recommended to take backups after any successful deployment, prior to any software upgrades, and after any major Day 2 change.

The backup preserves wiring diagrams, fabric intents, system and user settings and optionally events, syslogs, and telemetry and monitoring data The recommendation is to store backup copies on a separate server than the one where SFD is running. SFD supports FTP and secure FTP (sFTP) to transfer the backup .tar file to the backup server.

In the unlikely event that an SFD instance is corrupted and a new SFD OVA (of the same SFD Image version) is to be launched, the operator can spare the trouble of reimporting the fabric and reconfiguring the fabric Intent by restoring to a previously known state from backed up data.

NOTE: The intention of backup and restore is to restore previously backed up data within the same version of SFD, and not across SFD versions. The upgrade feature must be used to upgrade SFD to a higher version.

Topics:

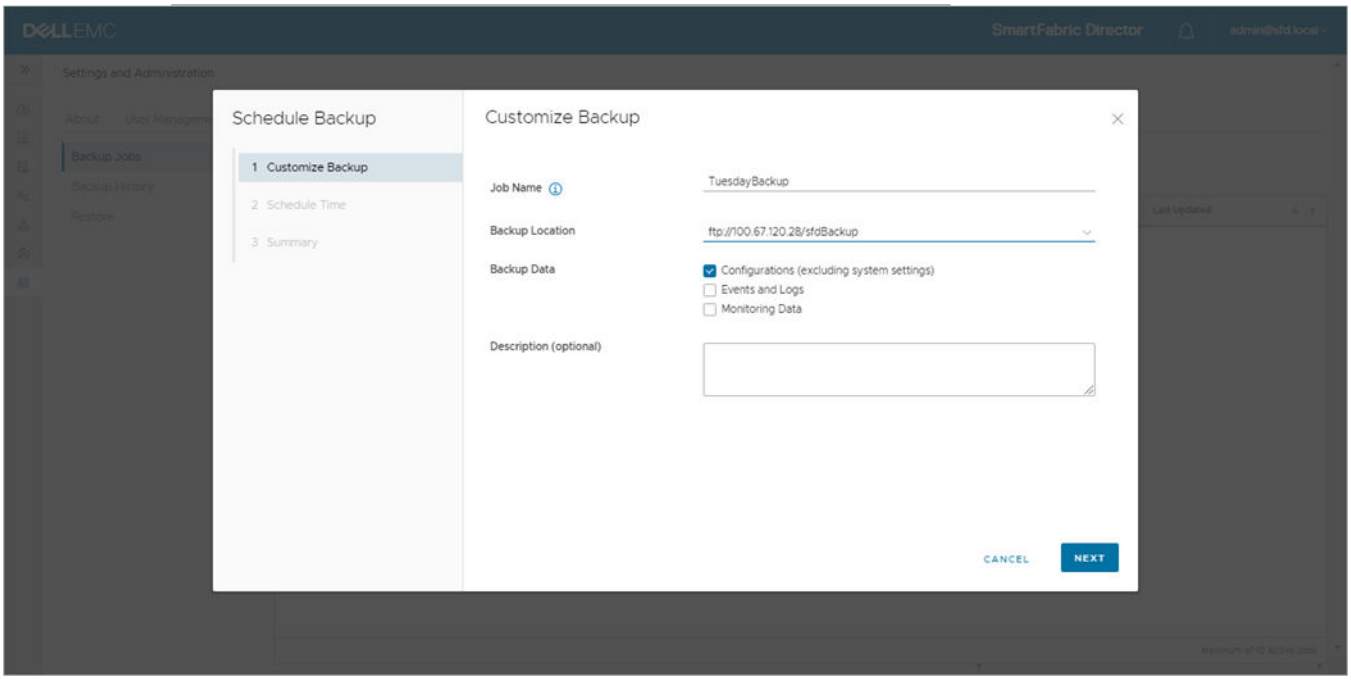
SFD backup

Prior to SFD 2.0, backup and restore could be done using SFD CLI. SFD 2.0 adds user interface support for backup and restore.

Create a new backup job

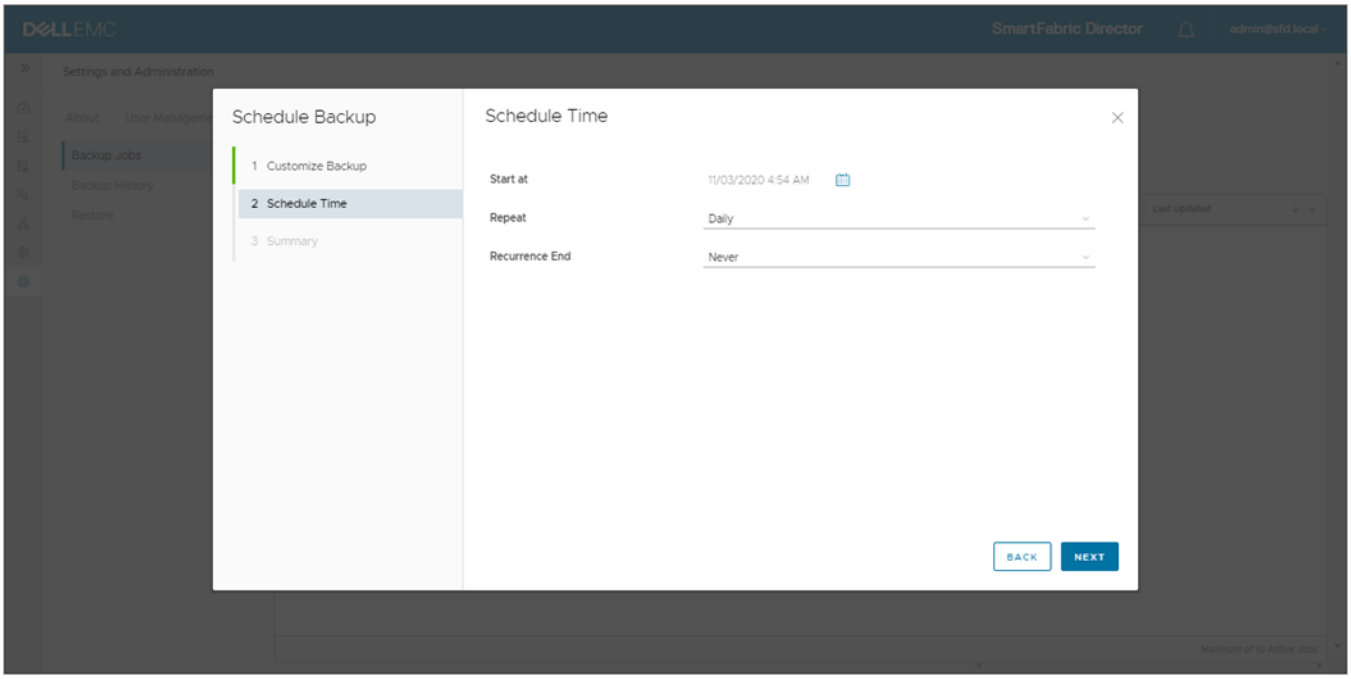
1. Select **Settings and Administration > Backup & Restore**.
2. Click **New Job**, specify a job name and the backup location where SFD uploads the backup .tar file, which optional data to backup, then click **Next**.

   NOTE: Events and logs, and monitoring data is optional. Select these check boxes if you would like to include this information in your backup.



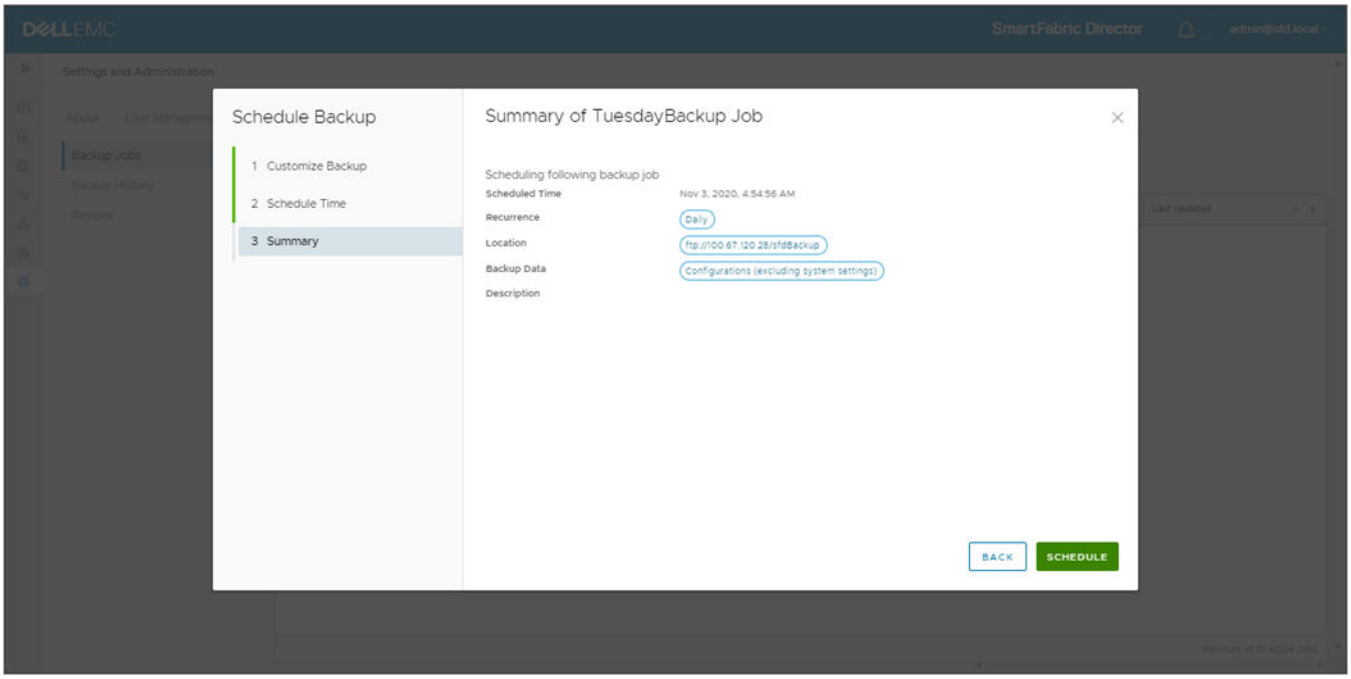
SFD supports FTP or secure file transfer protocol (SFTP). By default, the configuration (wiring diagrams, fabric intent, user management) is in the backup file. You can choose to add Events and Logs to be in the backup file. You can also choose to include Monitoring data including switch syslogs in the backup datafile.

3. Specify if the backup should repeat, when to end, then click **Next**.

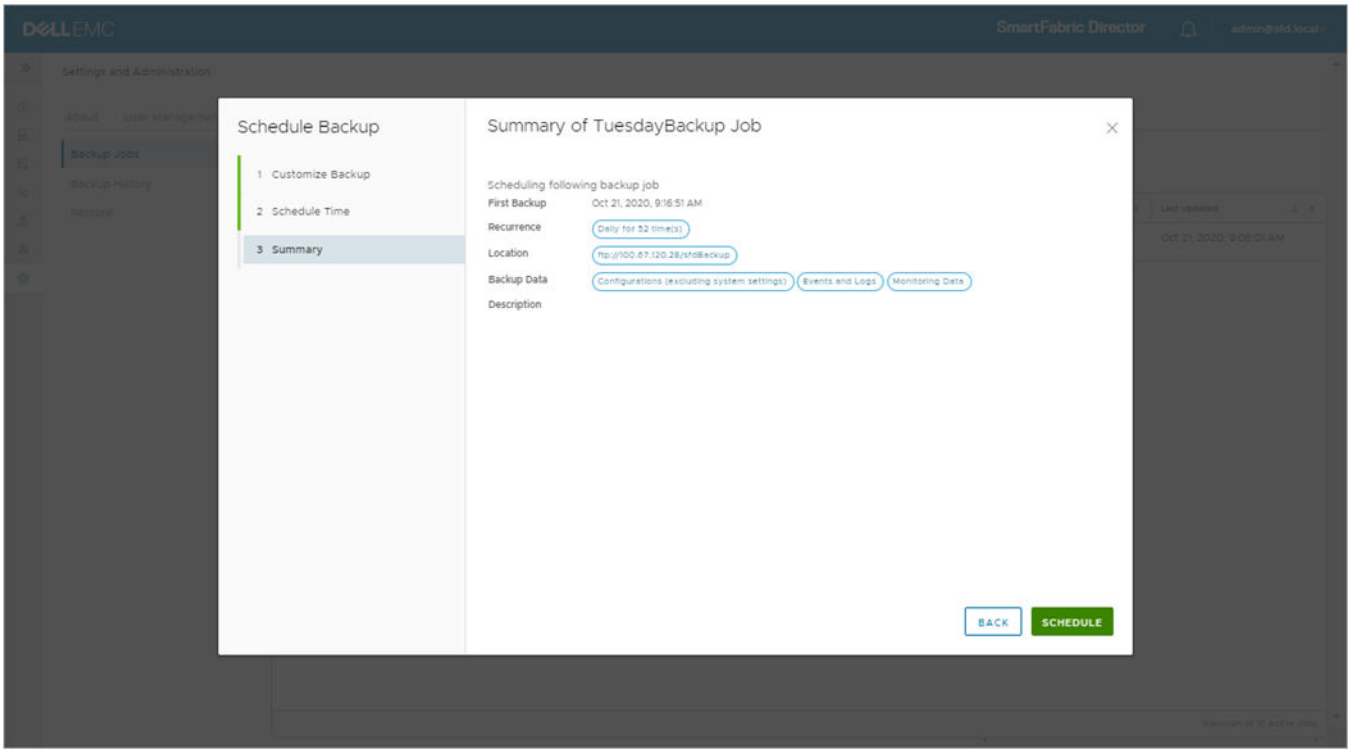


SFD allows regularly scheduled backups or a nonrecurring backup job. For a one time or nonrecurring job, select **Does not repeat**. SFD supports backup recurring hourly, daily, or monthly. If Hourly is selected, then a backup job is run every hour starting from the day and time selected. For Daily, a job is scheduled every day at the time specified.

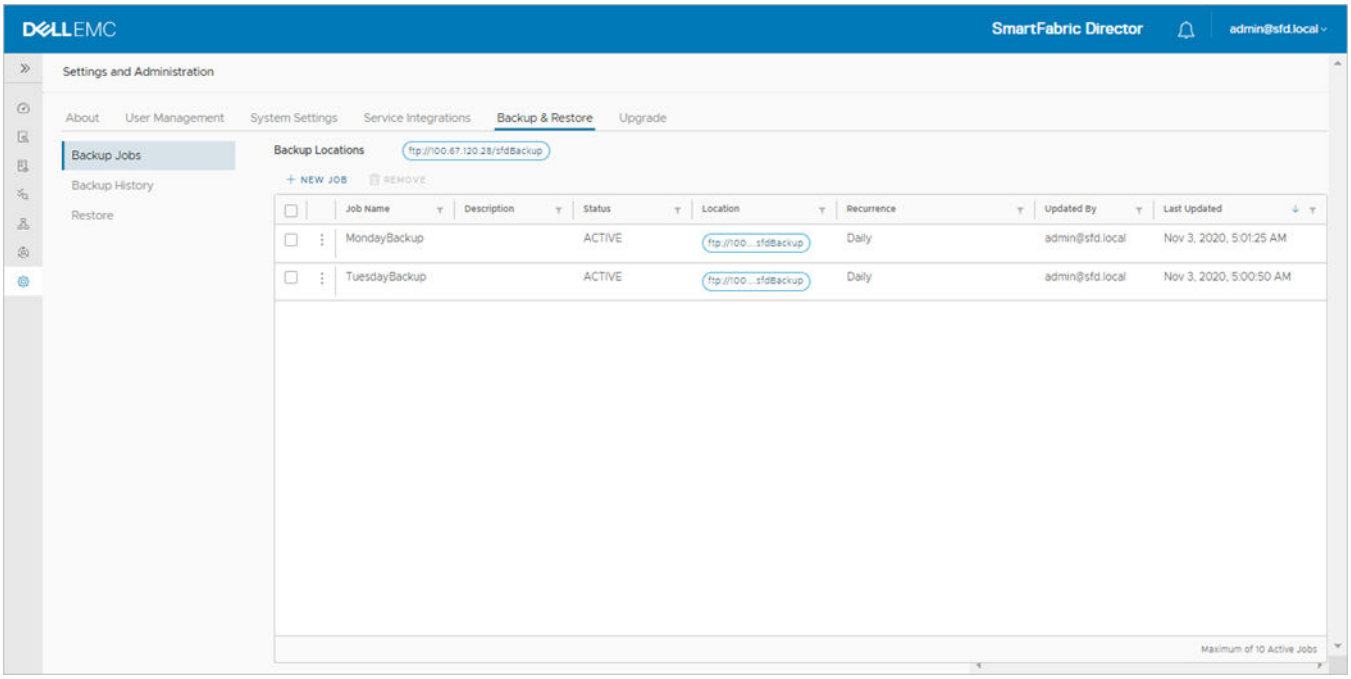
4. Review the information, then click **Schedule**.



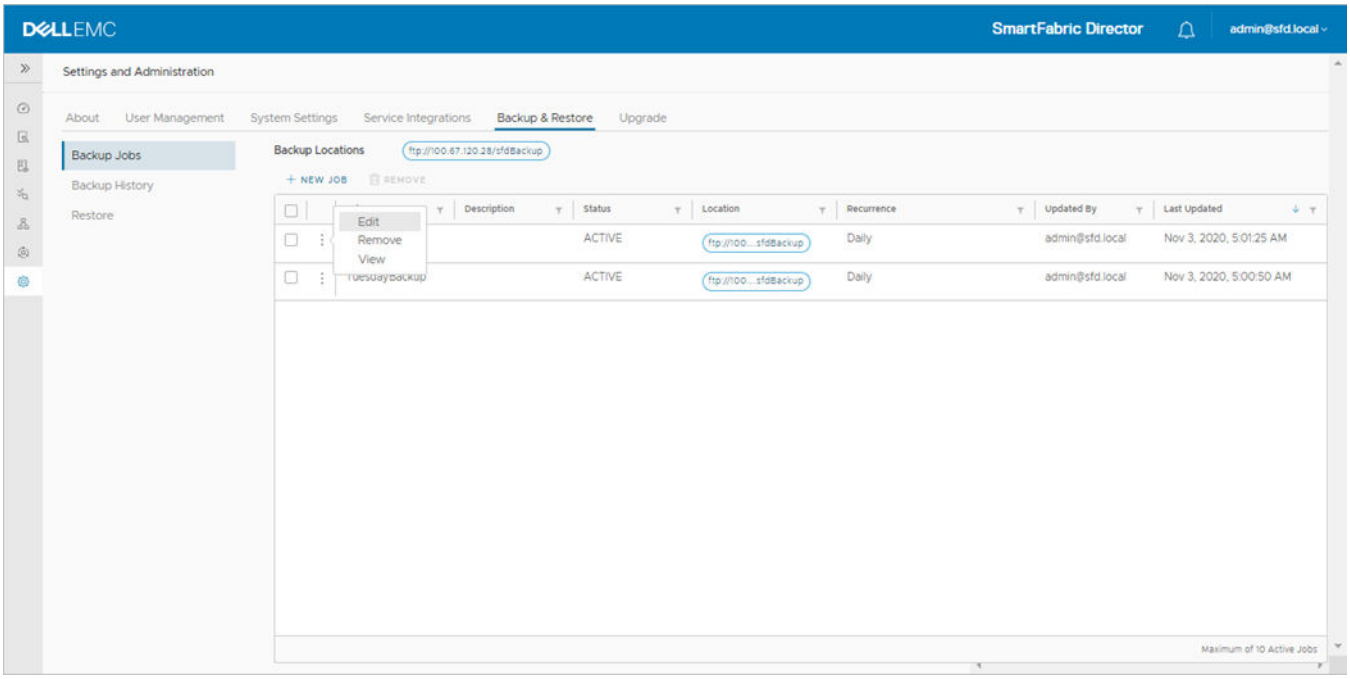
Here is an example for a TuesdayBackup job. This job repeats daily for 52 weeks.



Both scheduled backup jobs display.

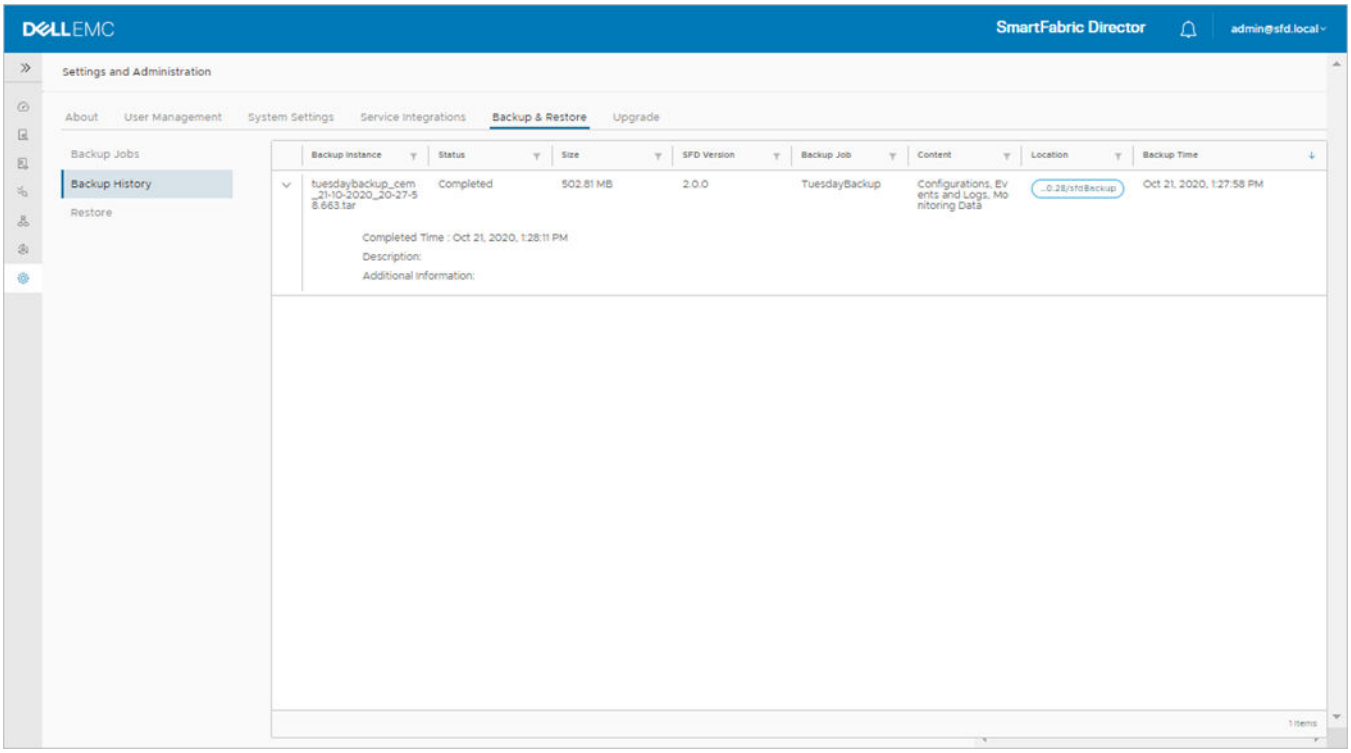


5. Continue adding backup jobs, or you can click on the three dots of any scheduled backup, then select **Edit**, **Remove**, or **View**.



