Dell EMC Network Validation Tool for VxRail

December 2019

H17633.3

User Guide

Abstract

This user guide describes the capabilities of the Network Validation Tool (NVT) for VxRail. It outlines NVT validation procedures and provides information about using NVT for VxRail Appliances.

Dell EMC Solutions

Copyright

Published in the USA December 2019 User Guide H17633.3.

Contents

Revisions

Table 1. Revision table

Date	User Guide part number	Description
February 2019	H17633	• New user interface • Additional enhancements
June 2019	H17633.1	VxRail NVT v5.1.0 feature enhancements: • Universal JSON filetype support • Ping enhancement for reply from same IP address check • Forward and reverse nslookup enhancements • Peer link validation • Port part of port Channel validation • SRS validation message enhancement • Validation support with chart and status
August 2019	H17633.2	VxRail NVT v5.2.0 feature enhancements: • NVT Terms of Use • NVT executable digitally signed so that it is not blocked by Windows Defender • Validation results summary filename with customer name and timestamp • Exported JSON filename with customer name and timestamp • Option to skip ping tests • Enhancement to import 10 Guest VM network VLAN IDs from PEQ JSON • External VxRail vCenter version validation • External vCenter validation enhancement for data center and cluster when authentication fails • Customer name import support from PEQ NVT JSON • External vCenter management credential authentication fix • Dell OS9 switch log parsing fix for the show version • Dell OS10 first port member under first port channel parsing fix

Date	User Guide part number	Description

December 2019	H17633.3	VxRail NVT v5.3.0 feature enhancements:
		• Stretched cluster validation
		• vSAN 2-Node validation
		• New enhanced switch log import UI
		  ○ Auto discover Switch make and OS version from imported switch file
		  ○ Fill template filename enhancement
		• DNS forward/reverse lookup enhancement check when more than one IP address/FQDN is returned
		• Inherit mode (trunk/access) when port is part of port channel
		• Improvement in estimated time to complete when skip ping test is enabled
		• Hostname/domain name format validation
		• Validation of IPs when VxRail cluster is already deployed
		• Splash screen when NVT is launched

Executive summary

The Network Validation Tool (NVT) enables you to validate configurations before you deploy the VxRail Appliance. NVT ensures that there are no invalid configurations at the time of deployment. If there is a missing configuration, you can complete it before you schedule a VxRail Appliance deployment to avoid delay. Trained Dell EMC employees, partners, and customers can download NVT after completing all the network configurations that are required for the VxRail Appliance installation at the customer site.

For a new VxRail Appliance installation, reserve a set of IP addresses for the VMware ESXi host and virtual machines (VMs). Also, configure the fully qualified domain name (FQDN) in the DNS servers and complete top-of-rack (ToR) switch configuration.

We value your feedback

Dell EMC and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell EMC Solutions team by email or provide your comments by completing our documentation survey.

Authors: Claire O'Keeffe, Ganesh Chichakar

Contributors: Penelope Howe-Mailly, David Warren

VxRail NVT-initiated tests

The following figure shows the components that NVT for VxRail validates:

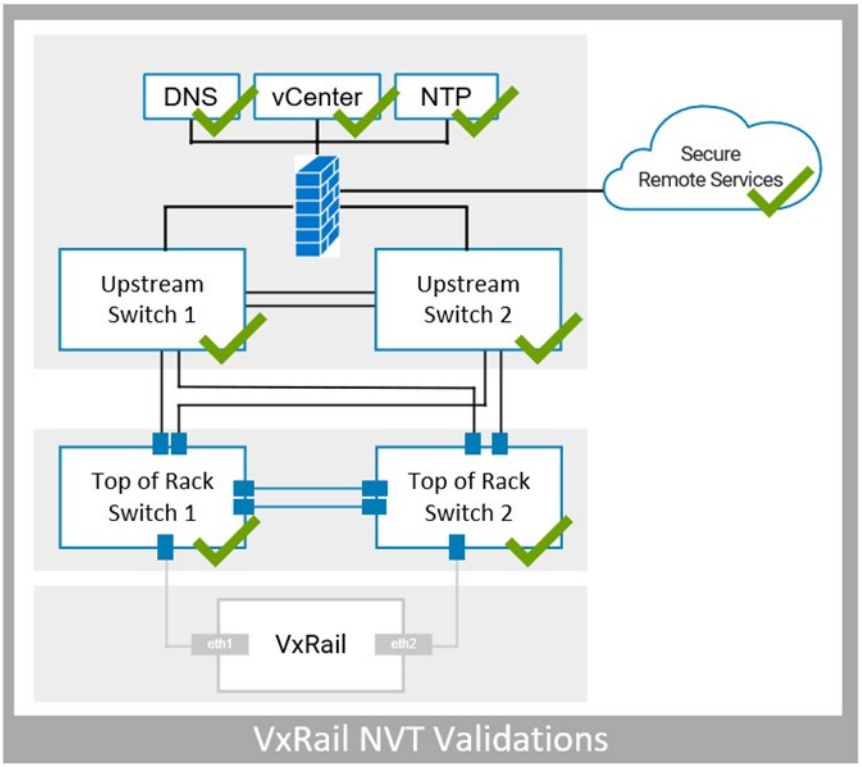

Figure 1. Components validated by NVT for VxRail

To initiate tests, run NVT from a workstation on the management network. The following table defines the validations that NVT initiates and the commands that are used:

Table 2. NVT-initiated validations

Validations performed	Commands used	Components validated	Note
IP address availability	Ping	• ESXi hosts • VxRail Manager VM • Log Insight VM • SRS VM (internal) • Internal VCenter VM • Internal PSC VM • VxRail Manager default IP address	Do not use IP addresses that are reserved for VxRail Appliance hosts or VMs in the customer's local network. An IP conflict might occur when a new host powers on with the same IP address.
IP address reachability	Ping	• Management default gateway • Syslog server • SRS gateway (external)	The IP address must be reachable to provide necessary services at the time of VxRail Appliance installation.

Validations performed	Commands used	Components validated	Note
DNS server access	`Telnet`	DNS server	DNS servers must be reachable.
DNS resolution	`nslookup`	• ESXi hosts • VxRail Manager VM • Log Insight VM • Internal vCenter VM • Internal PSC VM	NVT verifies forward and reverse lookup for each VxRail node and any service VMs that are internal to the VxRail Appliance.
NTP server access	`W32tm`	NTP Servers	NTP servers must be reachable.
vCenter access	`vSphere API calls`	External vCenter	NVT tests authentication to log in to the vCenter server.
vCenter configuration	`vSphere API calls`	External vCenter	The vCenter Datacenter (VDC) must exist. There must be no cluster name.
vCenter version	`vSphere API call`	External vCenter	The vCenter version validates the compatibility of the external vCenter version with the VxRail appliance product version selected.
Public SRS server access	`Telnet`	• SRS V3 FTPS servers • SRS V3 global access servers	To configure the VxRail dial home feature, connectivity from the management network to SRS global access servers is required. A workstation that is running NVT must have access to the Internet for successful test results. SRS global access servers must be reachable on the required TCP Ports.
VLANs	`Show vlan` `Show running-config`	• Show vlan • Show running-config	The VLAN ID for the ESXi Management, vSAN, vMotion, and Guest VM networks must exist in the ToR and upstream switch output. For VxRail 4.7.0, the ESXi Management-Internal VLAN ID must exist in the ToR switch output.
STP mode	`Show run`	• ToR switch output • Upstream switch output	NVT determines if STP mode is present in the ToR or upstream switch output and provides informational messages.
STP priority	`Show run`	• ToR switch output • Upstream switch output	NVT determines if STP mode is present and the STP priority.
Trunk mode	`Show run`	• ToR switch output • Upstream switch output	NVT verifies that trunk mode is configured on the ToR and upstream switch ports.

Validations performed	Commands used	Components validated	Note
Trunk-allowed VLAN	`Show run`	• ToR switch output • Upstream switch output	NVT verifies that trunk mode is configured and allows the required VLANs on ToR and upstream switch ports.
Peer-link VLAN	`Show running-config`	• ToR switch output • Upstream switch output	NVT verifies that correct VLANs are present on the switch port peer link as tagged VLANs.
Port is a member of the port channel	`Show running-config`	• ToR switch output • Upstream switch output	NVT verifies that the port is a member of the port channel. Also displays the mode, if it is present.