6. The backup job scheduled, and the backup location are available to view. SFD activities show the progress of the backup. The name of the backup .tar file that is saved on the backup server is generated by SFD and is based on the job name. Select **View** to display the details.

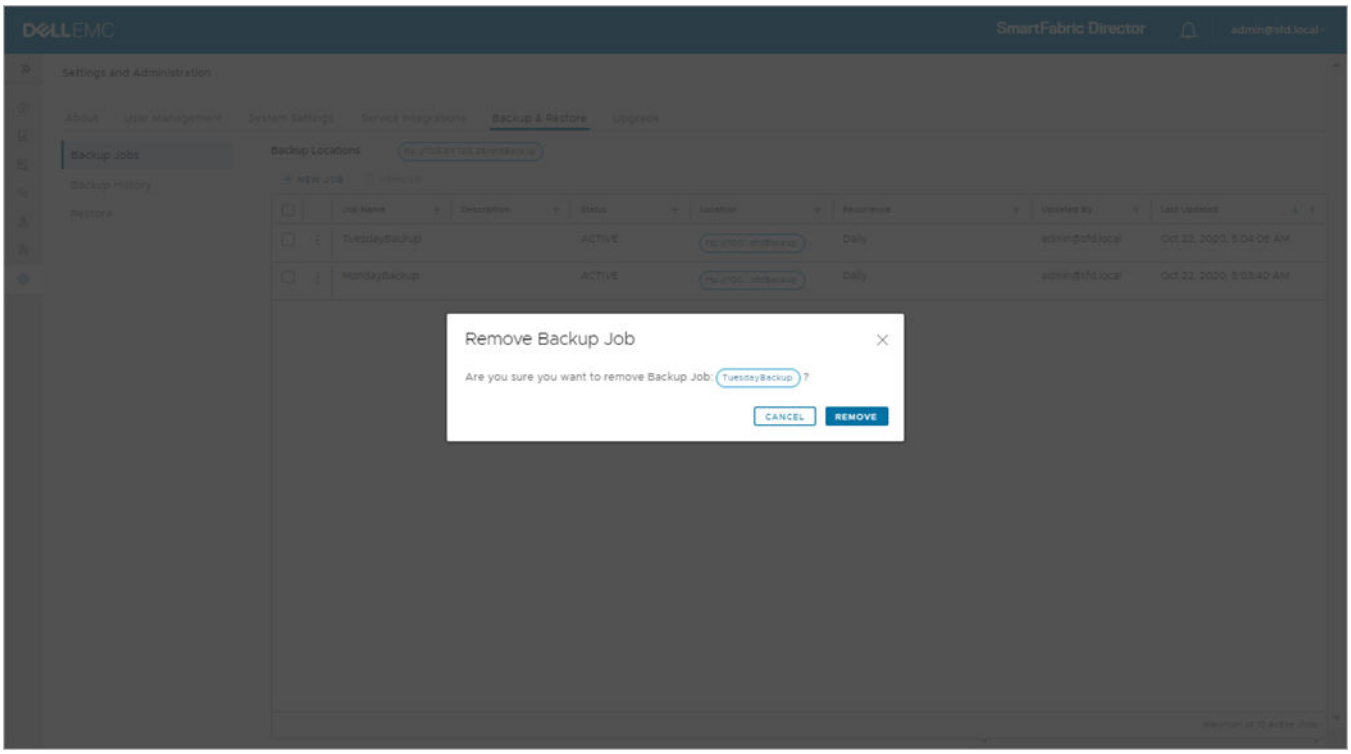
NOTE: It is recommended to not rename the backup file on the destination backup server.



Remove backup job

Removing a backup job cancels any future running of the job. The backup job history is preserved, and any backup files that are generated by the previous execution of the job would have been saved on the destination backup server, as SFD does not alter backup jobs.

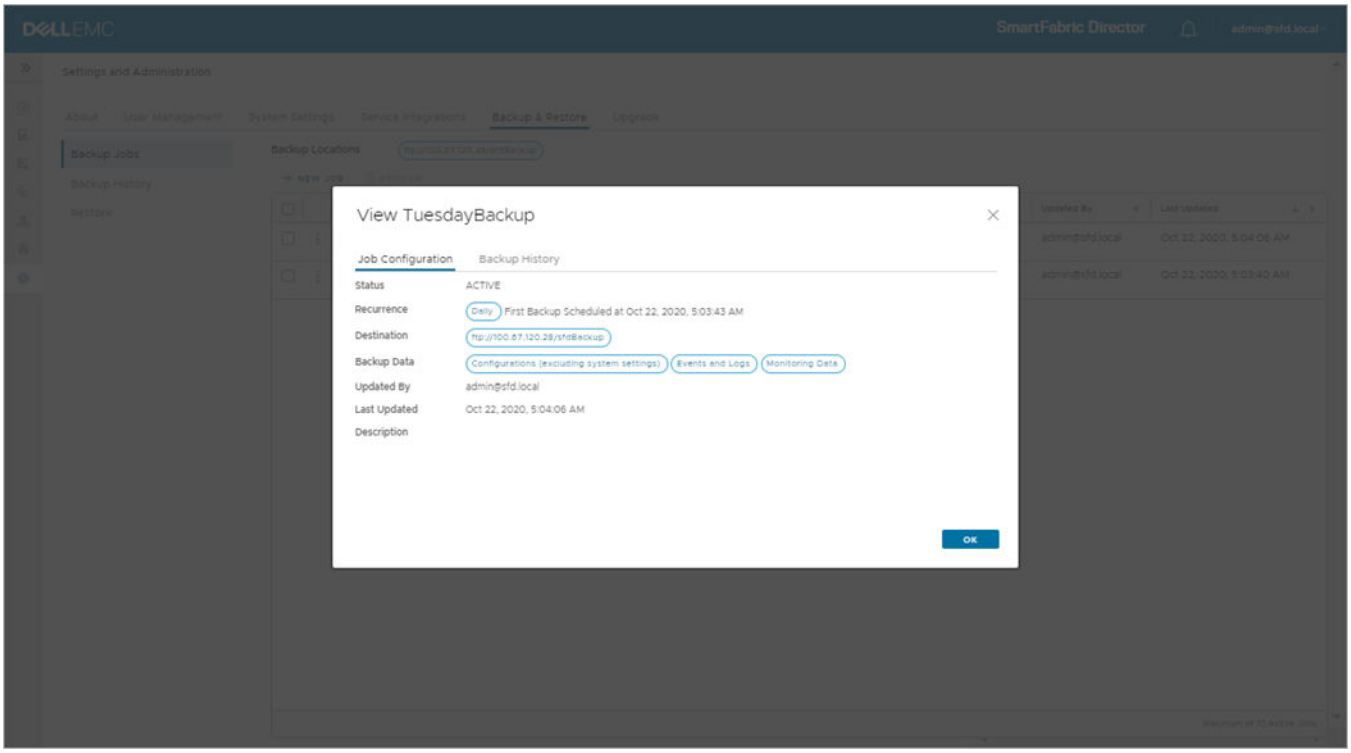
1. Select a backup job, click on the three dots, then select **Remove**.
2. Click **Remove** to confirm removal of the backup job.



View backup job

1. Select a backup job, click on the three dots, then select **View**.

2. Click **OK** to close the window.



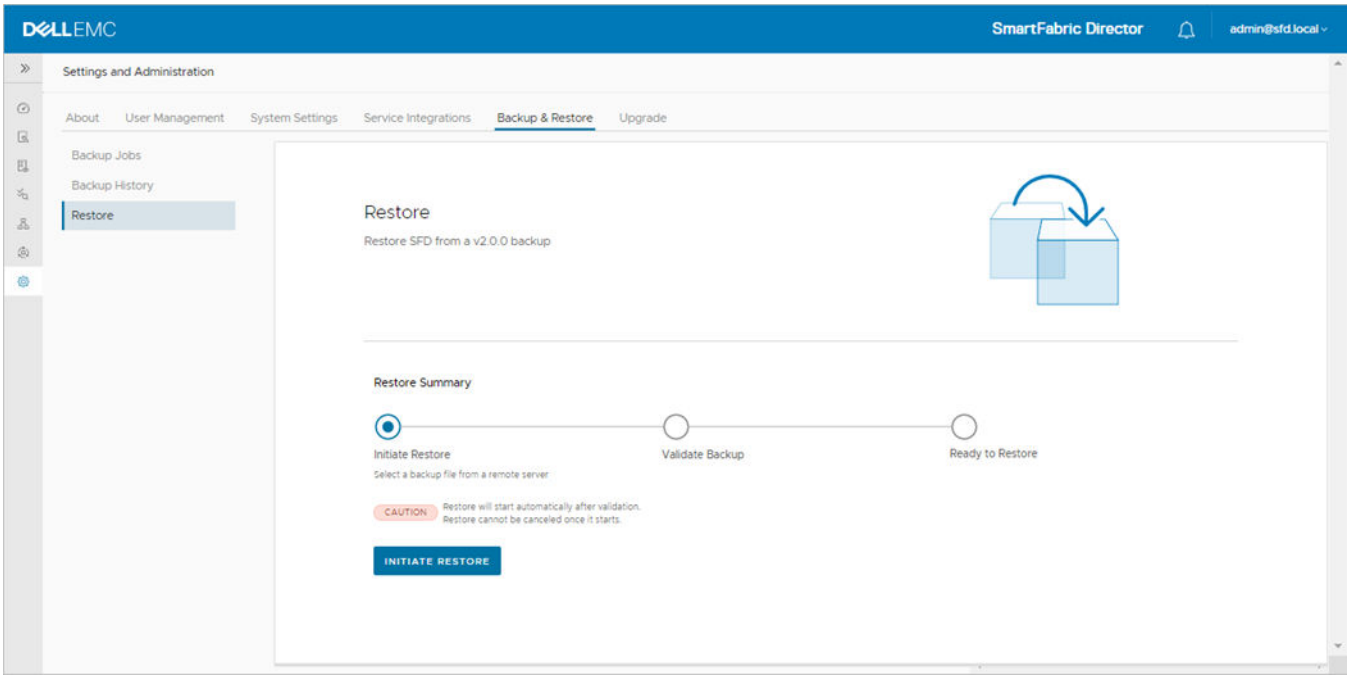
SFD restore

In the rare instance that the SFD instance is corrupted, you can install a fresh instance and restore it from a previously backed up instance.

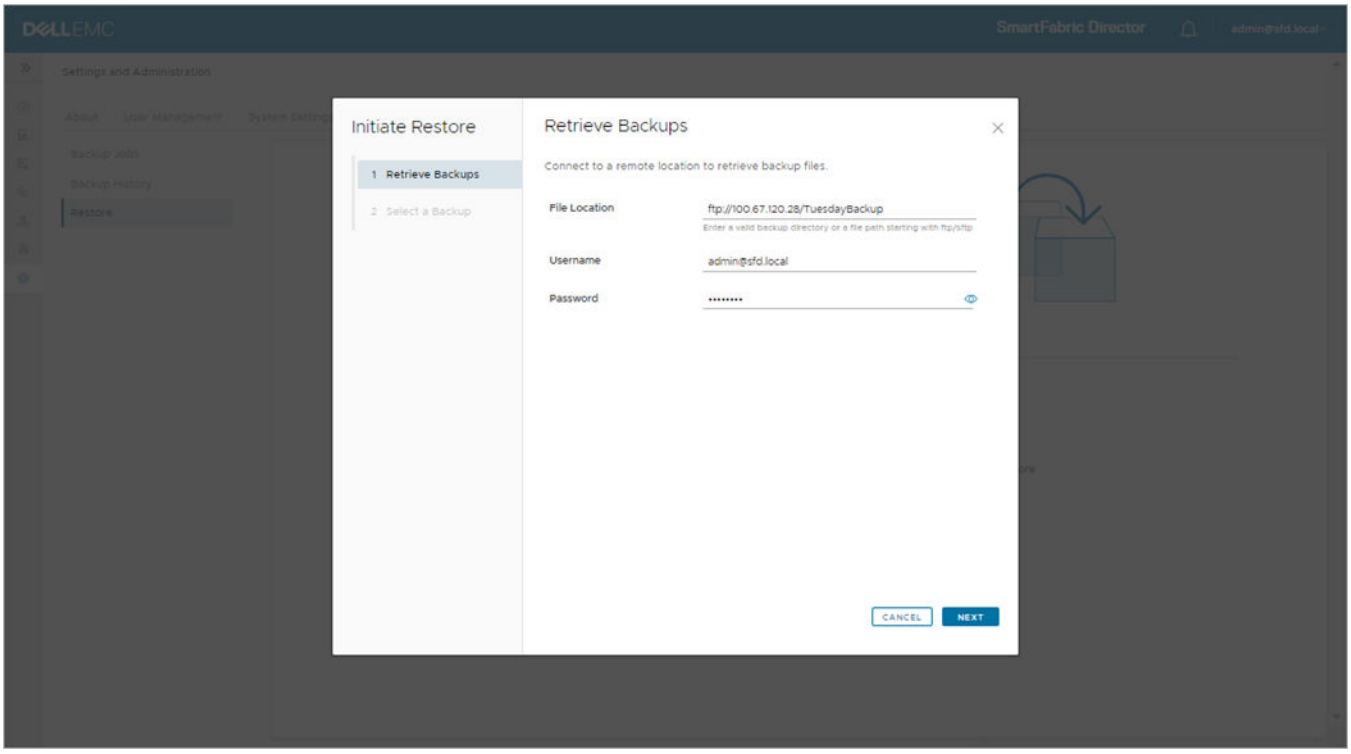
NOTE: Restore of backup data between dissimilar SFD versions is not supported due to potential data model changes across SFD versions. SFD upgrade must be used to upgrade SFD to preserve data across SFD versions and data model reconciliation. SFD restore should not be used for upgrading SFD.

Restore backup job

1. Select **Settings and Administration > Backup & Restore > Restore**, then click **Initiate restore**.

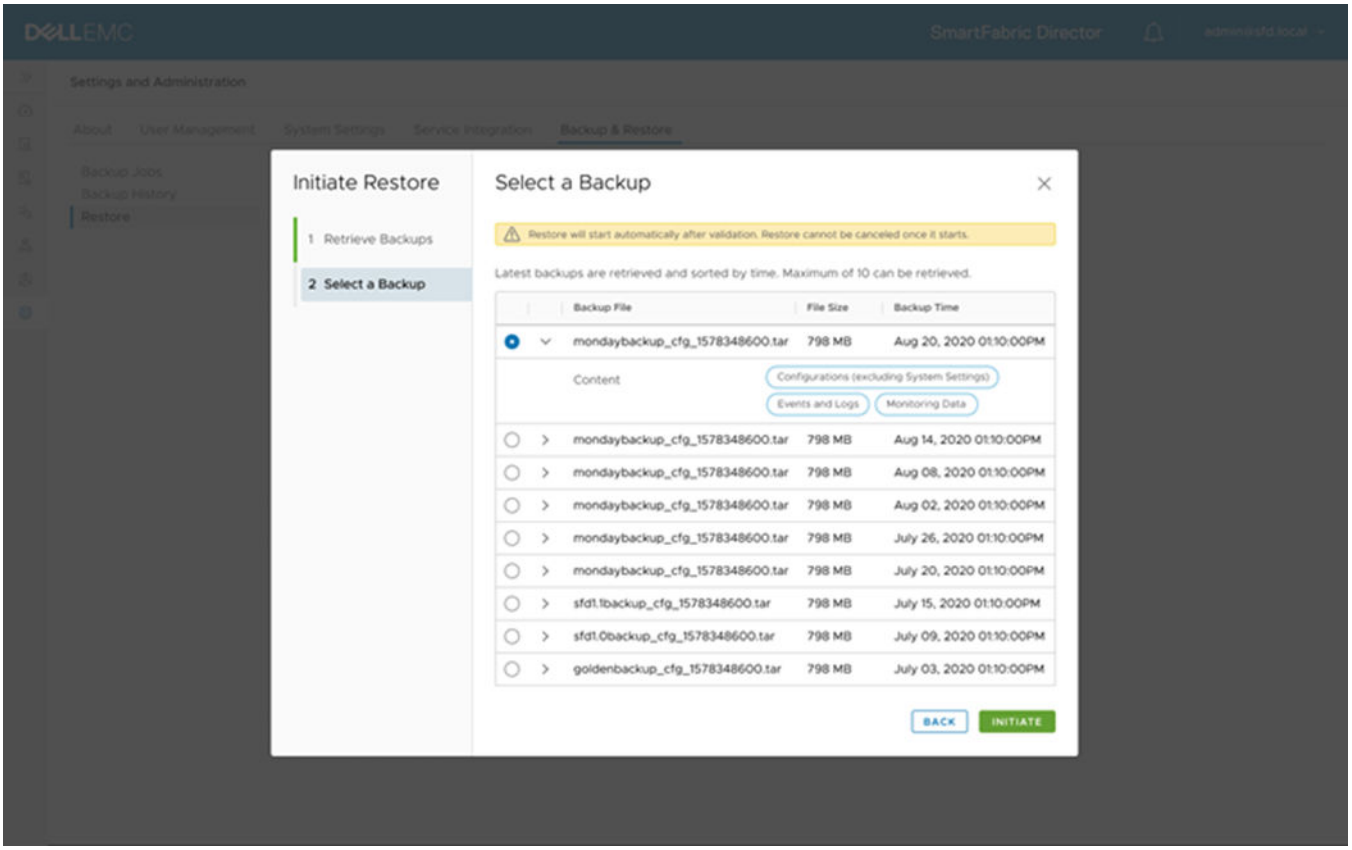


2. Specify the file location and the credentials that are required to retrieve the backup file, then click **Next**.

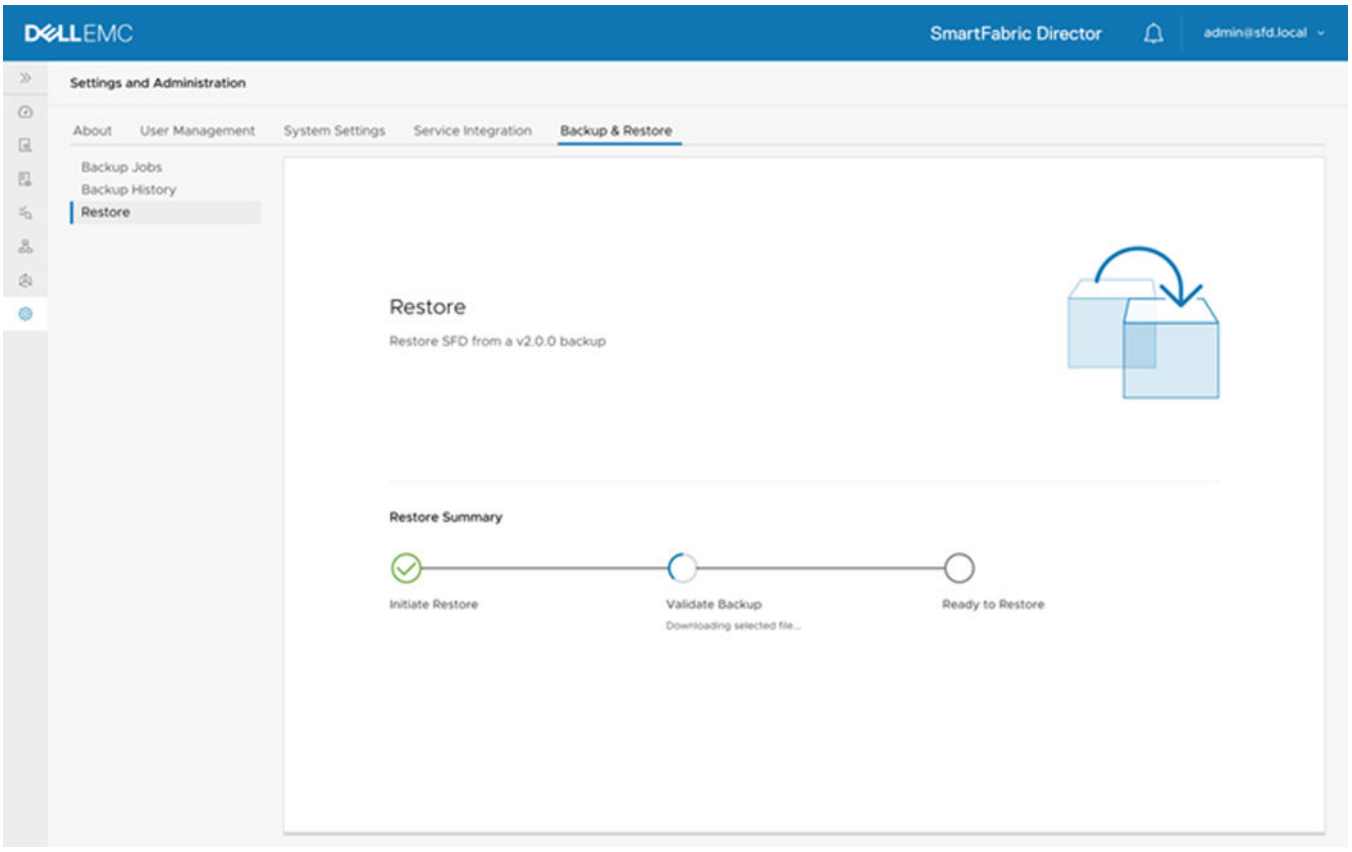


SFD uses this information to obtain a list of backup files from the specified location. The first step in restoring is to direct SFD to retrieve the backup .tar file to restore from. SFD fetches up to 10 backup files and sorts them based on the timestamp.

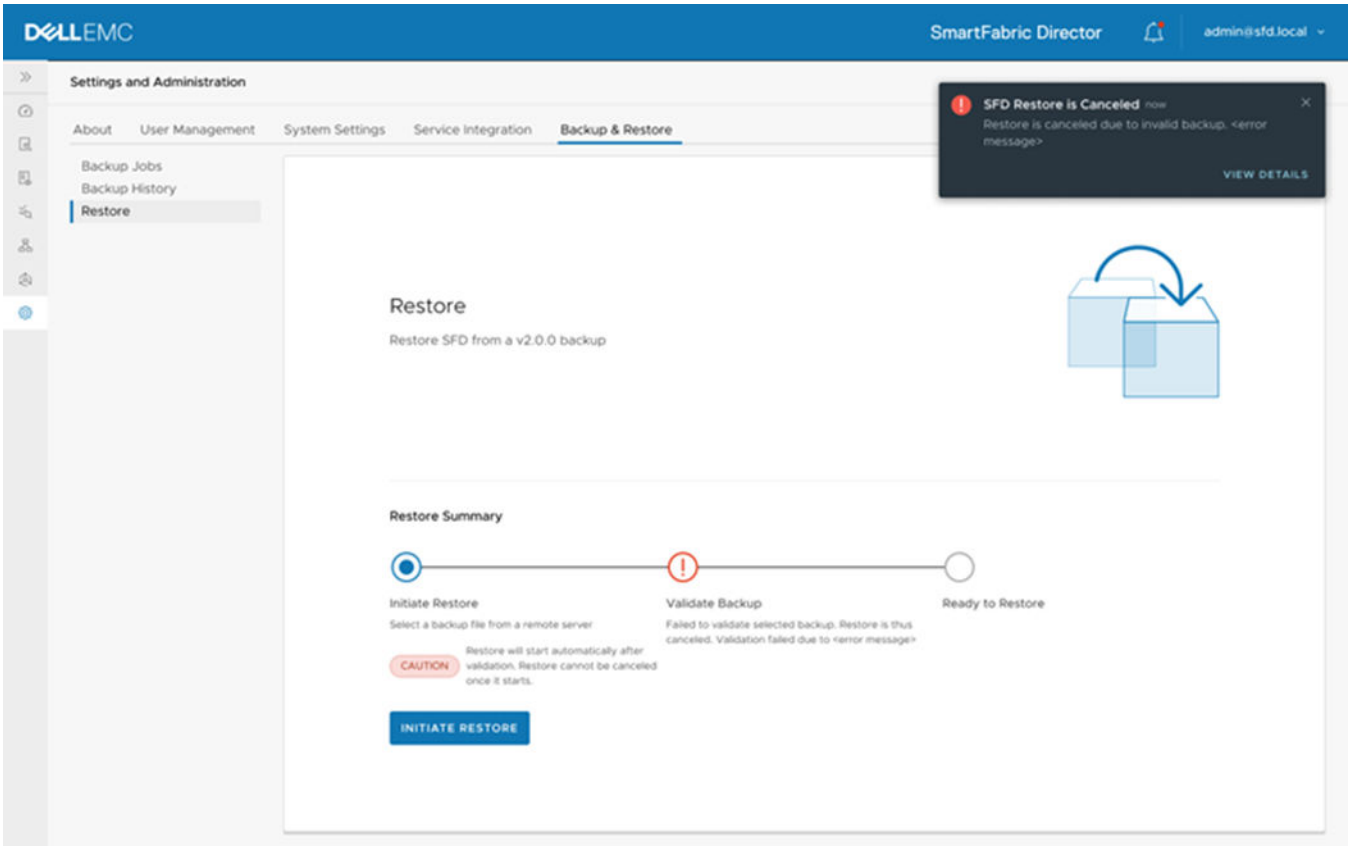
3. Select a file to initiate a restore, then click **Initiate**.



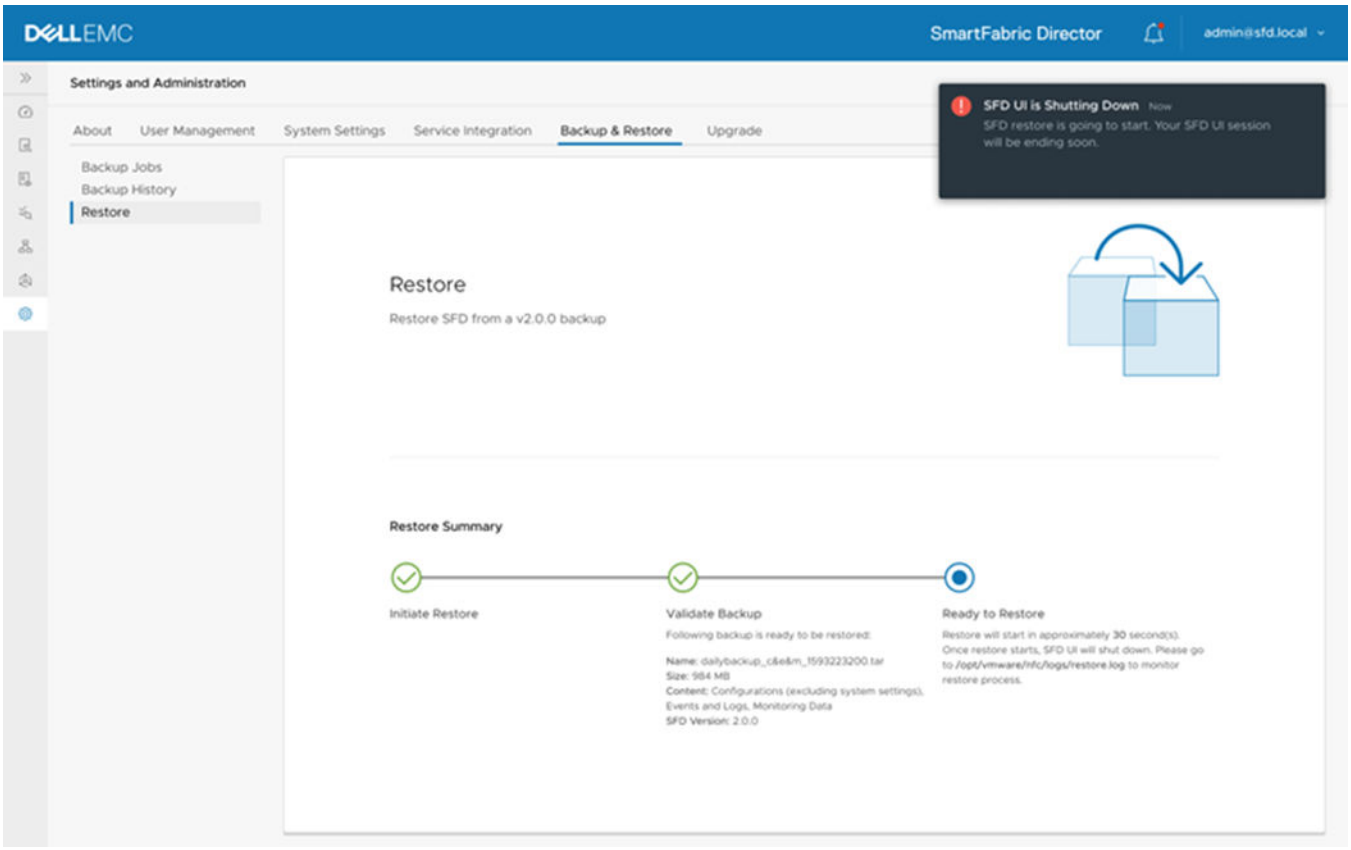
When a file is selected, details about the contents display. This information is decoded by SFD from the backup filename. SFD downloads the selected backup file and starts the validation process. The progress of the initiate restore displays.



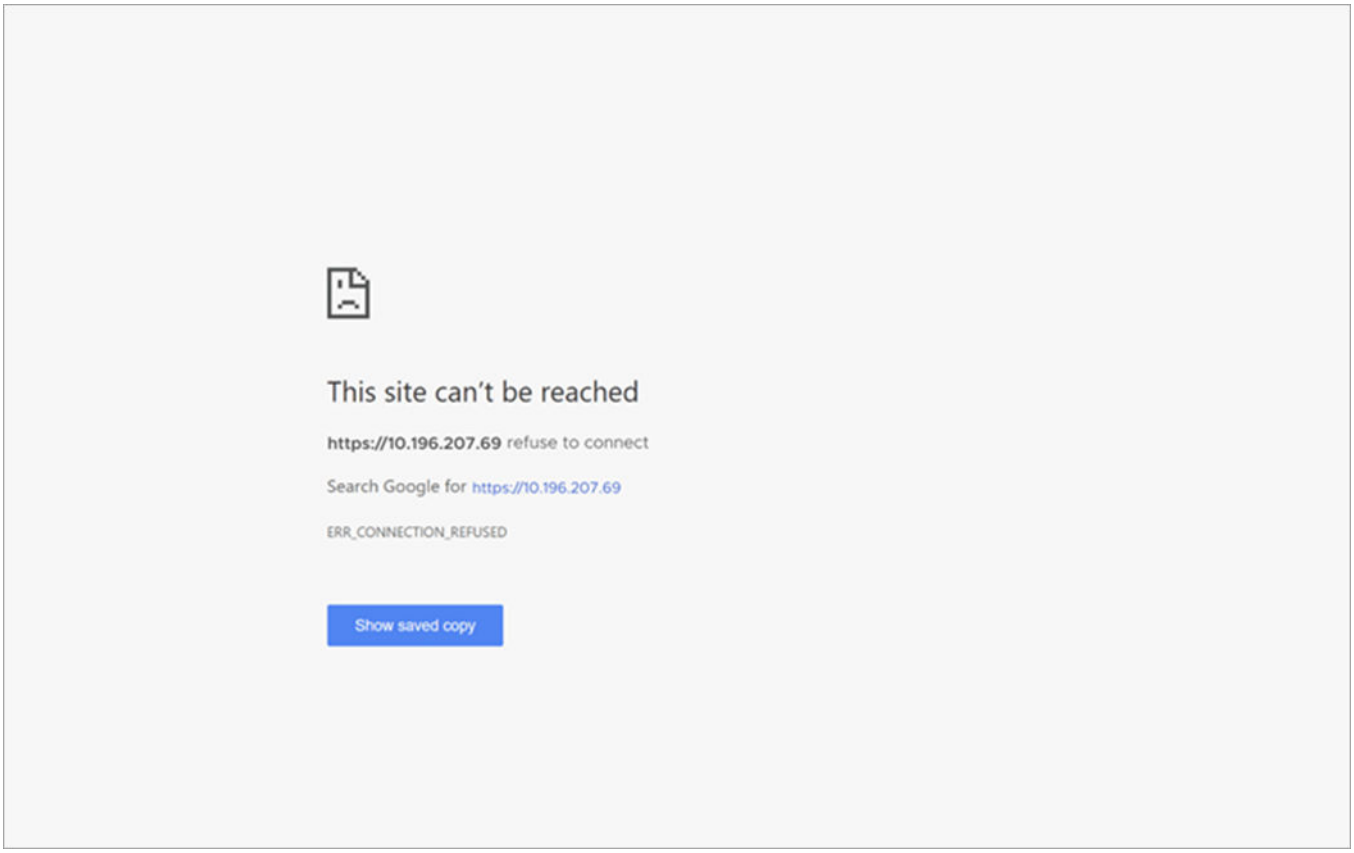
If the validation fails, the failure displays in the restore summary. The SFD restore is canceled, and a notification displays.



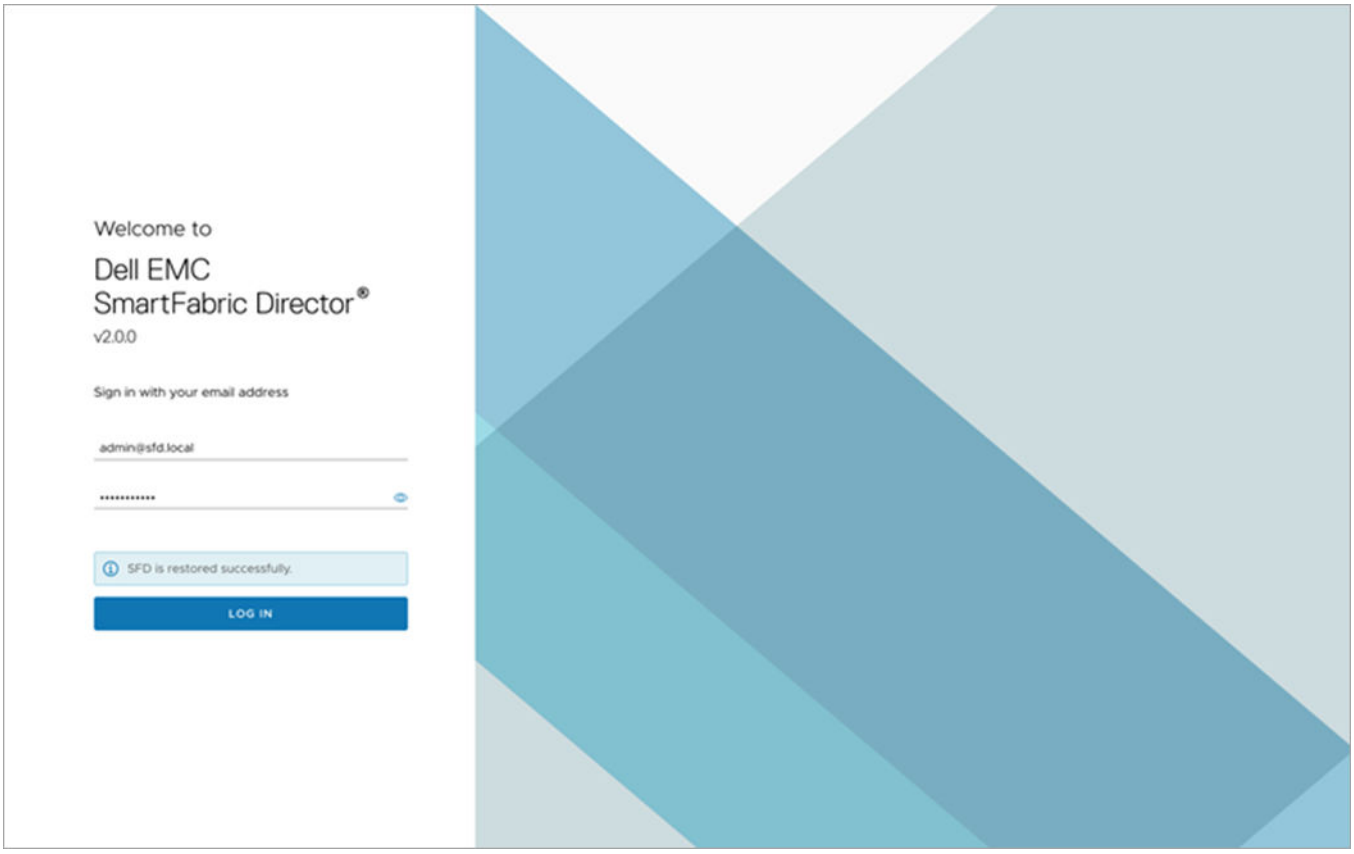
On successful validation, SFD is ready to be restored. During restoration, access to SFD is lost and the browser session shuts down and restarts.



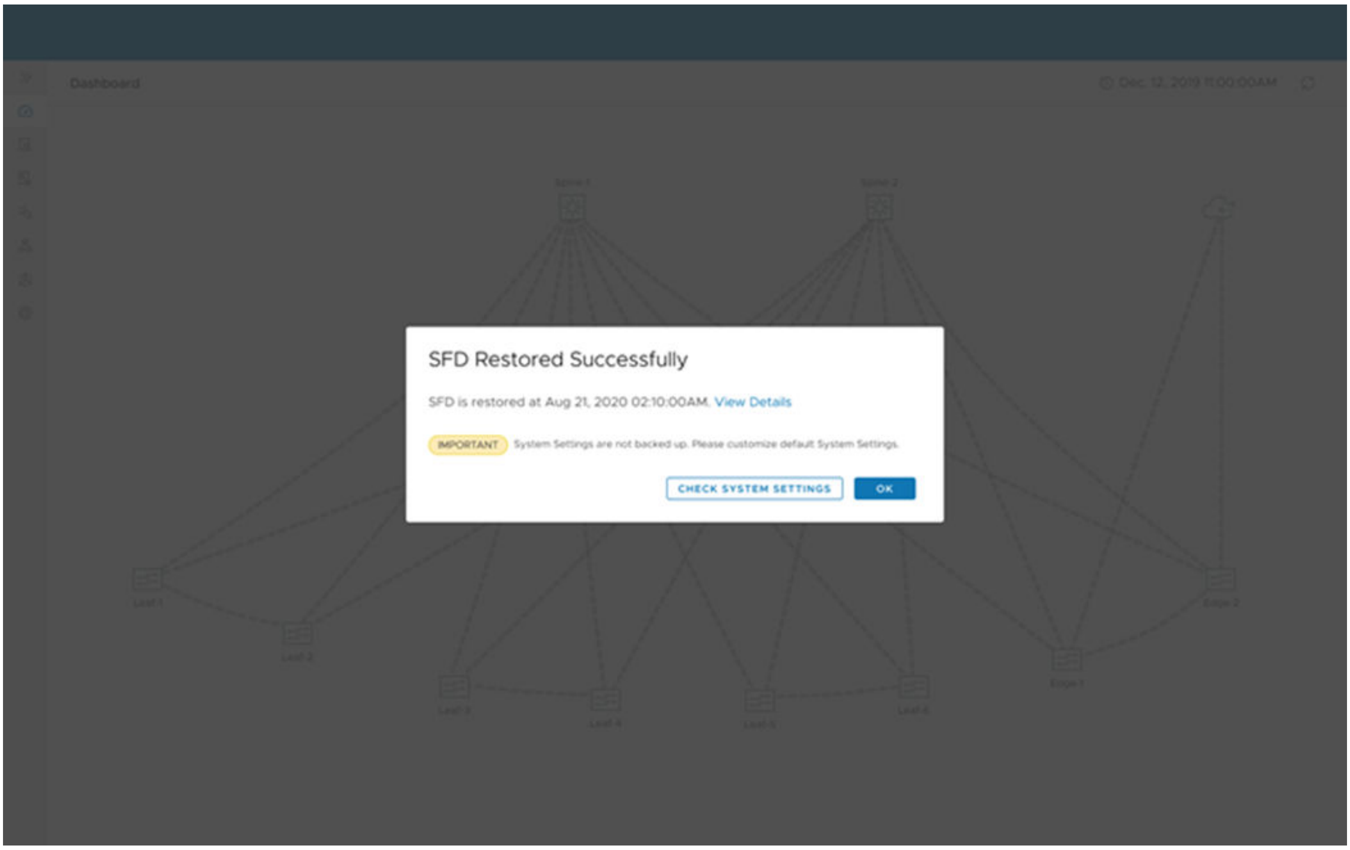
When SFD has shut down the browser session, this example shows the lost connection.



4. Reconnect to SFD, enter your SFD credentials, then click **Log in**. The login screen shows that SFD was successfully restored.



5. Click **Check system settings** and verify that the fabric intent is correctly configured on the switches, and the fabric is operating correctly.



NOTE: Any SFD intent changes, events, alerts, switch telemetry, and syslogs that happened after the time it was backed up in the file that is used for restoration will be overwritten by the restore process.

Backup and restore CLIs

Use these commands to backup and restore data using the command-line interface (CLI) within the SFD application. See Using the CLI for complete information.

backup instance list

Lists all backup instances.

Command `backup instance list`

Options None

Usage None

Example

```
sfd> backup instance list

+-----------------------------------------------+----------+--------+-------------+----------------+------------------+------------------------------------+---------------------------+----------
|               Backup Instance                 |  Status  |  Size  | SFD Version |   Backup Job   |     Content      |              Location              | Backup Scheduled Time(UTC) | Backup Co
+-----------------------------------------------+----------+--------+-------------+----------------+------------------+------------------------------------+---------------------------+----------
| wednesdaybackup_cem_24-06-2020_18-55-09.tar | Completed | 226 MB |    1.1.1    | WednesdayBackup |  Configurations | ftp://10.196.207.12:21/sfdBackup |    2020-06-24 18:55:09    |   2020-0
|                                               |          |        |             |                | Events and Logs  |                                    |                           |
|                                               |          |        |             |                | Monitoring Data  |                                    |                           |
+-----------------------------------------------+----------+--------+-------------+----------------+------------------+------------------------------------+---------------------------+----------
```

Releases 2.0 or later

backup job delete

Selects one backup job then deletes the job.

Command `backup job delete`

Options None

Usage None

Example

```
sfd> backup job delete
+---+-----------------+---------+-----------------------------------+------------+-----------------+------------+----------------------+
| # |    Job Name     | Status |            Location               | Recurrence |     Content     | Created By |   Created At(UTC)    |
+---+-----------------+---------+-----------------------------------+------------+-----------------+------------+----------------------+
| 1 | WednesdayBackup | Expired | ftp://10.196.207.12:21/sfdBackup |   Never    |  Configurations |    root    | 2020-06-24 18:55:01 |
|   |                 |         |                                   |            | Events and Logs |            |                      |
|   |                 |         |                                   |            | Monitoring Data |            |                      |
+---+-----------------+---------+-----------------------------------+------------+-----------------+------------+----------------------+
Please enter backup job number: 1
Backup job configuration status: BACKUP_JOB_OPERATION_SUCCESS
Successfully delete backup job!
```

Releases 2.0 or later

backup job list

Lists all backup jobs.

Command `backup job list`

Options None

Usage None

Example

```
sfd> backup job list
+---+----------+--------+-----------------------------------+------------+-----------------+------------+----------------------+
| # | Job Name | Status |            Location               | Recurrence |     Content     | Created By |   Created At(UTC)    |
+---+----------+--------+-----------------------------------+------------+-----------------+------------+----------------------+
| 1 |   job2   | Active | ftp://10.196.207.12:21/sfdBackup |   Never    |  Configurations |    root    | 2020-06-24 19:00:50 |
|   |          |        |                                   |            | Events and Logs |            |                      |
|   |          |        |                                   |            | Monitoring Data |            |                      |
| 2 |   job1   | Active | ftp://10.196.207.12:21/sfdBackup |   Never    |  Configurations |    root    | 2020-06-24 19:00:30 |
|   |          |        |                                   |            | Events and Logs |            |                      |
|   |          |        |                                   |            | Monitoring Data |            |                      |
+---+----------+--------+-----------------------------------+------------+-----------------+------------+----------------------+
```

Releases 2.0 or later

backup job schedule

Schedules a one-time backup job.

Command `backup job schedule [-h] --name NAME [--time TIME] [--content {config,config_and_events,config_and_monitoring,all}] [--description DESCRIPTION]`

Options

- `--name` — Backup job name
- `--time[OPTIONAL]` — Backup time in UTC; current time by default
- `--content[OPTIONAL]` — Backup content; configuration data by default
- `-description[OPTIONAL]` — Backup location description

Usage None

Example

```
sfd> backup job schedule --name WednesdayBackup --content all --description test
+---+------------------+---------+------------------+----------+------------+---------------------+
| # | IP Address/FQDN  |  User   | Backup Directory | Protocol | Created By |   Created At(UTC)   |
+---+------------------+---------+------------------+----------+------------+---------------------+
| 1 | 10.196.207.12:21 | ftpuser |    /sfdBackup    |   FTP    |    root    | 2020-06-24 18:51:23 |
+---+------------------+---------+------------------+----------+------------+---------------------+
Please enter number of backup location that you want to store backup data: 1
Backup job scheduling status: BACKUP_JOB_OPERATION_SUCCESS
```

Releases 2.0 or later

backup location add

Adds a backup location.

Command `backup location add [-h] --host HOST [--port PORT] --user USER --password PWD --backupdir PATH --protocol {ftp,sftp} [--description DESCRIPTION]`

Options

- `--host` — Host of backup location such as 10.196.207.12
- `--port[OPTIONAL]` — Port of host
- `--user` — Username of remote backup server
- `--password` — Password of remote backup server
- `--backupdir` — Backup directory to store backup file such as */sfdBackup*
- `--protocol` — ftp or sftp server
- `--description[OPTIONAL]` — Backup location description

Usage None

Example

```
sfd> backup location add --host 10.196.207.12 --port 21 --user ftpuser --password vmware --backupdir sfdBackup --protocol ftp
Backup location configuration status: BACKUP_LOCATION_OPERATION_SUCCESS
```

Releases 2.0 or later

backup location delete

Selects a backup location then deletes the location.

Command `backup location delete`

Options None

Usage A backup location cannot be deleted if it is currently used by a backup job.

Example

```
sfd> backup location delete
+---+------------------+---------+------------------+----------+------------+---------------------+
| # | IP Address/FQDN  |  User   | Backup Directory | Protocol | Created By |   Created At(UTC)   |
+---+------------------+---------+------------------+----------+------------+---------------------+
| 1 | 10.196.207.12:21 | ftpuser |    /sfdBackup    |   FTP    |    root    | 2020-06-24 18:47:18 |
+---+------------------+---------+------------------+----------+------------+---------------------+
Please enter backup location number: 1
Backup location configuration status: BACKUP_LOCATION_OPERATION_SUCCESS
Successfully delete backup location!
```

Releases 2.0 or later

backup location list

Lists all backup locations.

Command `backup location list`

Options None

Usage None

Example

```
sfd> backup location list
+---+------------------+---------+------------------+----------+------------+---------------------+
| # | IP Address/FQDN  |  User   | Backup Directory | Protocol | Created By |   Created At(UTC)   |
+---+------------------+---------+------------------+----------+------------+---------------------+
| 1 | 10.196.207.12:21 | ftpuser |    /sfdBackup    |   FTP    |    root    | 2020-06-24 18:47:18 |
+---+------------------+---------+------------------+----------+------------+---------------------+
```

Releases 2.0 or later

backup restore initiate

Restores SFD to the state saved in the specified backup .tar bundle.

Command `backup restore initiate [-h] --filepath <BACKUP_TAR_PATH> --username <USER> --passw <PWD>`

Options

- `-filepath` — URL of the backup file on a remote FTP/SFTP server such as `ftp://10.0.0.1:21/sfdbac file.tar`
- `--username` — Username to the remote backup server
- `--password` — Password to the remote backup server

Usage None

Example

```
sfd> backup restore initiate --filepath ftp://10.196.207.12/public/fittest/backupjobforfittest_ce_23-06-2020_16-29-17.tar --username
--password vmware
Retrieving backup file info
Retrieved Backup File Attributes
+------------------------+----------------------------------------------+
| Name                   |                                        Value |
+------------------------+----------------------------------------------+
| File Name              | backupjobforfittest_ce_23-06-2020_16-29-17.tar |
| File Size              |                                          7 MB |
| File Modified Timestamp |                          2020-06-23 16:29:00 |
+------------------------+----------------------------------------------+
Initiate restore request
Initiate restore status: RESTORE_INITIATED
Current restore state: DOWNLOAD_BACKUP_FILE_IN_PROGRESS
Current restore state: VALIDATE_BACKUP_FILE_SUCCESS
Backup File Metadata
+---------------+-----------------+
| Name          |           Value |
+---------------+-----------------+
| File Size     |            7 MB |
| SFD Version   | 1.1.1.1234567890 |
| Content Types |   Configurations |
|               |  Events and Logs |
+---------------+-----------------+
SFD Restore is going to start in 30 seconds. SFD UI session will shutdown during restore.
. . . .
. . . .
2020-06-23 17:11:35,698 [INFO ][main:init_restore] - --------------restore success!----------------
2020-06-23 17:11:35,698 [INFO ][main:init_restore] - SFD UI is up and ready to use
```

Releases 2.0 or later

backup restore result

Displays details of the last restore result.

Command `backup restore result`

Options None

Usage None

Example

```
sfd> backup restore result
Restore Result Info
+------------------------+---------------------+
| Name                   |               Value |
+------------------------+---------------------+
| Restore Start Time     | 2020-06-23 17:05:34 |
| Restored Contents      |      Configurations |
|                        |     Events and Logs |
| Restored Version       |    1.1.1.1234567890 |
| Restore Completed Time | 2020-06-23 17:06:54 |
+------------------------+---------------------+
```

Releases	2.0 or later

10

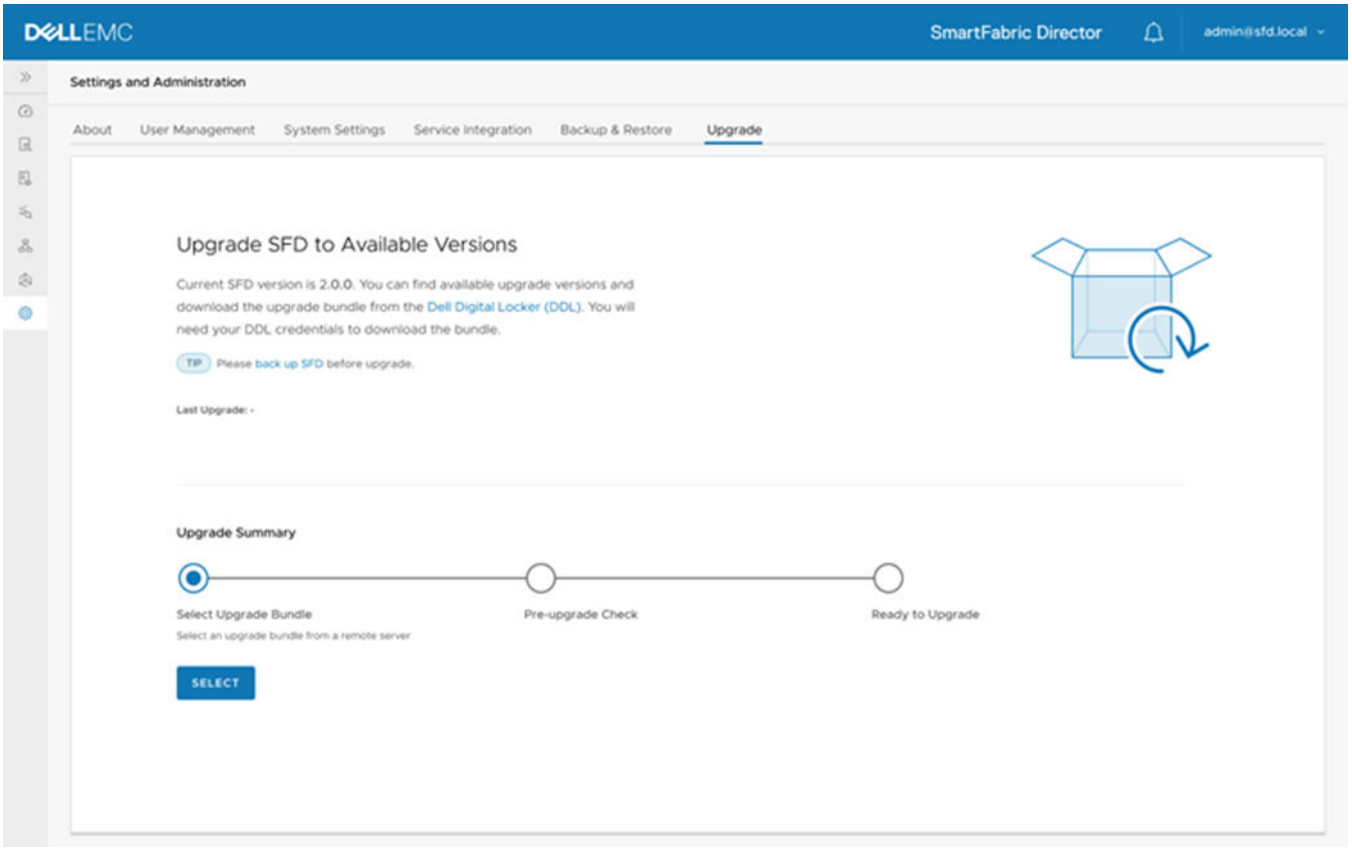
Upgrade SFD

Prior to upgrading SFD, see Download SFD image to download the upgrade bundle from DDL to a server which is reachable from SFD. You can use either the user interface or the CLI to upgrade SFD (see Upgrade CLIs).

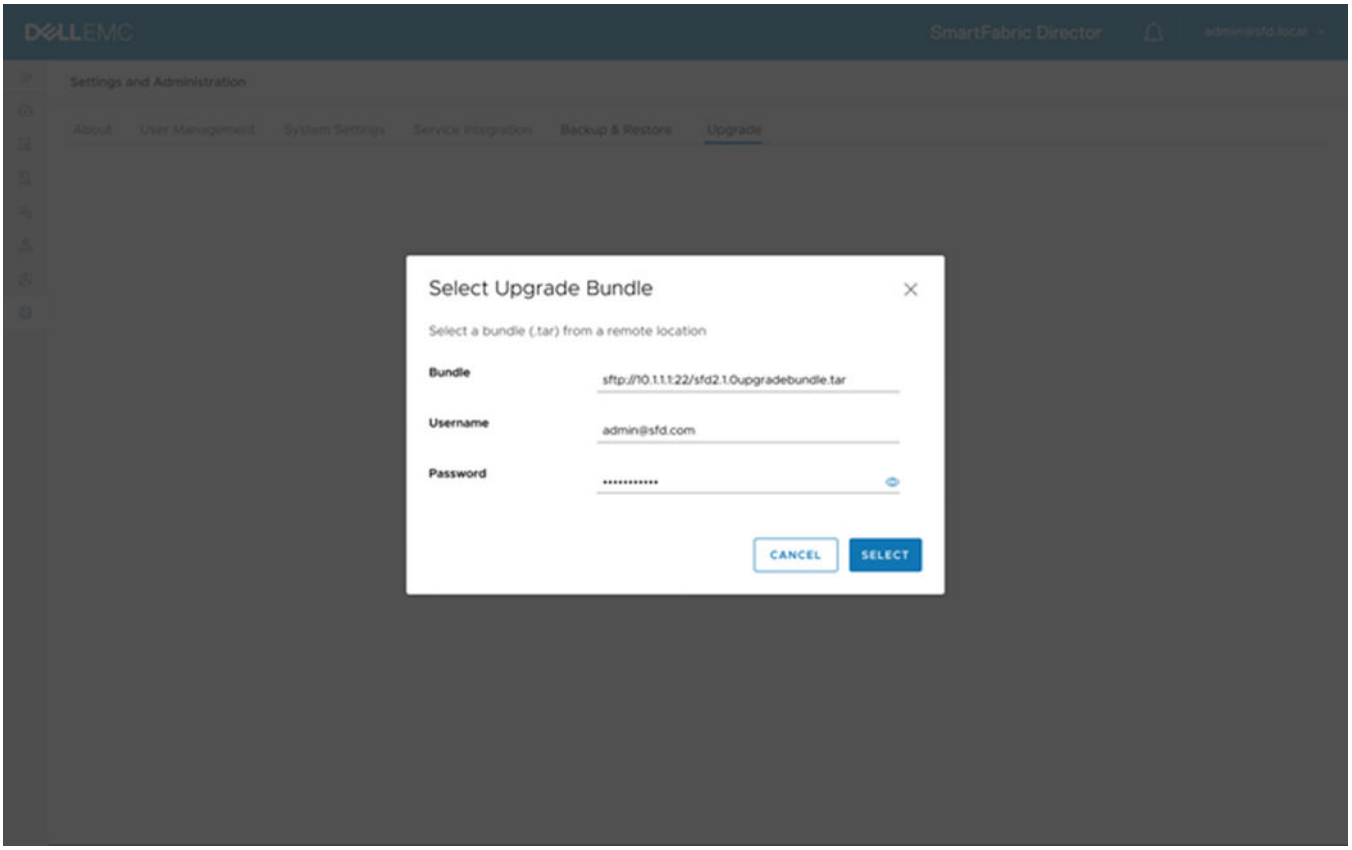
NOTE: It is recommended that you backup the current SFD before starting an upgrade. Verify that there are no pending tasks in progress, such as backup. If you do have pending tasks, complete those tasks before starting an upgrade.

SFD upgrade

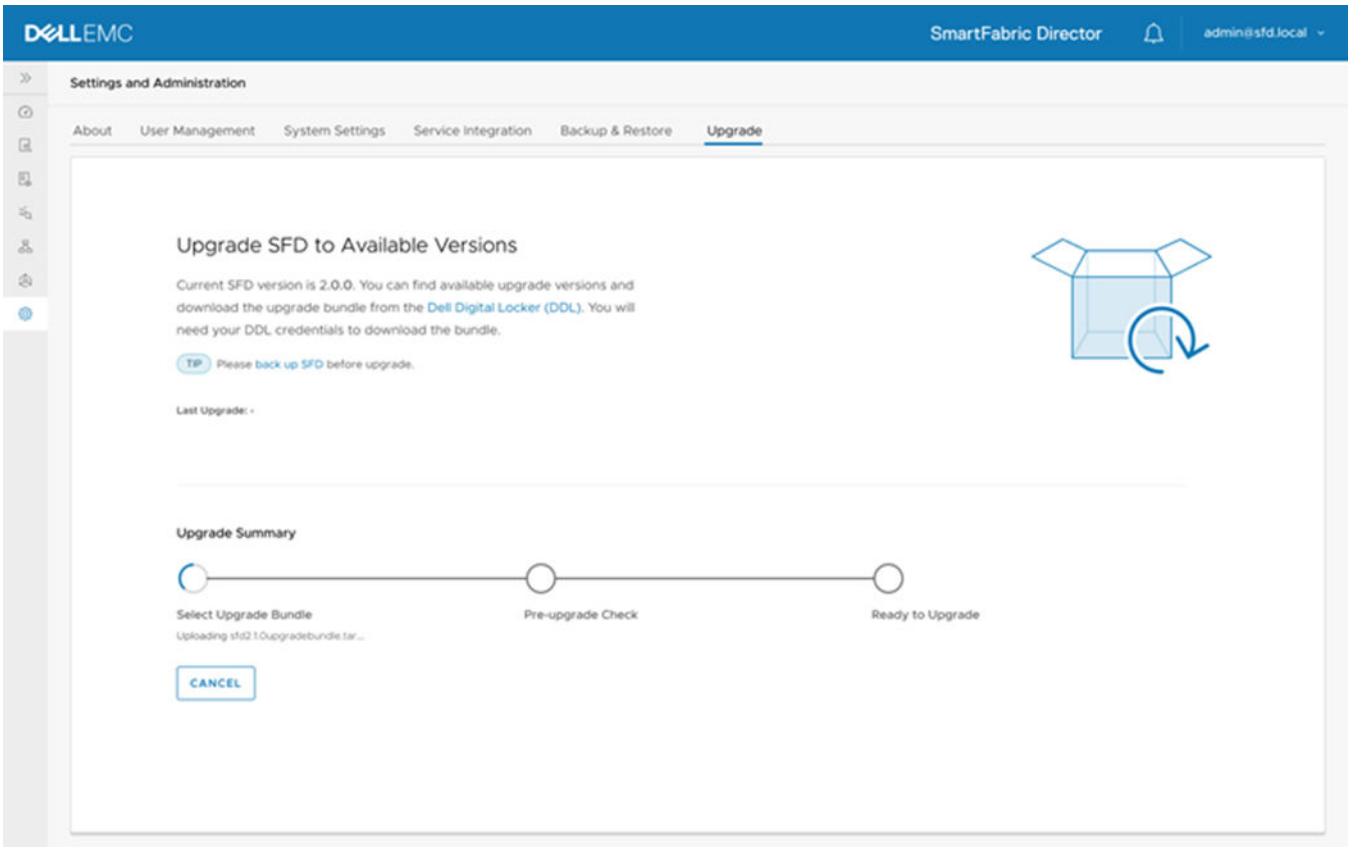
1. Go to **Settings and Administration > Upgrade**, then click **Select**.



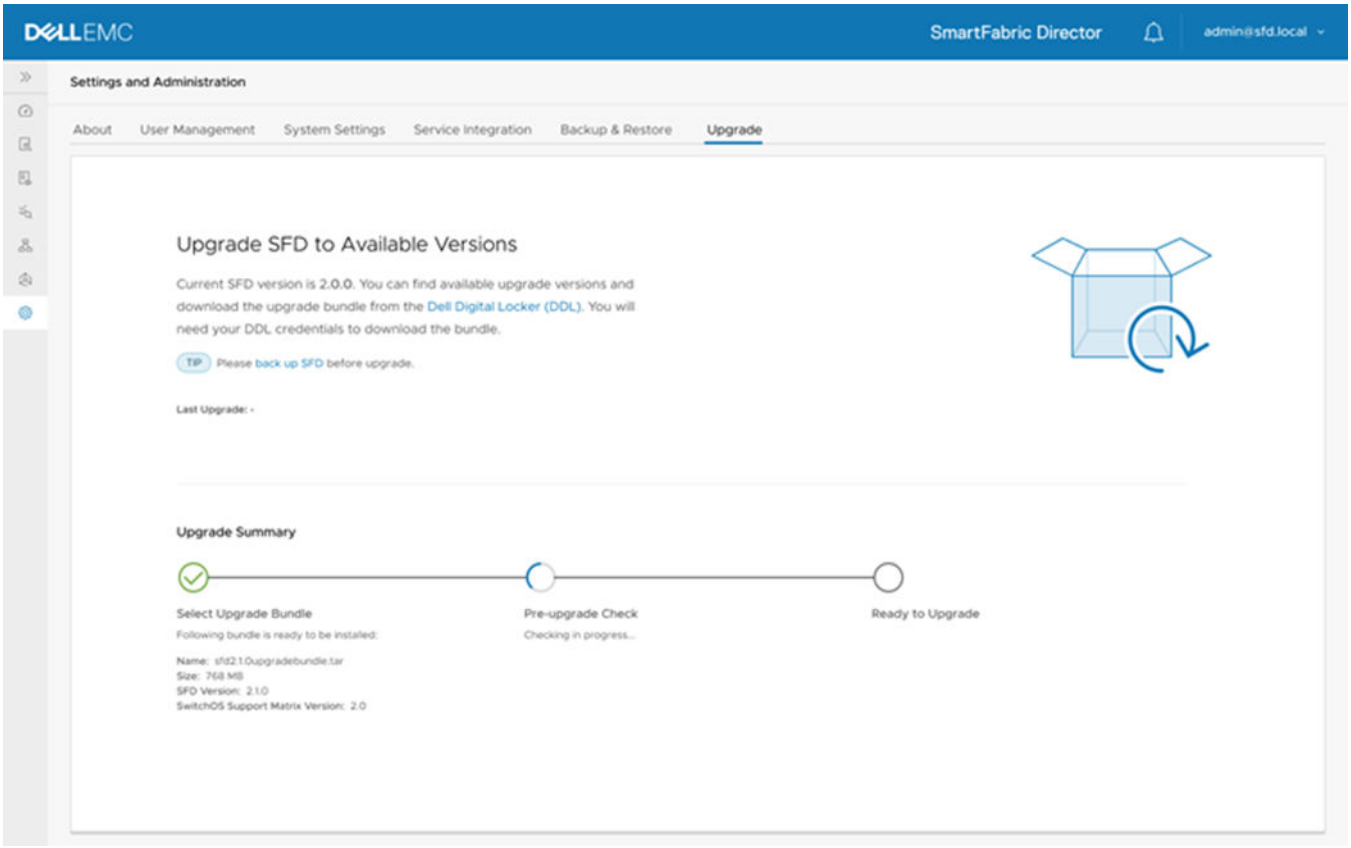
2. Enter the upgrade bundle filename including server IP address, server credentials for SFD to access the upgrade bundle, then click **Select**.



SFD supports FTP and Secure File Transfer Protocol to download the upgrade bundle. The upgrade bundle progress displays. Click **Cancel** to cancel the download and exit the upgrade process.



Once the upgrade bundle has downloaded, upgrade bundle information displays. SFD then performs the preupgrade check while the progress displays.



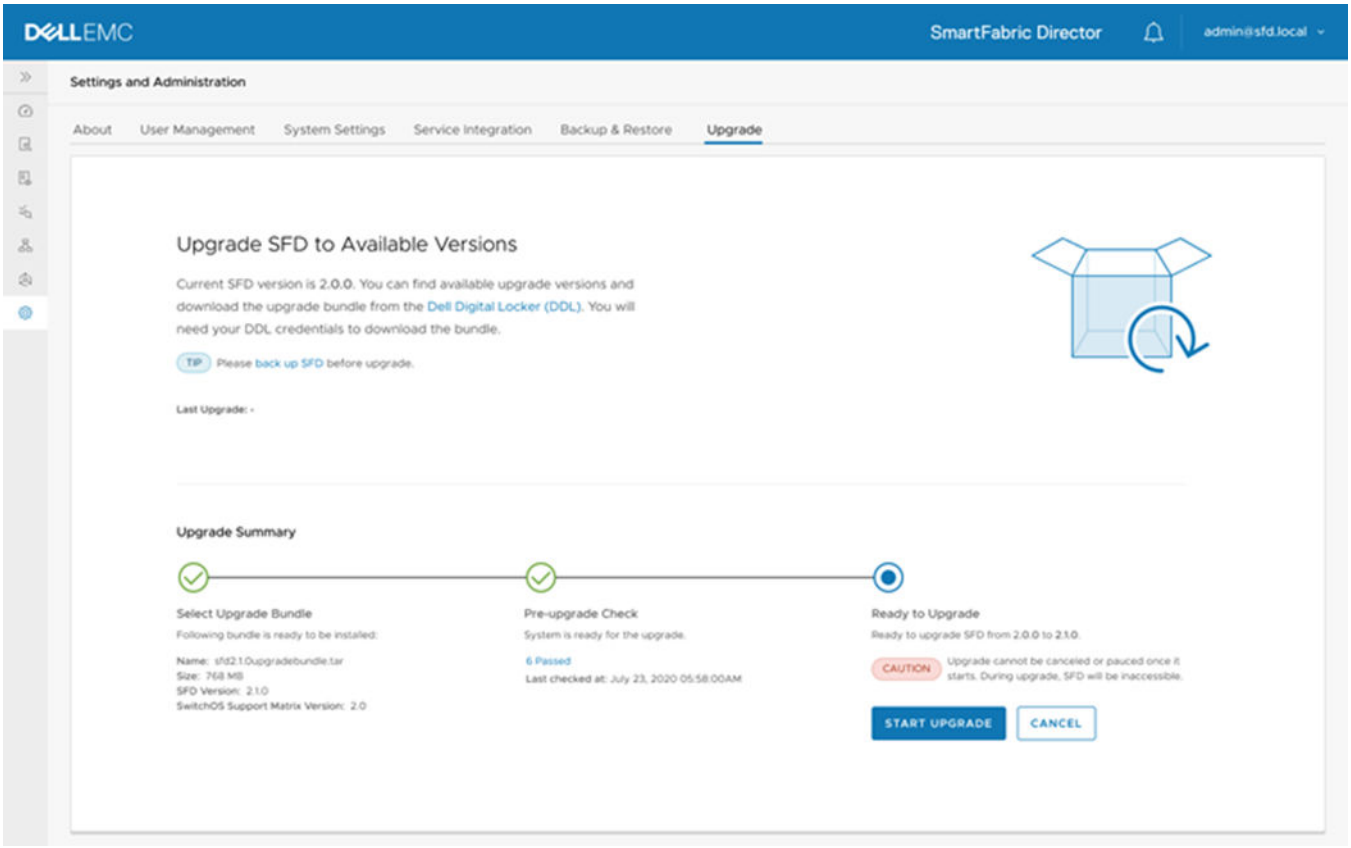
The preupgrade check includes verifying that the server hosting SFD has the required number of CPUs, memory, and disk space. The SFD upgrade matrix check verifies that SFD can migrate data from the current SFD version to the upgraded version.

Each SFD bundle comes with a manifest file that checks if the switches are running supported models and operating system versions. This check verifies against using older switch model or operating system versions which are not supported. SFD also checks system health to ensure that all services are operational.

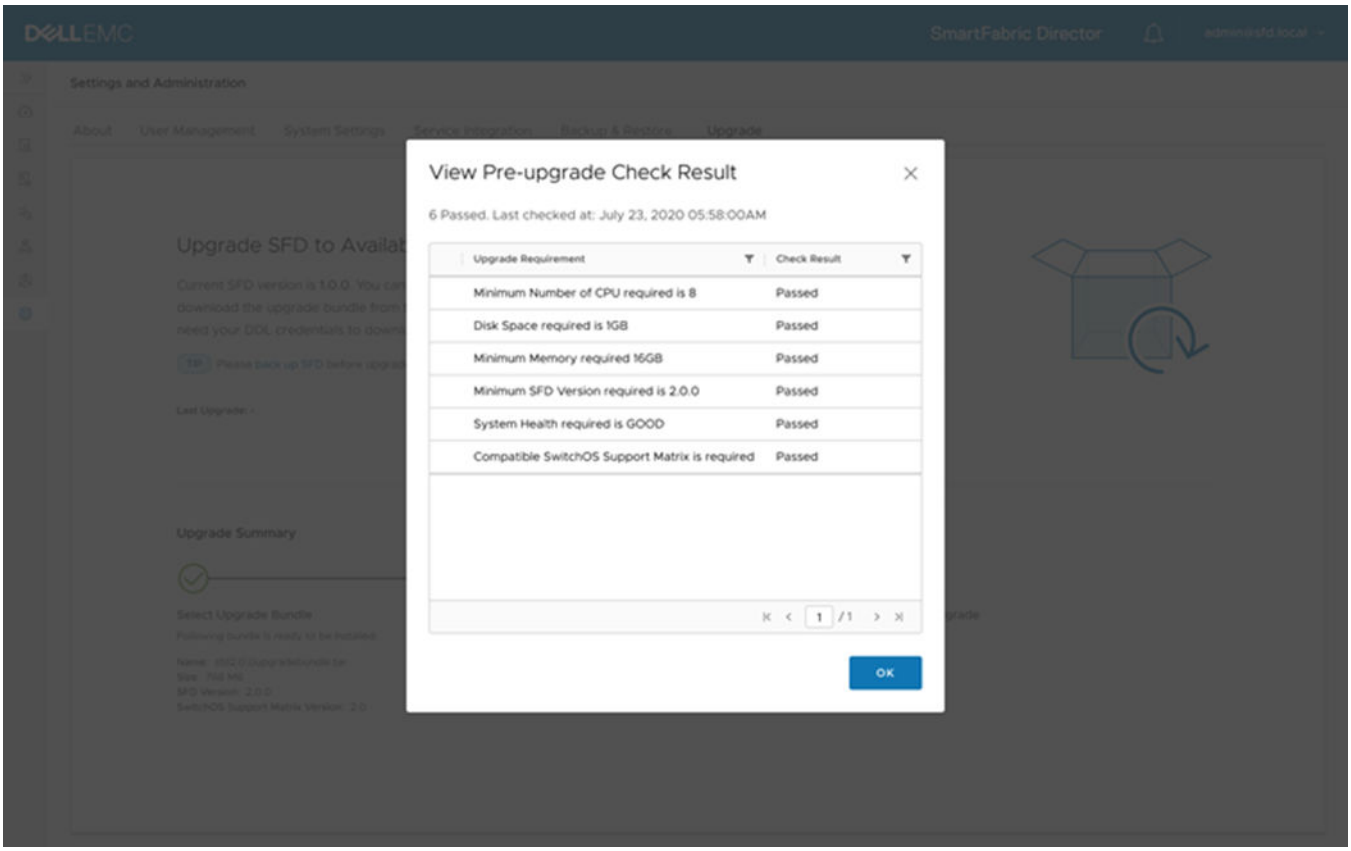
If there are any failures, the upgrade will not be allowed. You can then take corrective actions to retry the preupgrade checks.

NOTE: An upgrade from SFD 1.2.0 to 2.0.0 is allowed, but an upgrade from SFD 1.1.0 to 2.0.0 is not allowed.

3. Click **Start upgrade**.

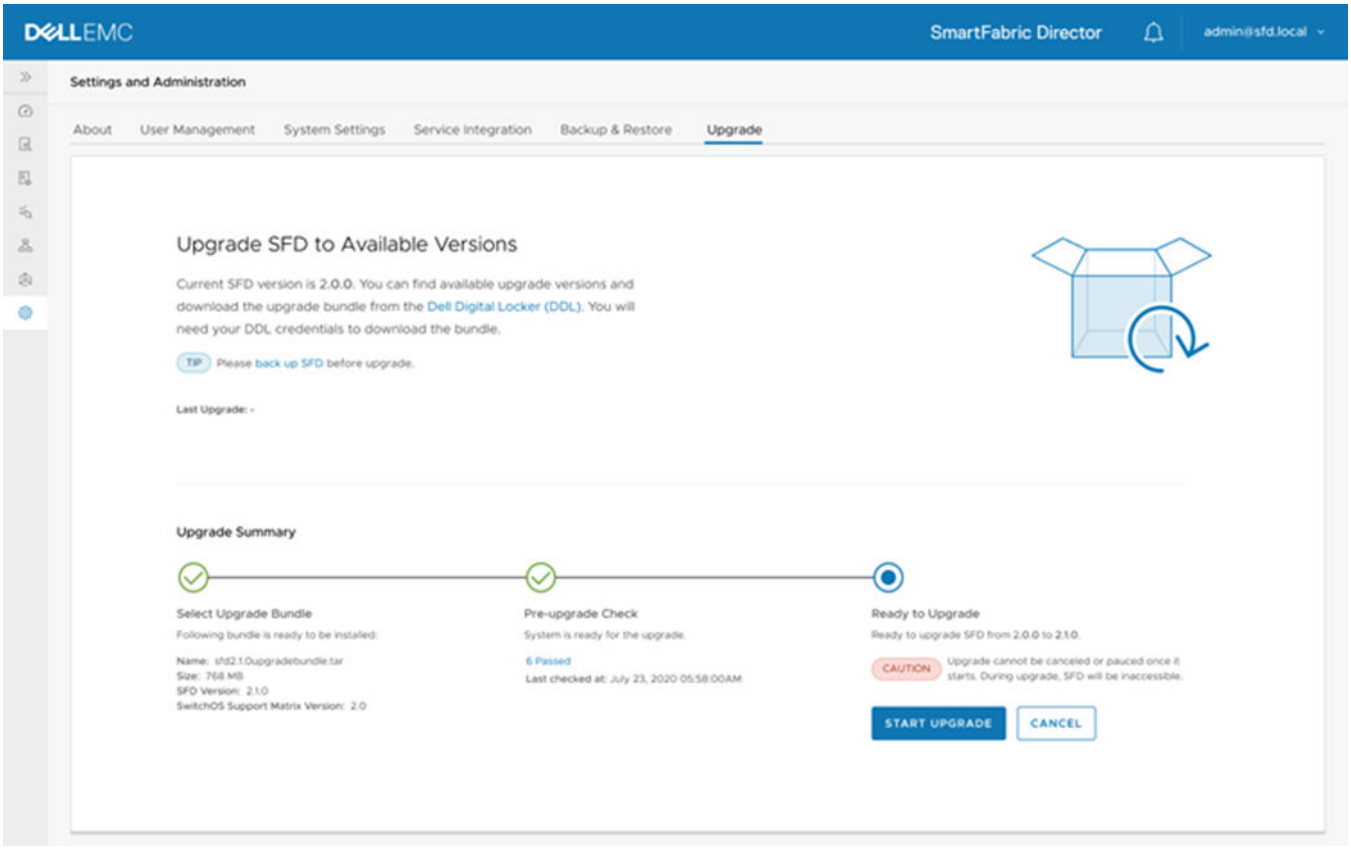


4. Click **OK** or close the window to cancel the upgrade.

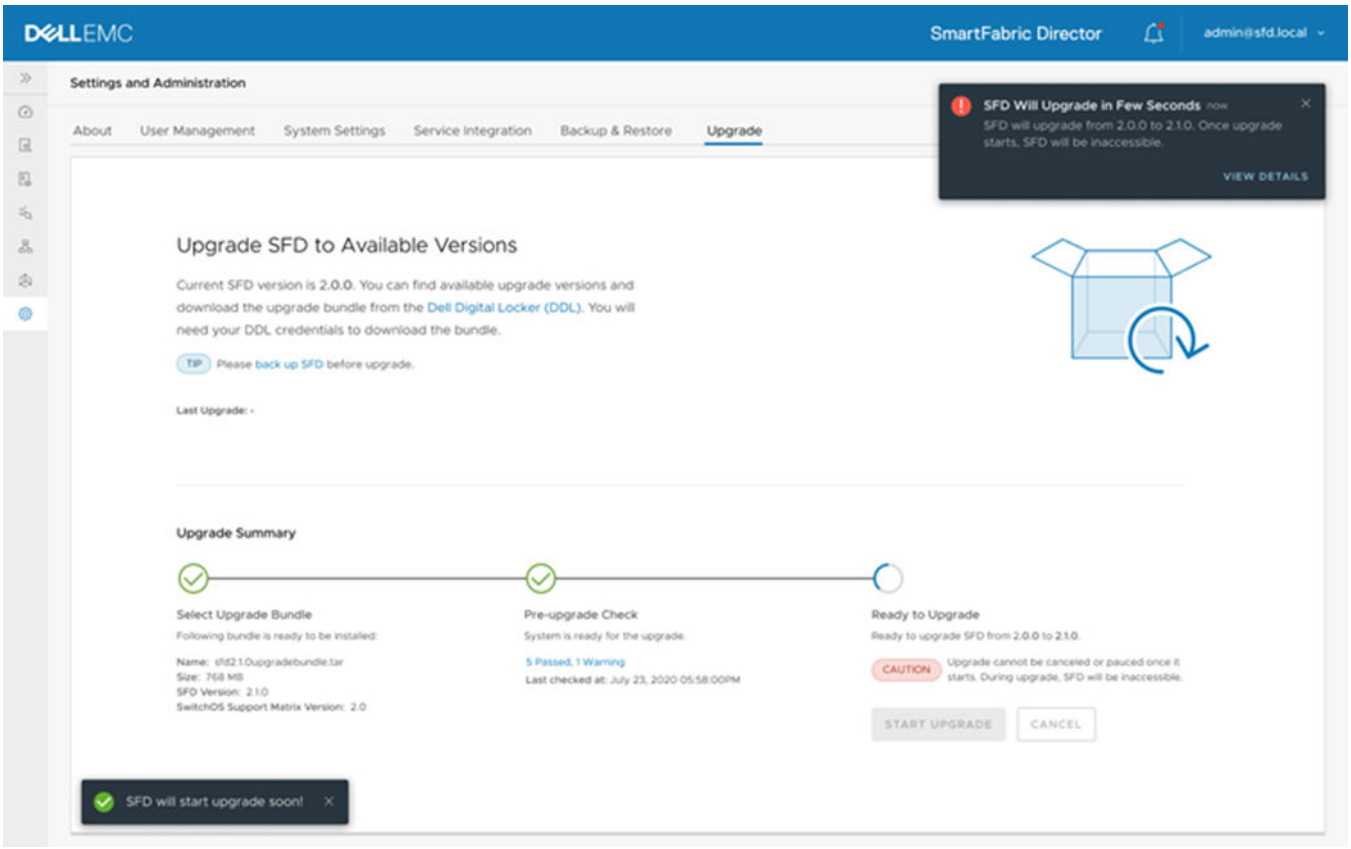


NOTE: Once the upgrade is initiated, SFD will not allow changes to the fabric including configuration or intent changes. Multiple upgrades should not be initiated simultaneously.

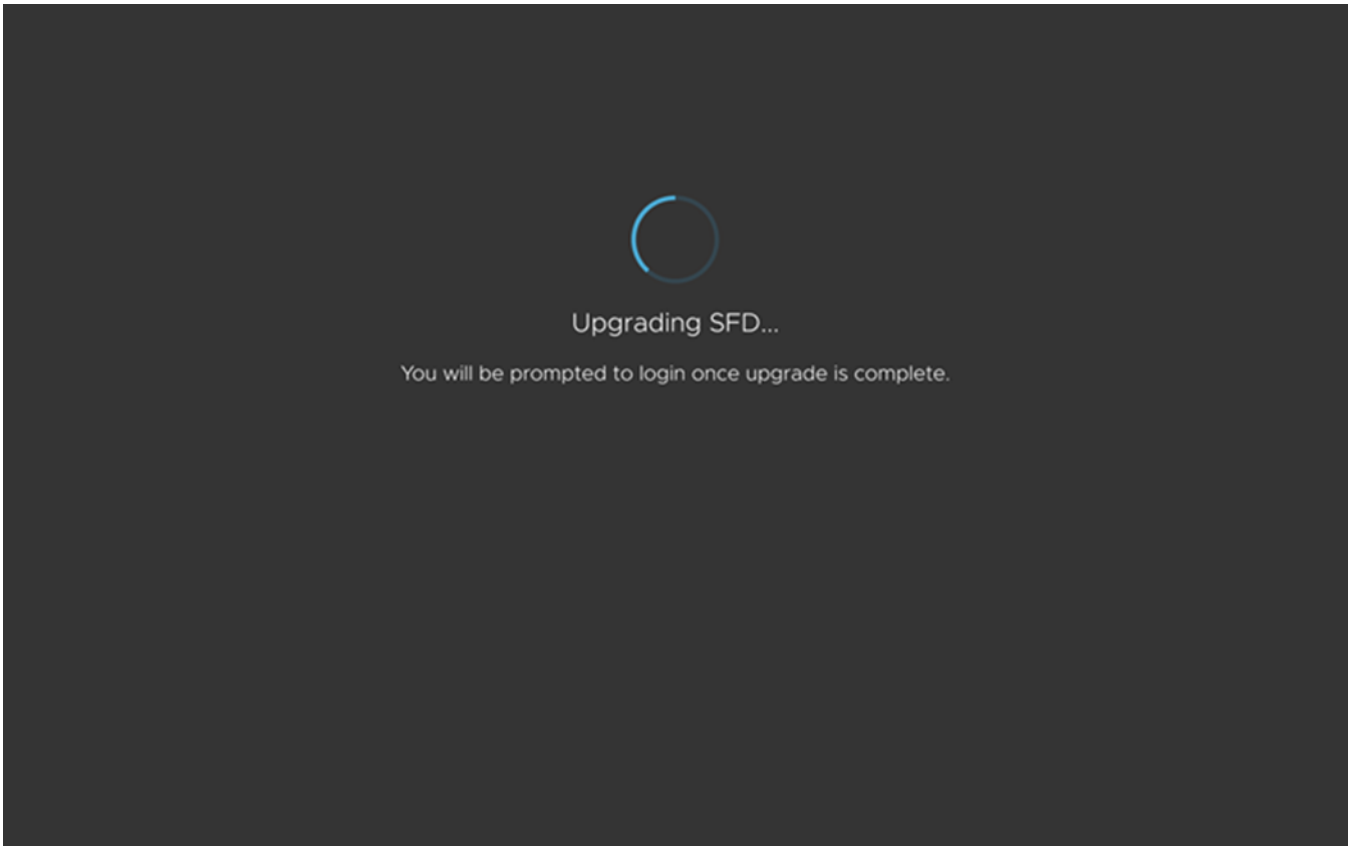
5. Click **Start upgrade** to begin the upgrade process.



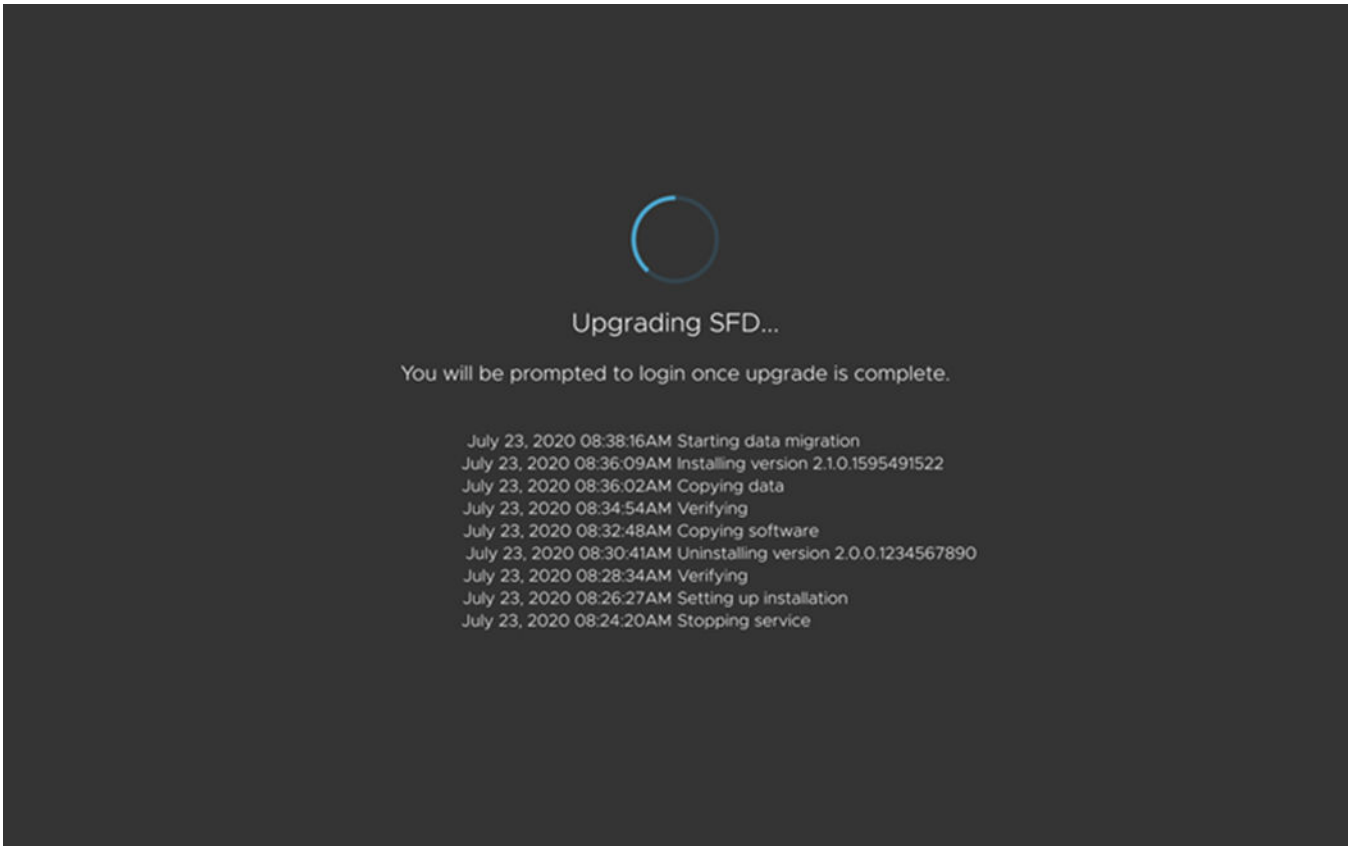
Once the upgrade process starts, the SFD will not be available for operations. Click **Cancel** to cancel the upgrade.



Once the upgrade starts, the progress is shown.

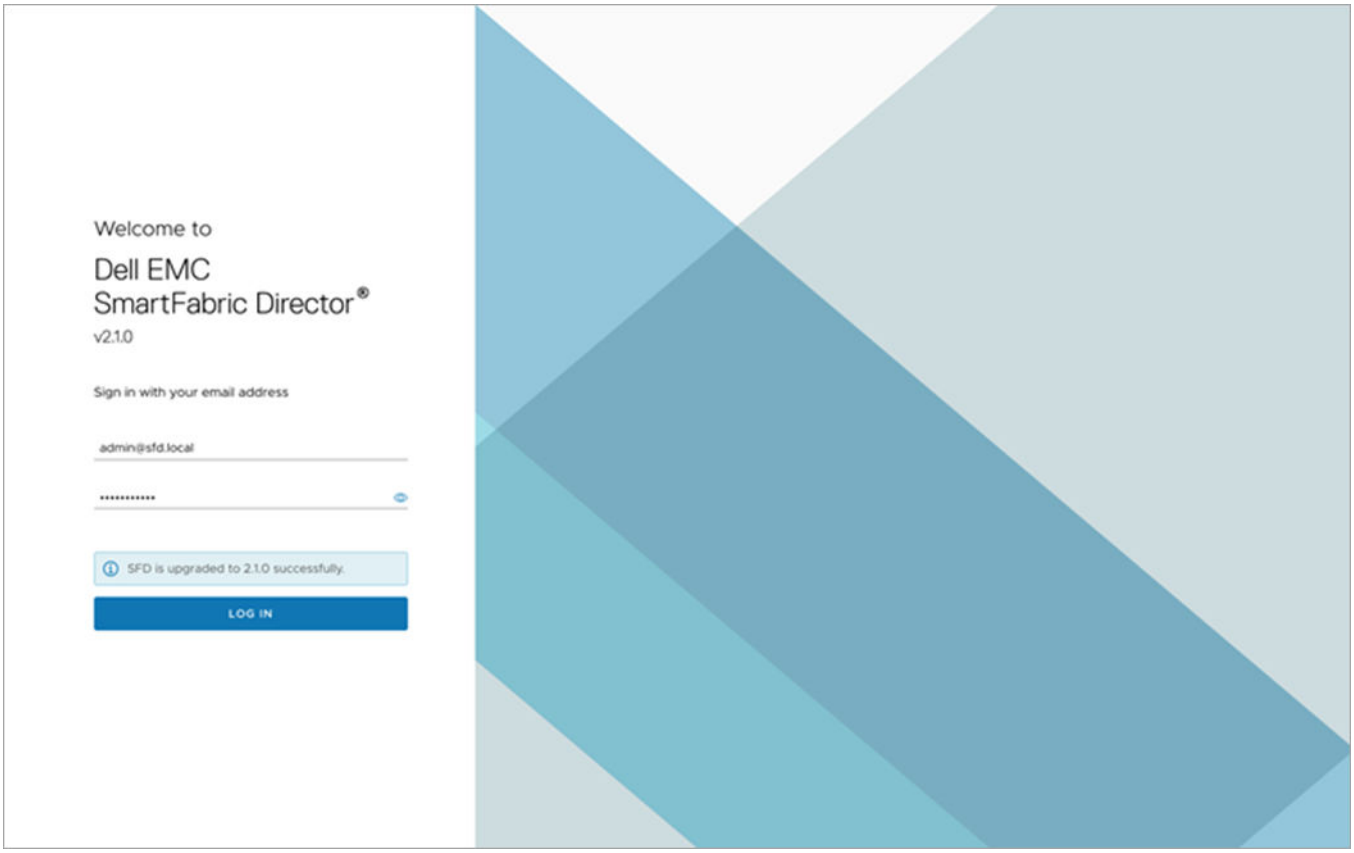


Updates display as the upgrade process progresses.



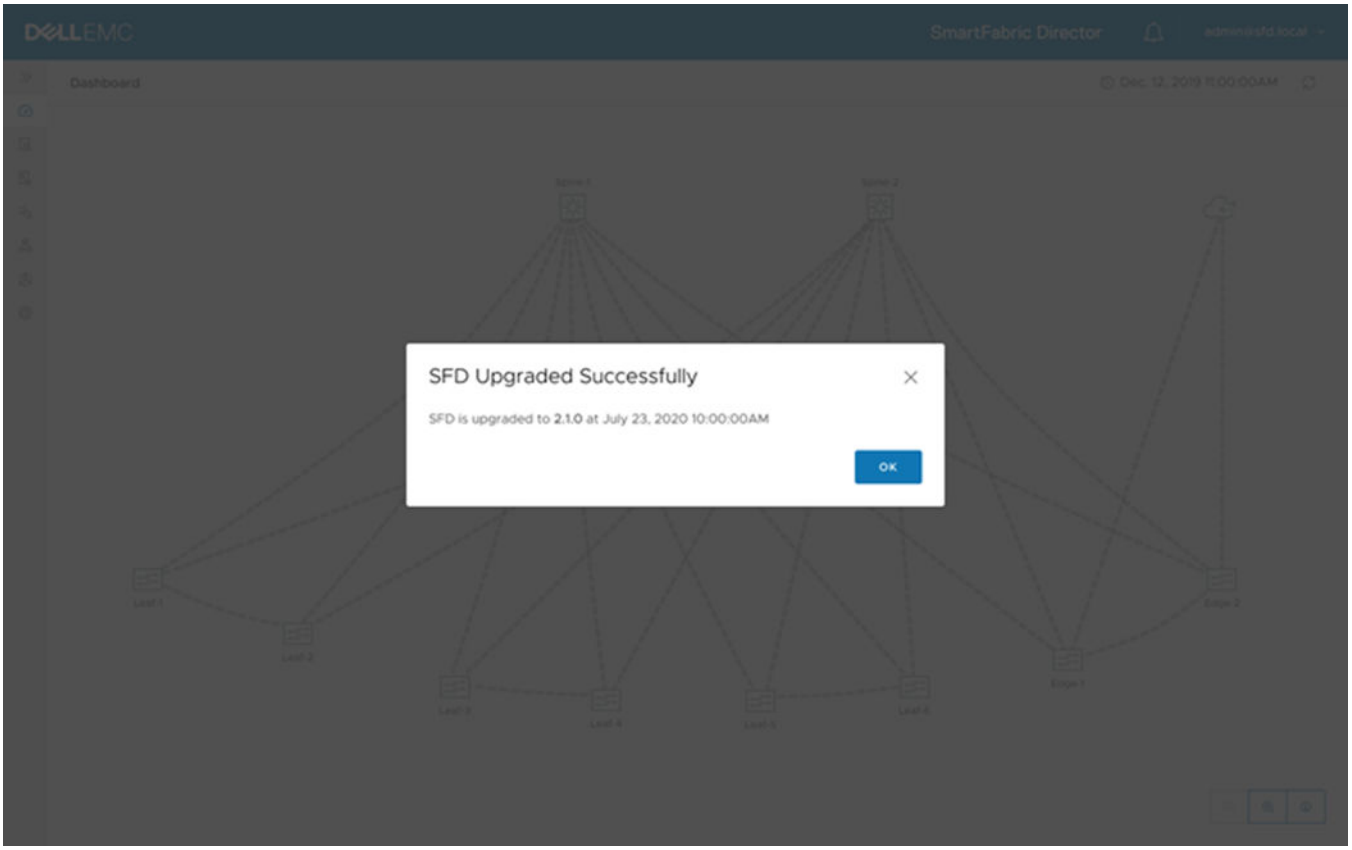
The current SFD version stops the services, uninstalls the current version, installs the new version, verifies the installation, copies the data, starts the new version, and starts the data migration. Once the data is migrated successfully, the SFD upgrade is complete, and SFD is ready for login.

6. Log in to the new version of SFD with your user credentials, then click **Log in**. A message displays showing that the SFD upgrade has been successful.



NOTE: The upgrade success message is only shown on the first new login to the upgraded SFD instance.

7. Click **OK** or close the window to go to the SFD dashboard.

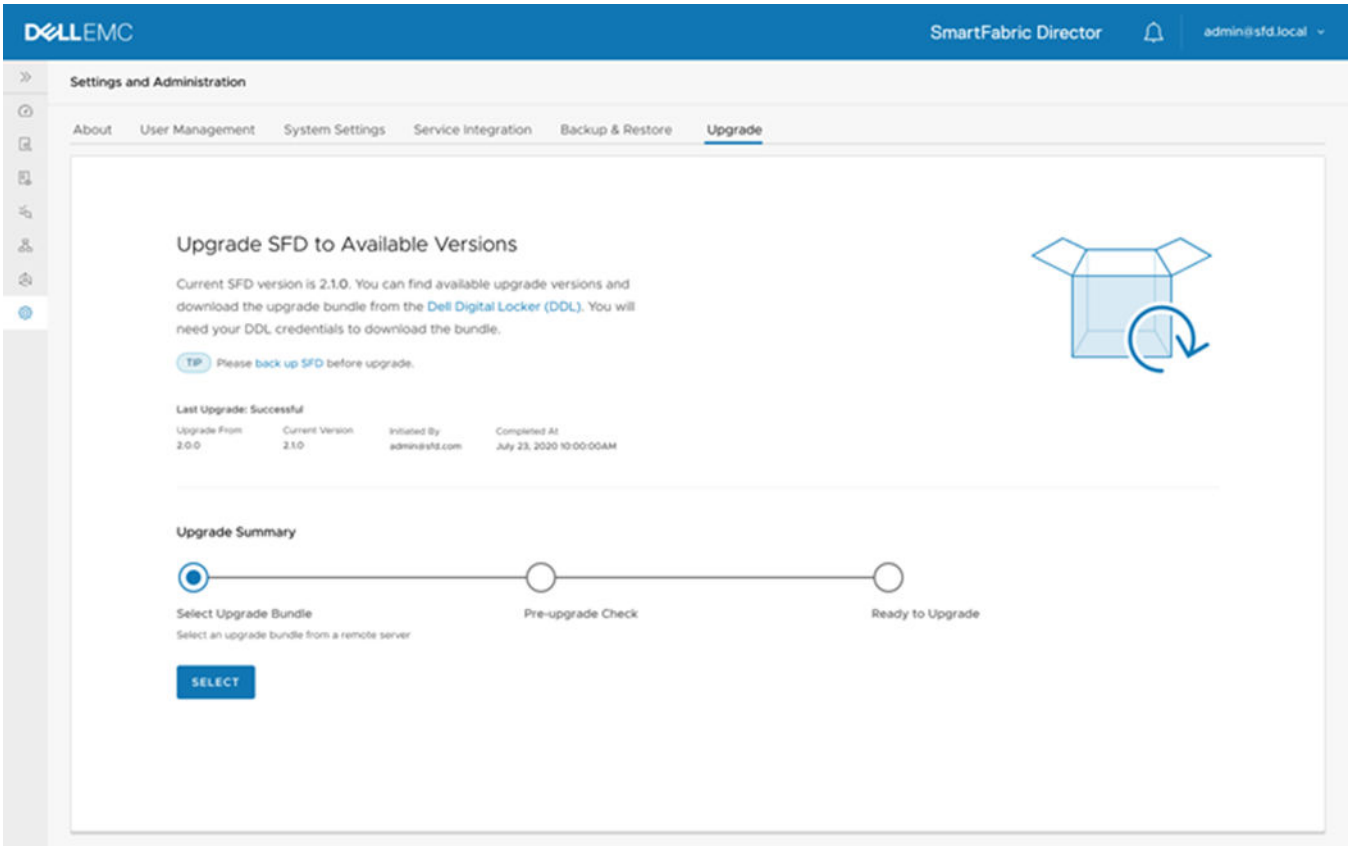


SFD reestablishes gNMI sessions with the switches and starts the discovery process. The dashboard updates accordingly. During the brief time that SFD is being upgraded, any telemetry streamed by or syslogs that are sent by switches will not be recorded by SFD.

If a switch rebooted during the time SFD is being upgraded and is operational before the SFD upgrade is complete, SFD cannot detect the reboot of the switch and configuration replay will not happen. The switch may not have the configuration based on the fabric intent.

NOTE: We recommend that the operator verify the fabric for correct operation after an SFD upgrade.

The upgrade page shows the last successful upgrade summary.



Topics:

- Upgrade CLIs

Upgrade CLIs

Use these commands to upgrade SFD using the command-line interface (CLI).

upgrade info

Displays the latest upgrade information and status.

Command	`upgrade info`
Options	None
Usage	None

Example

```
sfd> upgrade info
Upgrade Result
+-------------------------------------------------------------+
|                       Upgrade Result                        |
+----------------------+--------------------------------------+
| Name                 |                                Value |
+----------------------+--------------------------------------+
| Upgrade File Name    |              2.1.0.1598423656.tar    |
| Upgrade File Size    |                             1516 MB  |
| Upgrade From Version |                               2.0.0  |
| Upgrade To Version   |                               2.1.0  |
| Upgrade Status       |                 PRE_CHECK_SUCCESS    |
| Pre Check At (UTC)   |               2020-08-26 11:26:05    |
+----------------------+--------------------------------------+
Pre-check report
+-------------------------------------------------------+
|                    Pre-check report                   |
+-------------------------------+--------------+--------+
| Upgrade Requirement           | Check Result | Message |
+-------------------------------+--------------+--------+
| Minimum number of CPU         | PASSED       |         |
| required 4                    |              |         |
| Minimum free disk space       | PASSED       |         |
| required 1GB                  |              |         |
| Minimum memory required 8GB   | PASSED       |         |
| Minimum SFD version required  | PASSED       |         |
| [1.1.1.123456789]             |              |         |
| System Health required GOOD   | PASSED       |         |
| Compatible SwitchOS Support   | PASSED       |         |
| Matrix is required            |              |         |
+-------------------------------+--------------+--------+
```

Releases 2.0 or later

upgrade initiate

Starts an upgrade.

Command `upgrade initiate`

Options None

Usage None

Example

```
sfd> upgrade initiate
```

Releases 2.0 or later

upgrade upload local

Uploads a local upgrade bundle.

Command `upgrade upload local --path FILEPATH`

Options None

Usage To test an upgrade bundle, place one upgrade .tar inside a VM.

Example

```
sfd> upgrade upload local --filepath /home/admin@sfd.local/2.1.0.1598423656.tar
Pre processing upgrade bundle status: SUCCESS
Status: FILE_VALIDATION_IN_PROGRESS
Status: FILE_VALIDATION_IN_PROGRESS
Status: PRE_CHECK_IN_PROGRESS
Status: PRE_CHECK_IN_PROGRESS
Status: PRE_CHECK_IN_PROGRESS
Status: PRE_CHECK_IN_PROGRESS
Status: PRE_CHECK_IN_PROGRESS
Status: PRE_CHECK_IN_PROGRESS
Status: PRE_CHECK_IN_PROGRESS
Status: PRE_CHECK_SUCCESS
Upgrade Result
+-----------------------------------------------------------+
|                      Upgrade Result                       |
+----------------------+------------------------------------+
| Name                 |                              Value |
+----------------------+------------------------------------+
| Upgrade File Name    |             2.1.0.1598423656.tar  |
| Upgrade File Size    |                           1516 MB  |
| Upgrade From Version |                             2.0.0  |
| Upgrade To Version   |                             2.1.0  |
| Upgrade Status       |                 PRE_CHECK_SUCCESS  |
| Pre Check At (UTC)   |               2020-08-26 11:26:05  |
+----------------------+------------------------------------+
Pre-check report
+-------------------------------------------------------+
|                    Pre-check report                   |
+-----------------------------+--------------+----------+
| Upgrade Requirement         | Check Result | Message  |
+-----------------------------+--------------+----------+
| Minimum number of CPU       | PASSED       |          |
| required 4                  |              |          |
| Minimum free disk space     | PASSED       |          |
| required 1GB                |              |          |
| Minimum memory required 8GB | PASSED       |          |
| Minimum SFD version required| PASSED       |          |
| [1.1.1.123456789]           |              |          |
| System Health required GOOD | PASSED       |          |
| Compatible SwitchOS Support | PASSED       |          |
| Matrix is required          |              |          |
+-----------------------------+--------------+----------+
```

Releases 2.0 or later

upgrade upload remote

Uploads a remote upgrade bundle.

Command `upgrade upload remote --filepath PATH --username USER --password PWD`

Options

- `--filepath` — URL of the backup file on a remote FTP/sFTP server such as `ftp://10.0.0.1:21/2.0.0.1234567890.tar`
- `--username` — Username of the remote server
- `--password` — Password of the remote server

Usage The file path must end with a file name, and not a directory.

Example

```
sfd> upgrade upload remote --filepath ftp://10.196.207.12:21/2.0.0.1234567890.tar --username ftpuser --password vmware
Pre processing upgrade bundle status: SUCCESS
Current status state: FILE_DOWNLOADING
Current status state: FILE_DOWNLOADING
Current status state: FILE_DOWNLOADING
Current status state: FILE_DOWNLOADING
Current status state: PRE_CHECK_IN_PROGRESS
Current status state: PRE_CHECK_FAILED
Error message: UNTAR_UPGRADE_FILE_FAILED
Error: Pre check upgrade bundle failed
Upgrade Result
+----------------------+-----------------------------------+
| Name                 |                             Value |
+----------------------+-----------------------------------+
| Upgrade File Name    | 1594161748765_2.0.0.1234567890.tar |
| Upgrade File Size    |                          1381 MB |
| Upgrade From Version |                            1.1.1 |
| Upgrade To Version   |                            2.0.0 |
| Upgrade Status       |                 PRE_CHECK_FAILED |
+----------------------+-----------------------------------+
```

Releases 2.0 or later

11

Switch lifecycle management

This information explains switch lifecycle management. Each switch in the data center fabric must have the same software image. You can upgrade or downgrade the switch image software using SmartFabric Director. To ensure that unsupported models and images are not deployed in the fabric, a new feature called SwitchOS support matrix has been introduced.

Provide a file server (SFTP, FTP, SCP, TFTP, or HTTP) that is accessible through the Management port of switches, and reachable from SmartFabric Director. Download one or more relevant switch software images and manifest file to these servers.

Topics:

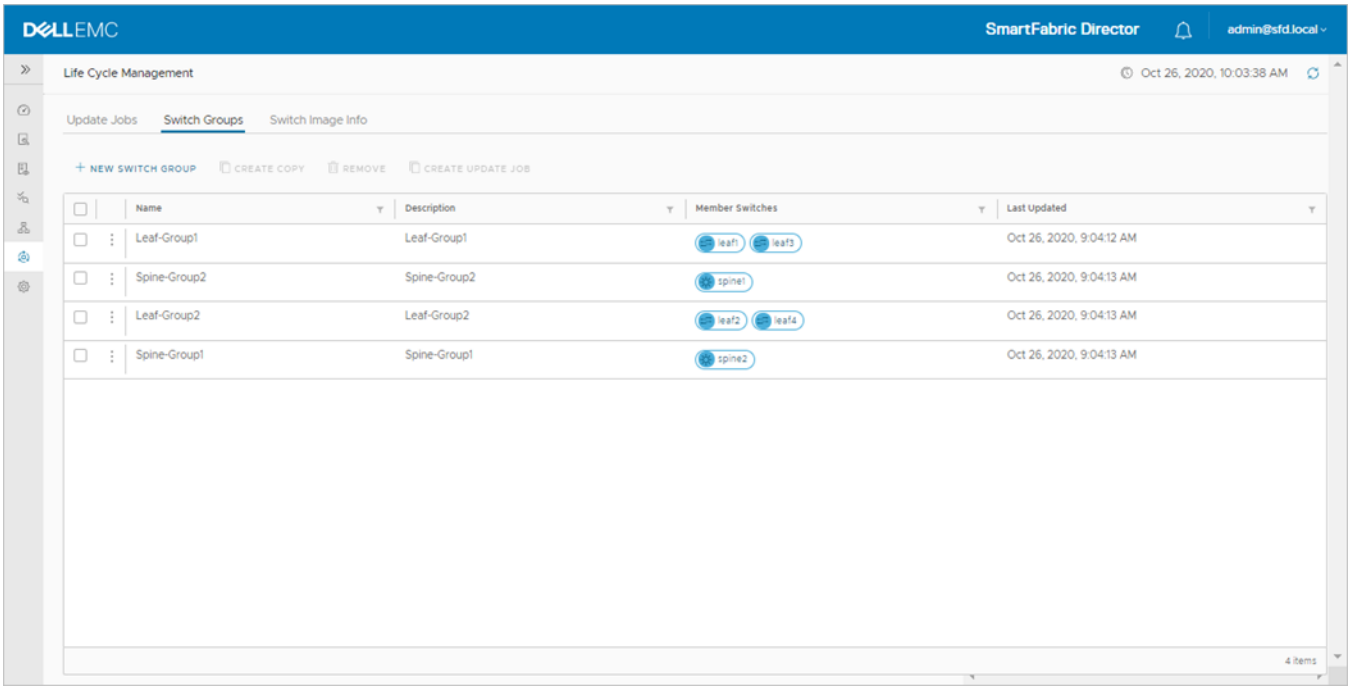
Define switch groups

This information describes how to create, edit, and delete switch groups to define an update job. To update a switch image, you must define an update switch lifecycle management job.

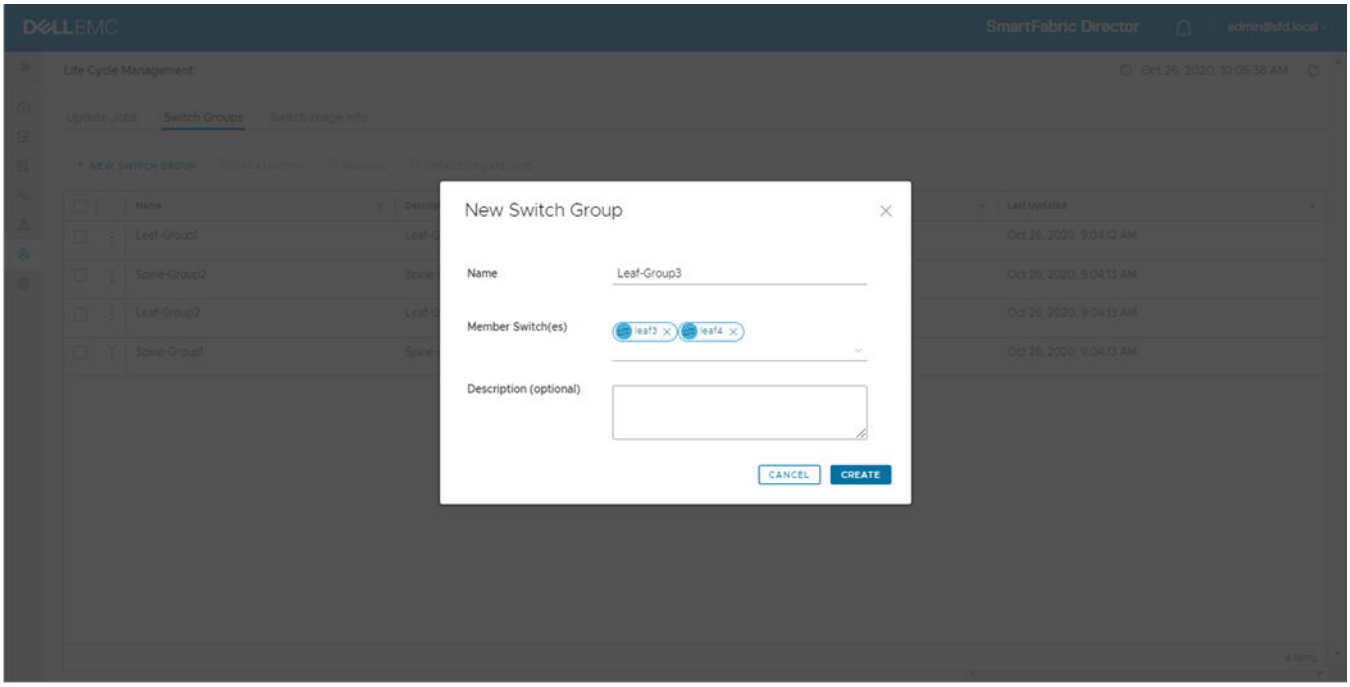
You can group switches into a switch group — SFD creates four default switch groups which are autopopulated based on the active fabric wiring diagram.

NOTE: Default switch groups cannot be edited or deleted. These switch groups are automatically created to enable users to upgrade all switches in the predefined switch groups without severely impacting availability of the fabric.

1. Select **Life Cycle Management > Switch Groups > New Switch Group** to define a new switch group.



2. Enter the name for the new switch group, select the switches to add to the switch group from the active wiring diagram, enter an optional description, then click **Create**.

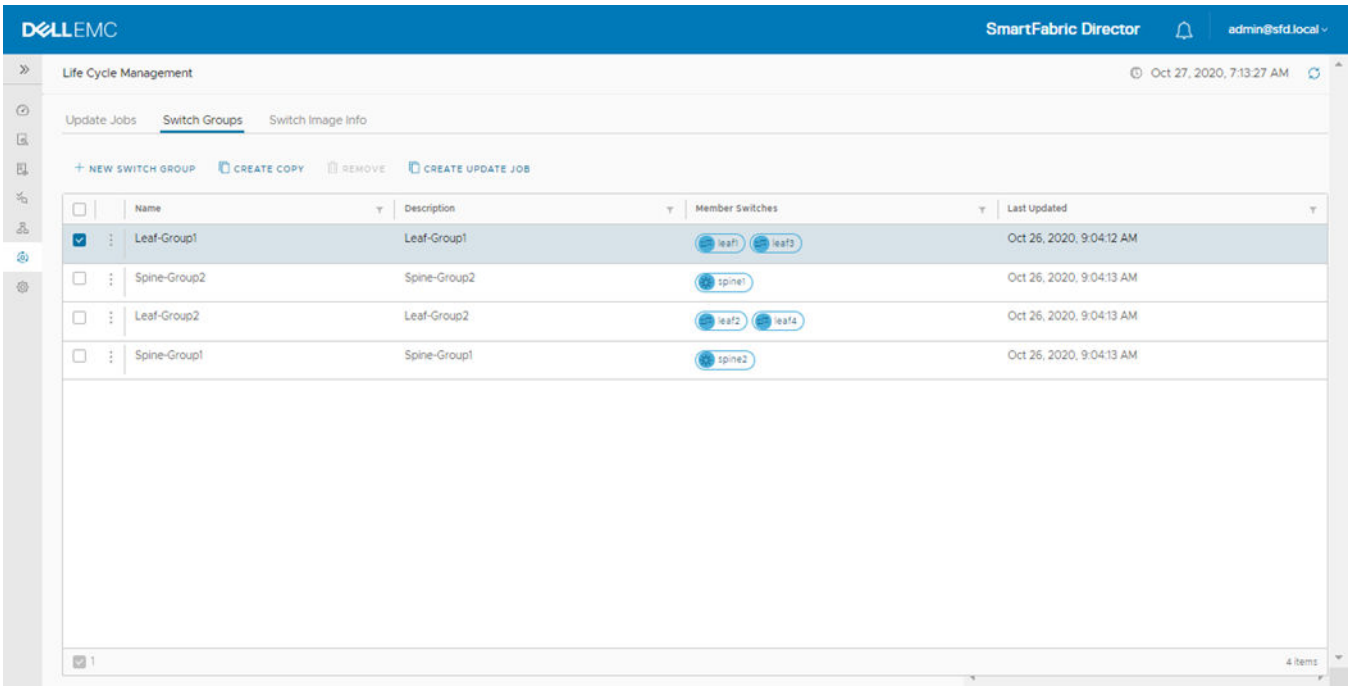


You are now ready to define a switch lifecycle job to create an update job.

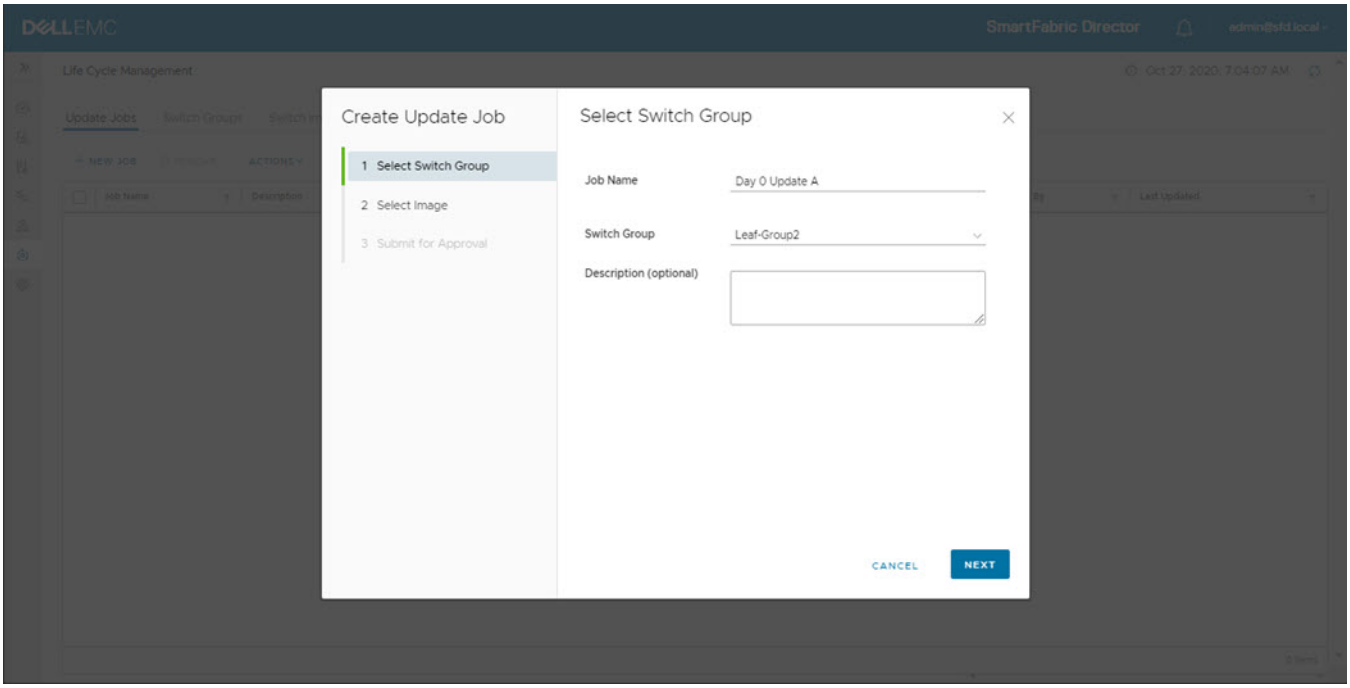
Create switch update job

This information describes how to create a switch update job. As part of the update job creation, you can select a switch group from the list of available switch groups.

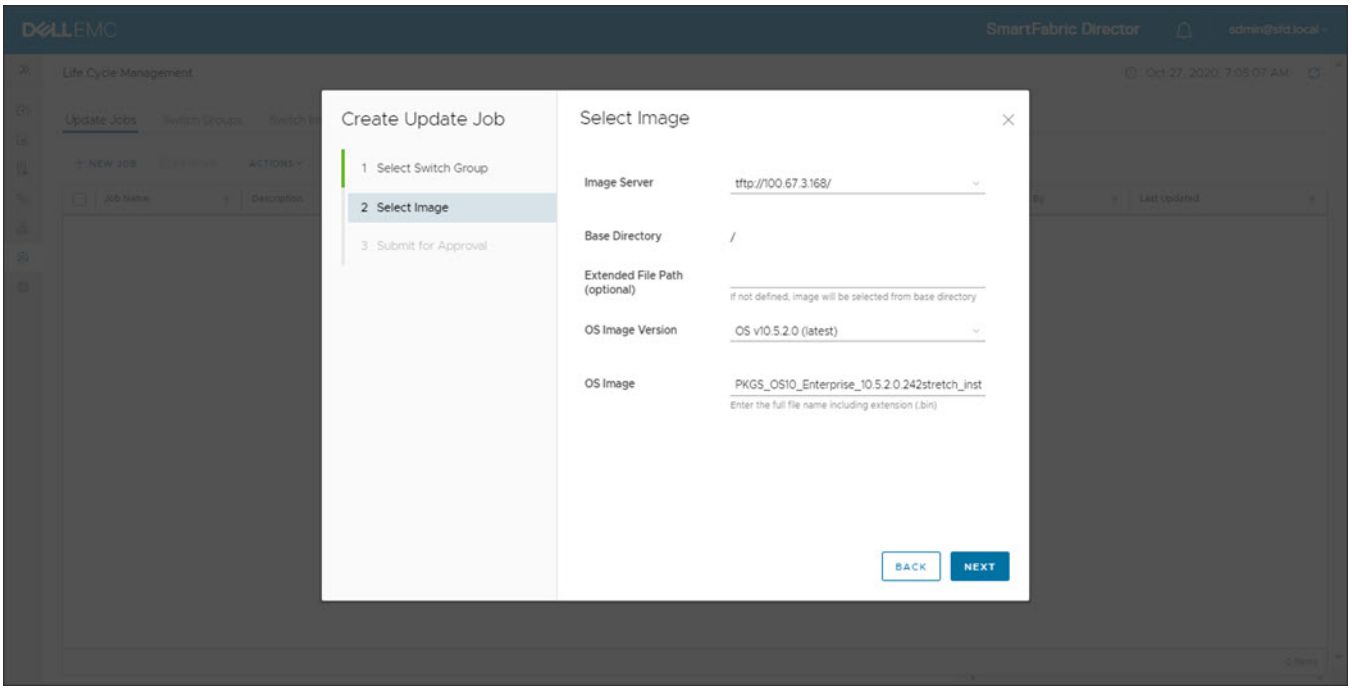
1. Select **Life Cycle Management > Switch Groups > Create Update Job**.



2. Enter the job name, select the switch group, enter an optional description, then click **Next**.

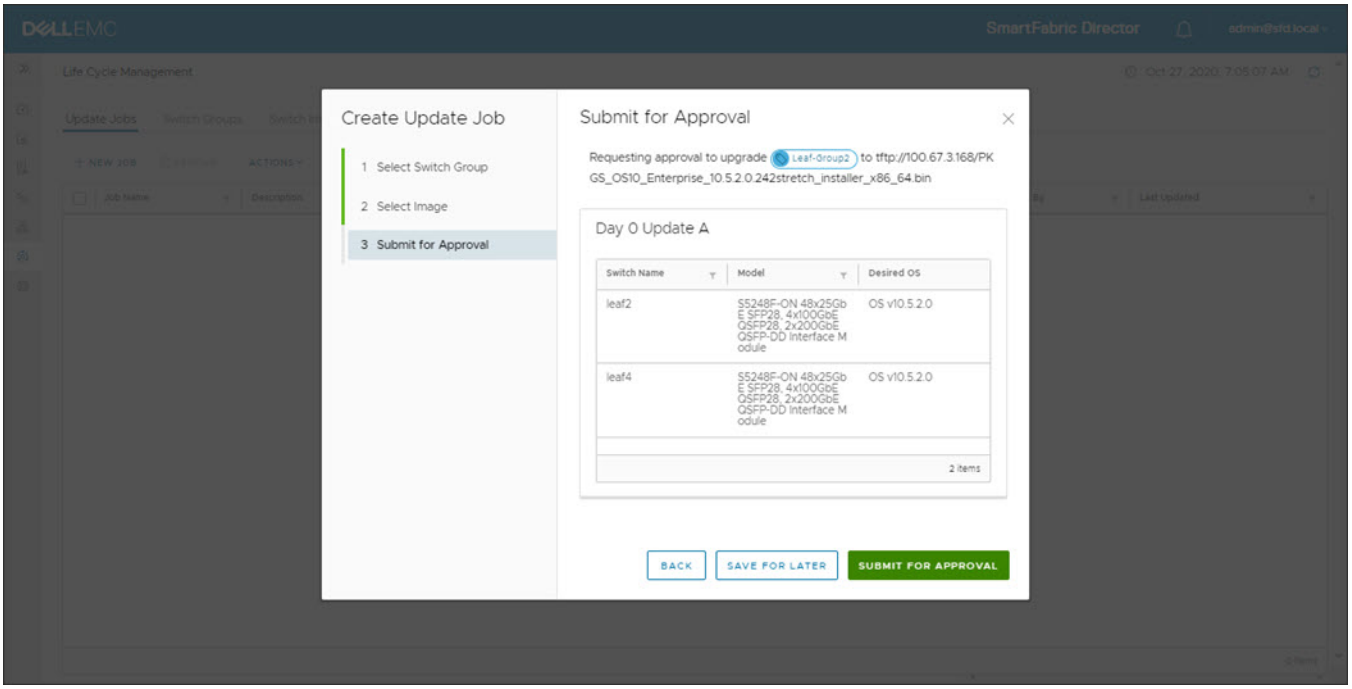


3. Specify an OS10 image including the file extension (.bin). Verify the specified image name matches the name of the image file on the remote server, then click **Next**. All switches in a switch group are updated to the specified image when the Update job is run.

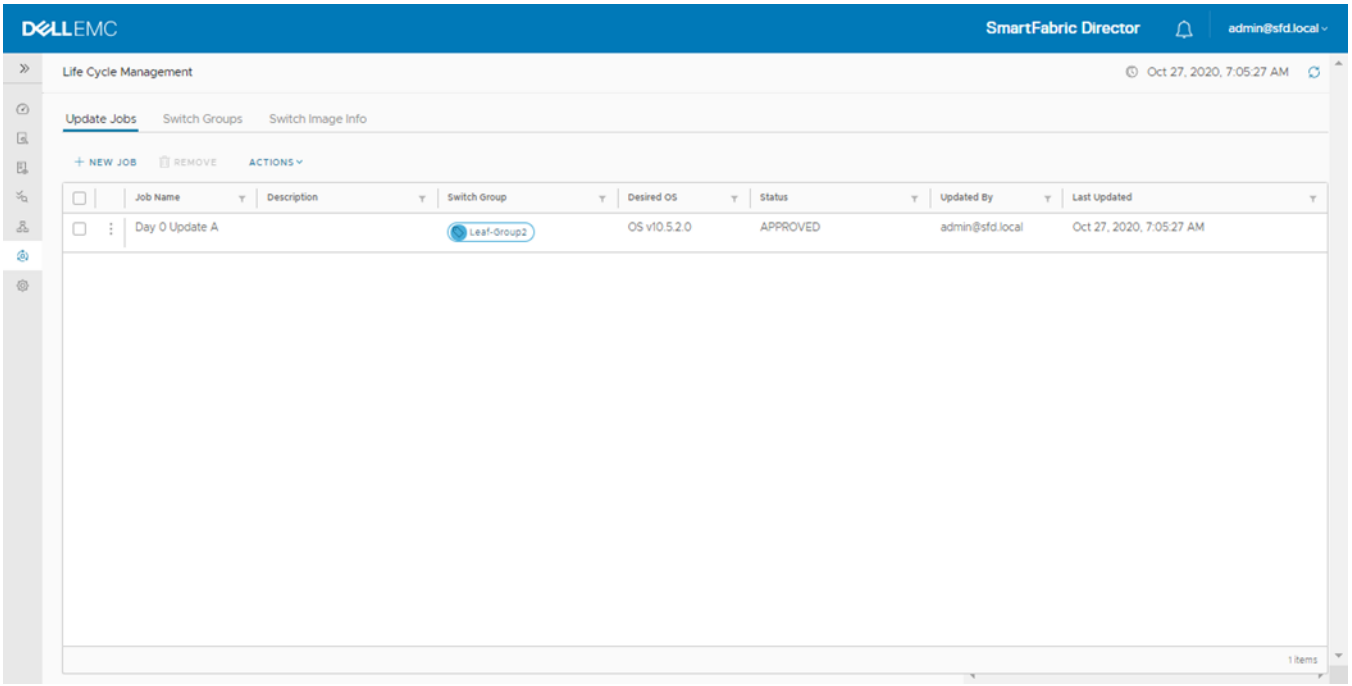


The content of the OS image version drop-down is populated from the SwitchOS image support matrix.

4. Review the image update information, then click **Submit for approval**. You can also click **Save for later** or **Back** to return to the previous screen.



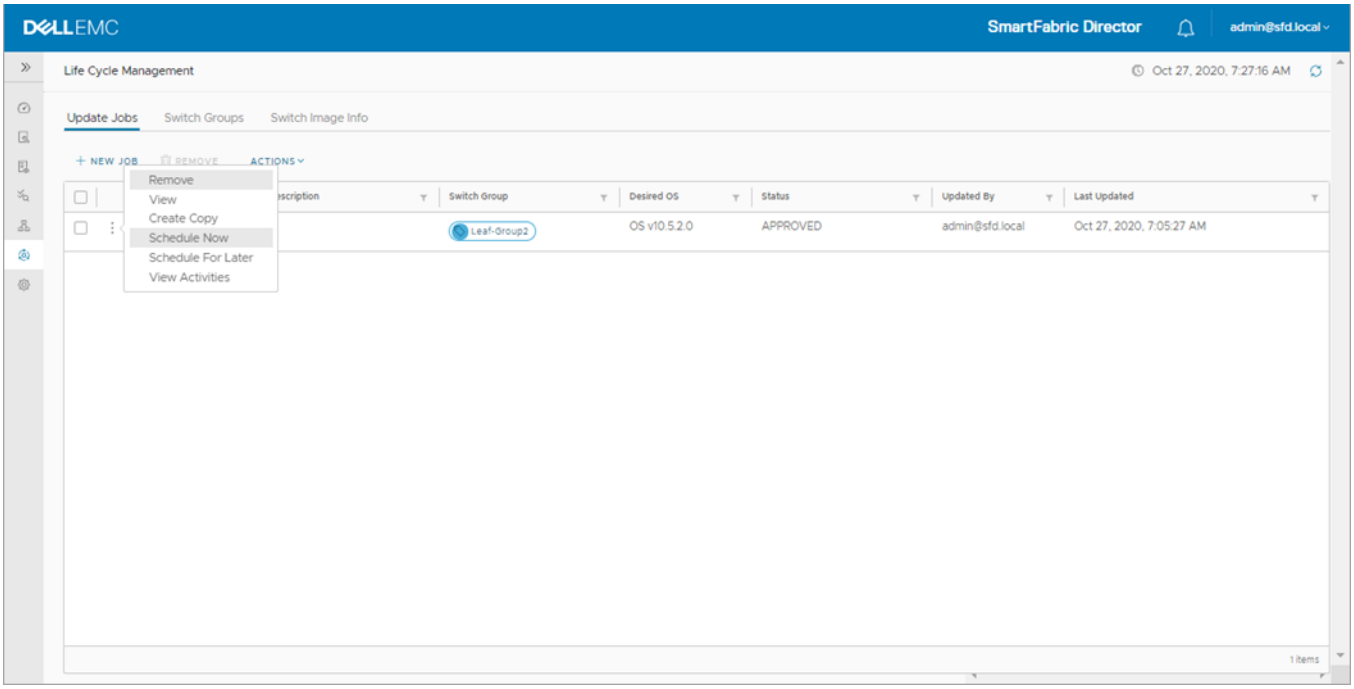
The status of the update job displays.



Schedule switch update job

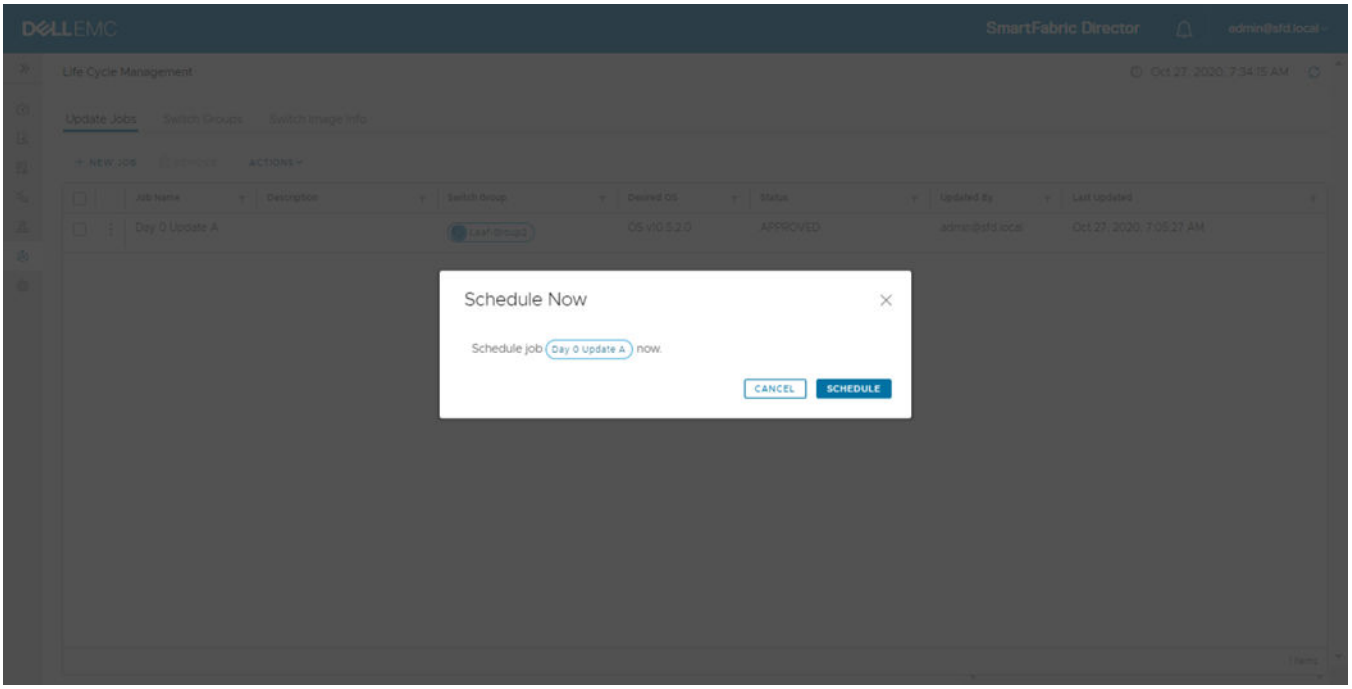
This information describes how to schedule an update job. You can schedule an approved job for execution now, or select a future date and time using the calendar.

1. Select **Schedule Now**.

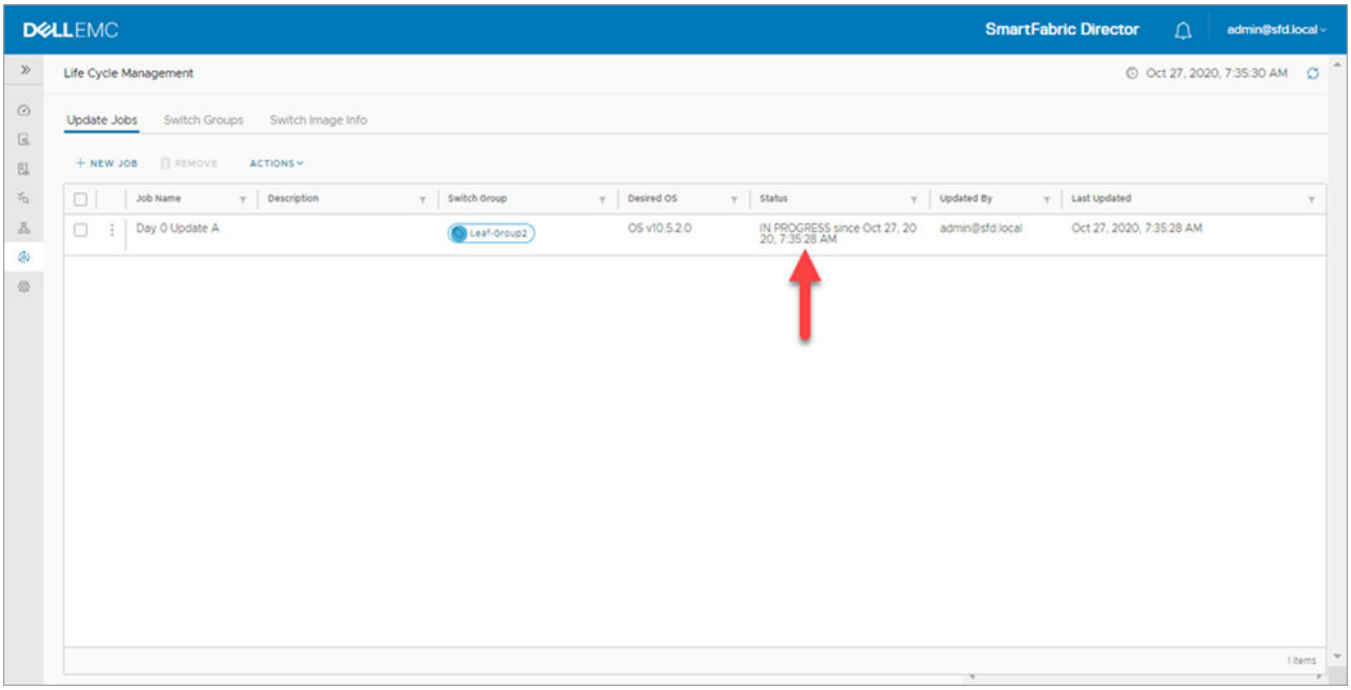


When the job is run, SFD directs the switches to the Image Server to download the specified image. The switch downloads the image, installs the new image, and reboots.

2. Click **Schedule**. You can also select to schedule the job for a future date and time.

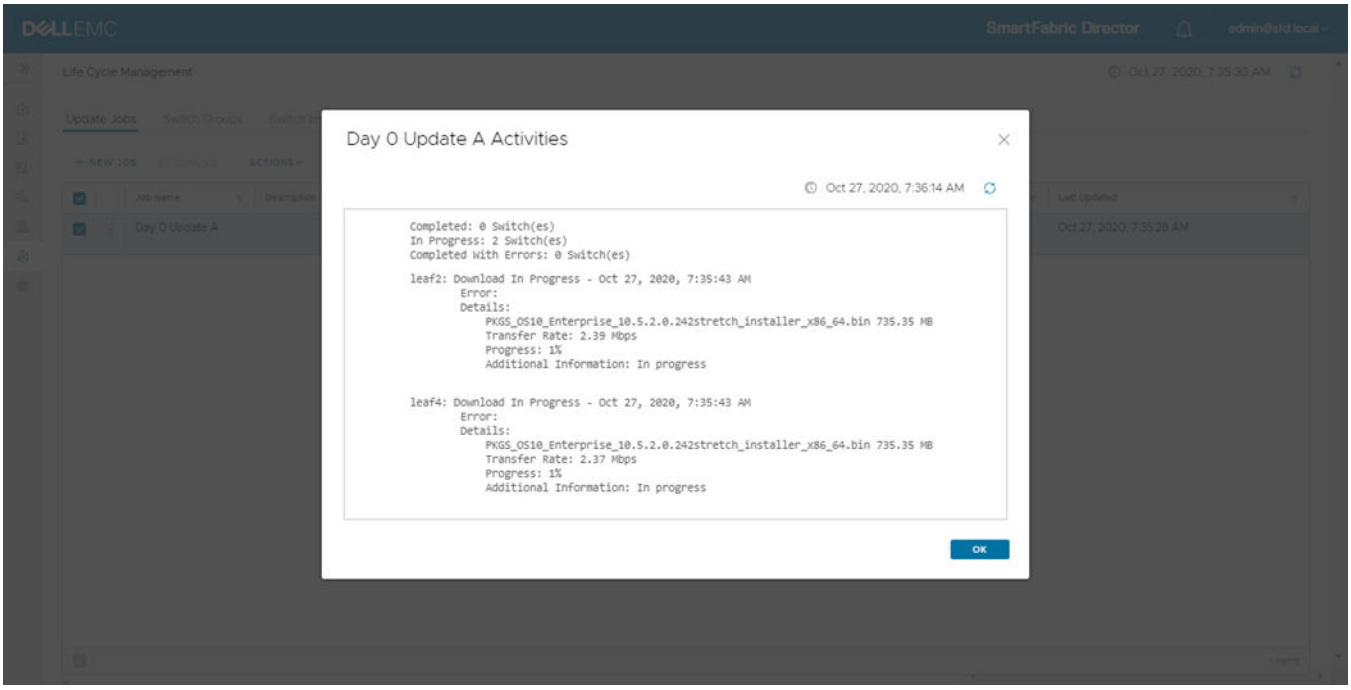


The status of the update job displays.



3. Select **View Activities** to display the switch update job activities in the open window, then click **OK**.

NOTE: You can also create a copy of the update job to simplify making changes to an existing job.

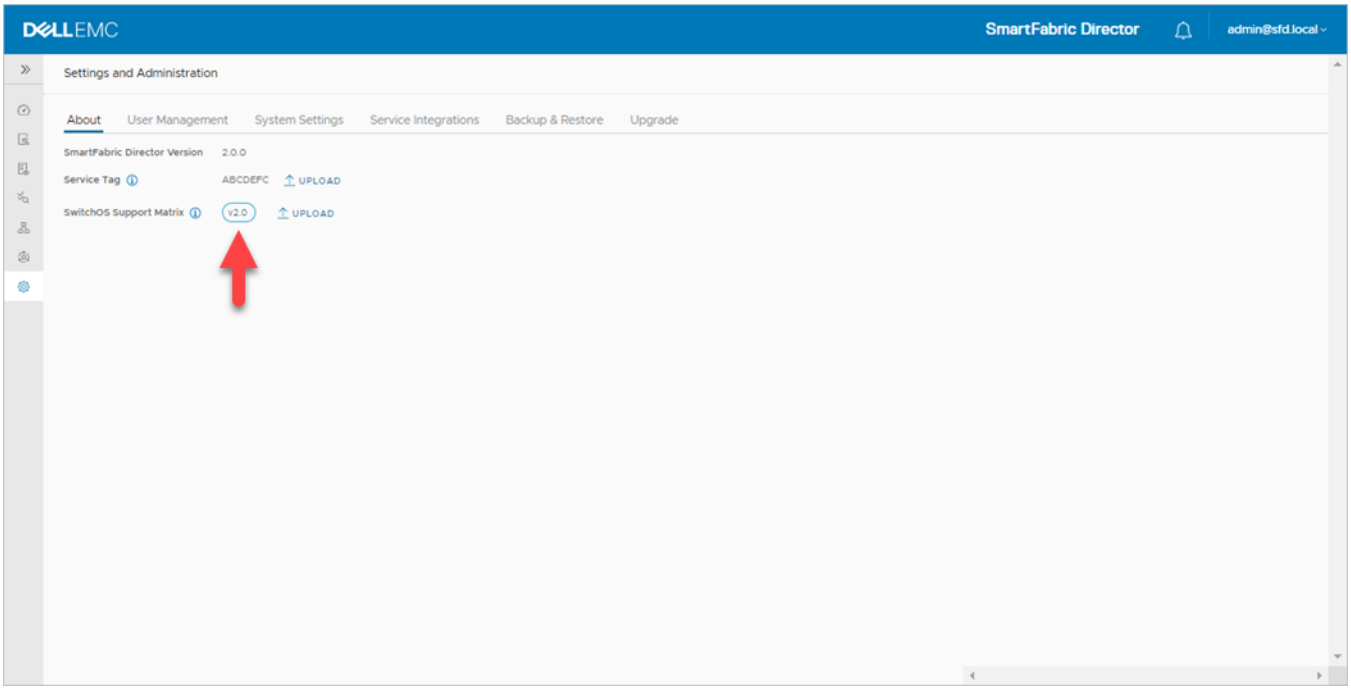


4. Once the update job finishes, select **View** to display the update job activities.

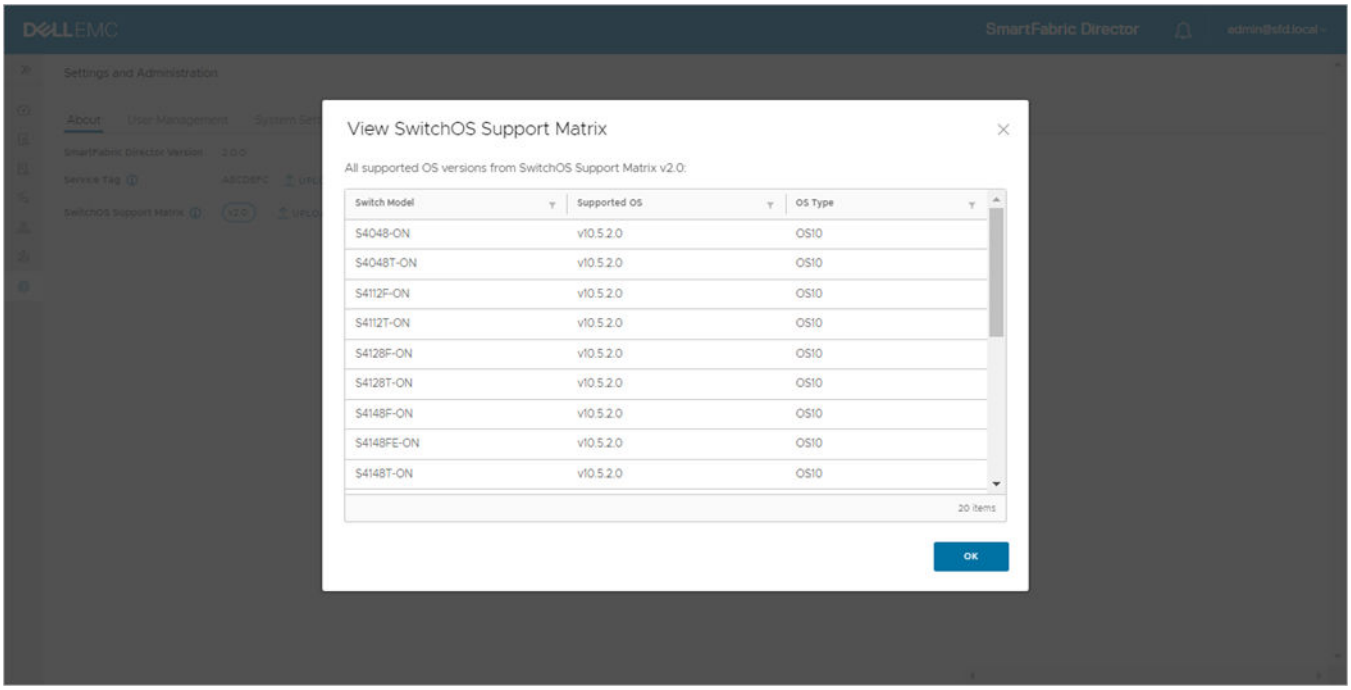
SwitchOS support matrix

This new feature allows you to select images specified in the SwitchOS support matrix. If a new SmartFabric OS10 image is released and the current SFD version is verified with it, you can upload the image to SFD to be available in life cycle management.

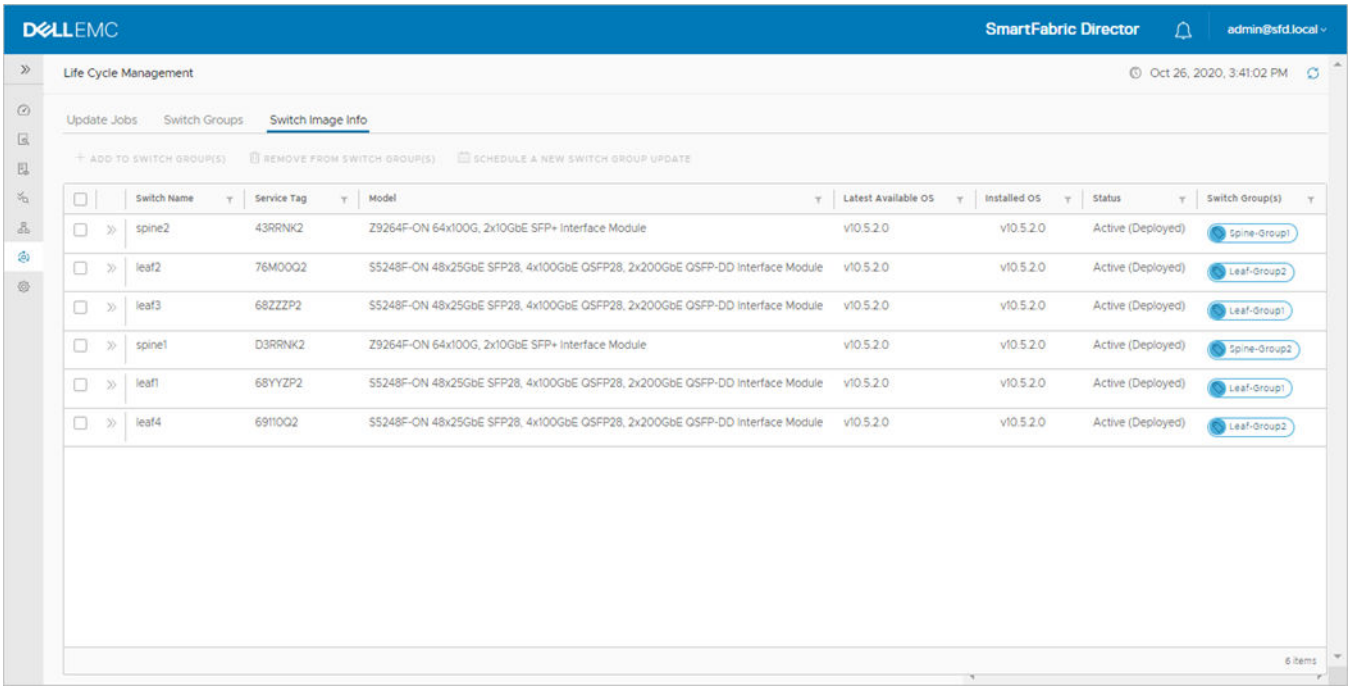
1. Click on the SwitchOS support matrix to view the compatibility matrix.



2. View the contents, then click **OK**.



3. Select **Life cycle management > Switch image info** to view the latest available SwitchOS image file available with the currently installed operating system on each discovered or active switch.


DELL EMC
SmartFabric Director
admin@sfd.local
Life Cycle Management
Oct 26, 2020, 3:41:02 PM
Update Jobs
Switch Groups
Switch Image Info
ADD TO SWITCH GROUP(S)
REMOVE FROM SWITCH GROUP(S)
SCHEDULE A NEW SWITCH GROUP UPDATE
Switch Name
Service Tag
Model
Latest Available OS
Installed OS
Status
Switch Group(s)
spine2 43RRNK2 Z9264F-ON 64x100G, 2x10GbE SFP+ Interface Module v10.5.2.0 v10.5.2.0 Active (Deployed) Spine-Group1
leaf2 76M00Q2 S5248F-ON 48x25GbE SFP28, 4x100GbE QSFP28, 2x200GbE QSFP-DD Interface Module v10.5.2.0 v10.5.2.0 Active (Deployed) Leaf-Group2
leaf3 68ZZZP2 S5248F-ON 48x25GbE SFP28, 4x100GbE QSFP28, 2x200GbE QSFP-DD Interface Module v10.5.2.0 v10.5.2.0 Active (Deployed) Leaf-Group1
spine1 D3RRNK2 Z9264F-ON 64x100G, 2x10GbE SFP+ Interface Module v10.5.2.0 v10.5.2.0 Active (Deployed) Spine-Group2
leaf1 68YYZP2 S5248F-ON 48x25GbE SFP28, 4x100GbE QSFP28, 2x200GbE QSFP-DD Interface Module v10.5.2.0 v10.5.2.0 Active (Deployed) Leaf-Group1
leaf4 69110Q2 S5248F-ON 48x25GbE SFP28, 4x100GbE QSFP28, 2x200GbE QSFP-DD Interface Module v10.5.2.0 v10.5.2.0 Active (Deployed) Leaf-Group2
6 items

12

Using the CLI

This information explains how to access the command-line interface (CLI), and the available commands.

Access the CLI

1. SSH to the IP address configured for SFD.

```
login-srv-05-user%:~> ssh username@sfd.local@ip_address
admin@sfd.local@10.12.124.125's password:
Last login: Mon Oct  17 18:00:59 2019 from 10.12.1.9
```

2. Enter `sfd` to access the SmartFabric Director CLI.

```
admin@sfd.local@SFD-R5:~$ sfd
DellEMC SmartFabric Director CLI
sfd>
```

Command help

To view a list of available options or arguments, enter `-h` or `--help` after any command.

```
sfd> backup --help
usage: backup [-h] {list,create,delete,restore} ...

SFD backup operations - create, delete, list, restore

positional arguments:
  {list,create,delete,restore}

optional arguments:
  -h, --help            show this help message and exit
```

Topics:

- log_level
- service
- support_bundle
- system

log_level

Sets the log-level for internal events and debug messages.

Command	`log_level list --service` *`service_name`* `all log_level set --service` *`service_name`* `--level` *`log_level`*
Options	• `--service` *`service_name`* — Lists log-levels for a specific service name • `all` — Lists log-levels for all available services

- `--level log_level` — Sets the specified service to the wanted log-level (`error`, `warn`, `info`, `debug`, `trace`)

Usage Use the `all` option to list all service levels.

Example

```
sfd> log_level list --service all
+-----------------------------------------+
| SERVICE LOG LEVELS                      |
+-----------------------------+-----------+
| Service Name                | Log Level |
+-----------------------------+-----------+
| config-builder-service      | INFO      |
| fabric-orchestrator-service | INFO      |
| host-network-service        | INFO      |
| notification-service        | INFO      |
| rest-api                    | INFO      |
| switch-manager-service      | INFO      |
| system-controller-service   | INFO      |
| topology-service            | INFO      |
| telemetry-collector-service | INFO      |
| telemetry-service           | INFO      |
+-----------------------------+-----------+
```

```
sfd> log_level set --service notification-service --level error
+----------------------------------+
| SET LOG LEVEL OPERATION STATUS   |
+-----------------------+----------+
| Service Name          | Status   |
+-----------------------+----------+
| notification-service  | success  |
+-----------------------+----------+
```

Releases 1.1.0 or later

service

Provides service operations including health and statistics.

Command `service [list | health --name service_name | stats --name service_name | restart --name service_name]`

Options

- `list` — List all internal services
- `health` — Status of internal services
- `stats` — Metrics including memory and CPU usage of internal services
- `restart` — Restarts the specified service
- `--name service_name` — Service name

Usage This command provides information about services, performance, and state which can be used for monitoring to diagnose possible problems.

Examples

```
sfd> service list
['config-builder-service', 'elasticsearch',
'external_syslog_collector', 'fabric-orchestrator-service',
'host-network-service', 'infra-processors', 'kube-state-metrics',
'nfc.host', 'nats', 'nats-exporter', 'nats-streaming',
'prometheus', 'prometheus-pgw', 'nginx-exporter', 'nginx-gw',
'node_exporter', 'notification-service', 'rest-api', 'switchmanager-
```

```
service', 'system-controller-service', 'topologyservice',
'telemetry-collector-service', 'telemetry-service']
```

```
sfd> service health --name rest-api
------------------------------------------------
Service-Status : RUNNING
Pod-Status : RUNNING
------------------------------------------------
```

Releases 1.1.0 or later

support_bundle

Creates a support bundle to be used for debugging purposes.

Command `support_bundle create --name bundle_name`

Options

- `create` — Creates a support bundle
- `--name bundle_name` — Name of the support bundle

Usage This command takes a snapshot of current internal states including health, debug messages, and logging. Verify you have enough local storage before running this command as the file size is large.

NOTE: Do not attempt any SFD operations while the support bundle is being created. Generating a support bundle is CPU intensive, could result in momentary CPU spikes, and may impact the performance of SFD.

Example

```
sfd> support_bundle create --name test
Starting creating support bundle. It will take few minutes to
collect data
Successfully created support bundle test.tar.gz at
/data/nfc_support_bundle/ path
```

Releases 1.1.0 or later

system

Displays the overall software health.

Command `system health`

Options None

Usage None

Example

```
+-----------------------------------------------------------+
| SFD-System-Resource                                       |
+-----------------------------------+------------+--------+
| Name                              | Value      | Unit   |
+-----------------------------------+------------+--------+
| CPU Usage                         | 14.87      | %      |
| Memory - Available                | 2540158976 | bytes  |
| Memory - Available - %            | 30.34      | %      |
| Available Disk (partition = /)    | 86.44      | Gb     |
| Available Disk (partition = /) - % | 89.34      | %      |
| Network Rate | 146.76 | bps |
+-----------------------------------+------------+--------+
+-----------------------------------------------------------+
| SFD-System-Health                                         |
+---------------------------+----------------+------------+
| SFD-Service               | Service-Status | Pod-Status |
```

```
+-----------------------------+----------------+------------+
| config-builder-service      | RUNNING        | RUNNING    |
| elasticsearch               | -              | RUNNING    |
| external_syslog_collector   | RUNNING        | -          |
| fabric-orchestrator-service | RUNNING        | RUNNING    |
| host-network-service        | RUNNING        | RUNNING    |
| infra-processors            | -              | RUNNING    |
| kube-state-metrics          | -              | RUNNING    |
| nfc.host                    | RUNNING        | -          |
| nats                        | -              | RUNNING    |
| nats-exporter               | -              | RUNNING    |
| nats-streaming              | -              | RUNNING    |
| prometheus                  | -              | RUNNING    |
| prometheus-pgw              | -              | RUNNING    |
| nginx-exporter              | -              | RUNNING    |
| nginx-gw                    | -              | RUNNING    |
| node_exporter               | RUNNING        | -          |
| notification-service        | RUNNING        | RUNNING    |
| rest-api                    | RUNNING        | FAILED     |
| switch-manager-service      | RUNNING        | RUNNING    |
| system-controller-service   | RUNNING        | RUNNING    |
| topology-service            | RUNNING        | RUNNING    |
| telemetry-collector-service | RUNNING        | RUNNING    |
| telemetry-service           | RUNNING        | RUNNING    |
+-----------------------------+----------------+------------+
+------------------------+
| System Overall Health |
+------------------------+
| DOWN                   |
+------------------------+
```

Releases 1.1.0 or later

13

Frequently asked questions

This information contains answers to frequently asked questions about SmartFabric Director.

Configuration

Do I need to configure the Management interface on each switch?

The Management interface must be configured and enabled on each switch in the fabric (see Management interface).

How do I view switch port profile configuration?

```
OS10# show switch-port-profile 1/1

|  Node/Unit   |  Current     |  Next-boot   | Default    |
|--------------+--------------------+--------------------|
|     1/1      |  profile-2   |  profile-2   | profile-1  |

Supported Profiles:
profile-1
profile-2
profile-3
profile-4
profile-5
profile-6
```

Lifecycle

How do I add a switch group?

See Define switch group for complete information.

Where can I view the status of my image update job?

See Schedule switch lifecycle job for complete information.

Administration

I cannot connect to my image server.

See Specify image servers for complete information.

Maintenance

How can I backup and restore SmartFabric Director?

SmartFabric Director supports back and restore to allow the software to return to a golden configuration at any time. Once the fabric has been defined, configured, and the behavior is verified the operator can use `backup create` to backup the SFD data including the fabric intent. See backup for complete information.

Index

T

U

V

W