VxRail NVT benefits

The benefits of using VxRail NVT include:

- Verification of site readiness before the VxRail Appliance arrives at the customer location
- Faster manual validation of prerequisites for the VxRail Appliance deployment
- Enforcement of Dell EMC-recommended best practices
- An easy-to-navigate user interface (UI)
- The ability to import and export configuration details

VxRail Appliance physical topology

The following figure shows the VxRail Appliance physical topology:

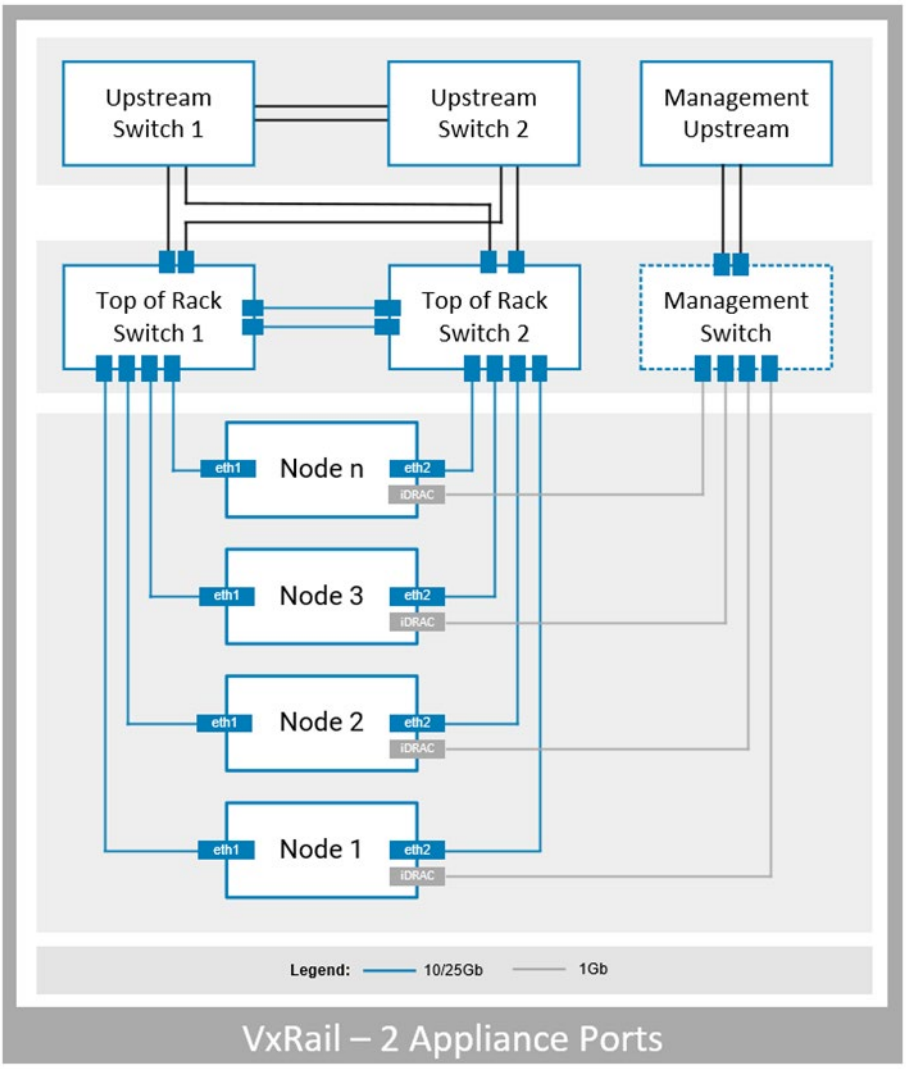

Figure 2. VxRail Appliance physical topology

VxRail Appliance logical topology

The following figure shows the VxRail Appliance V4.5 logical topology:

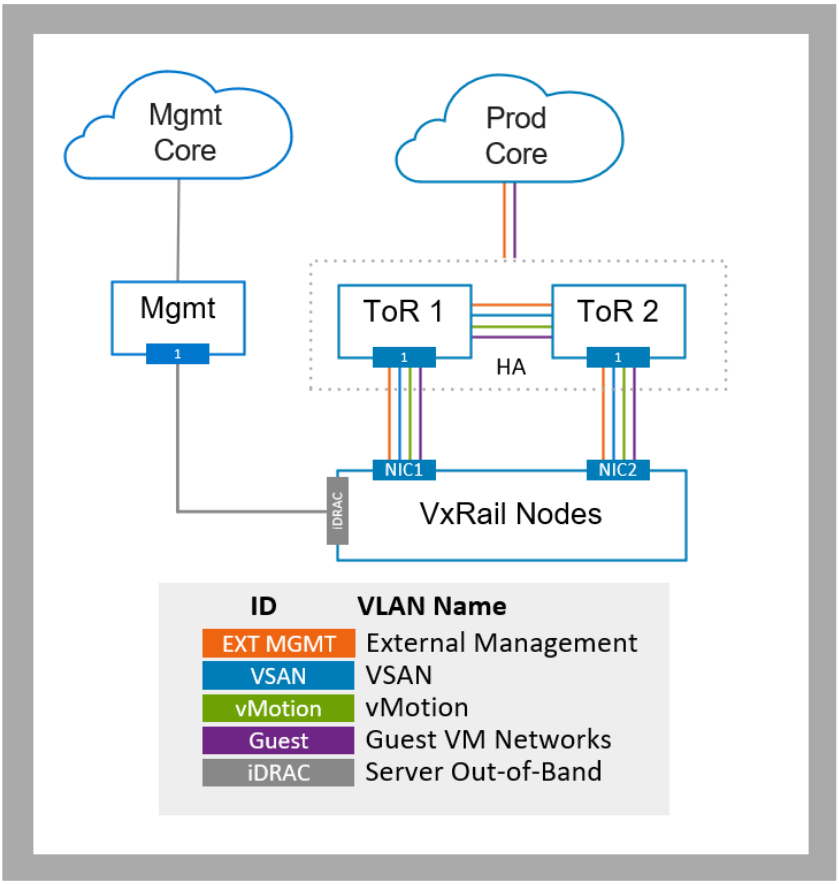

Figure 3. VxRail Appliance V4.5 logical topology

The following figure shows the VxRail Appliance V4.7 logical topology:

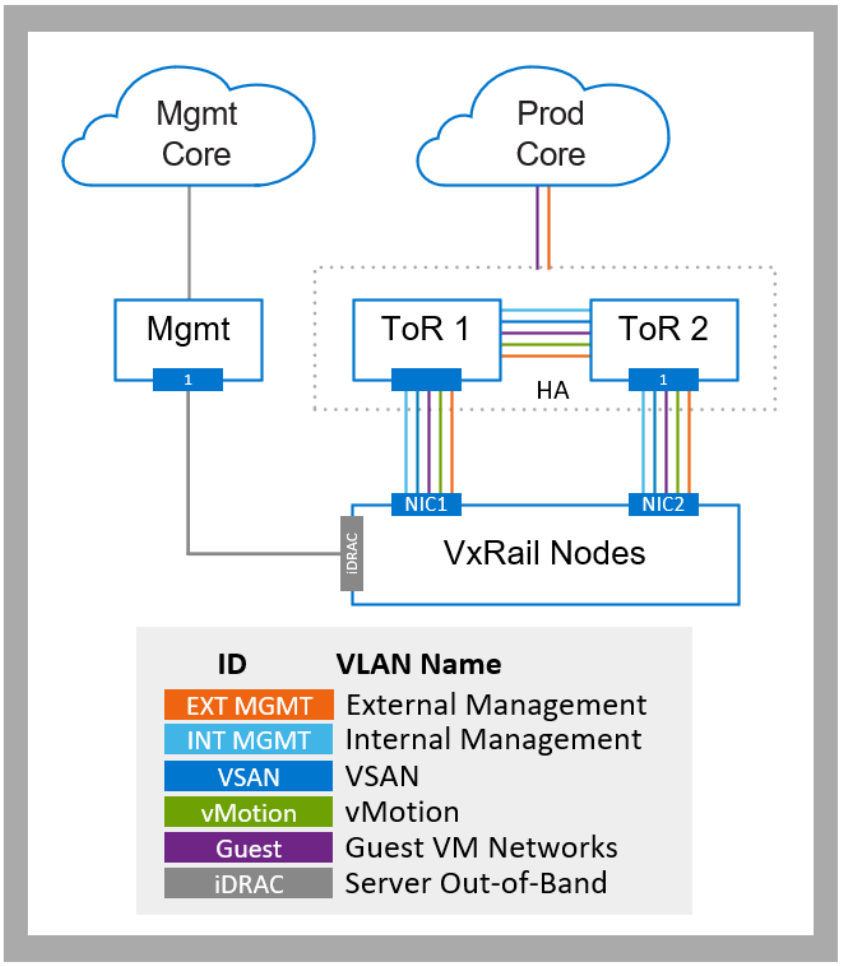

Figure 4. VxRail Appliance V4.7 logical topology

Compatibility matrix

The following table shows the compatibility matrix:

Table 3. NVT for VxRail Appliance compatibility matrix

Component	Version
VxRail Appliance	4.7.x, 4.5.x
NVT for VxRail Appliance	5.3.0
Operating system	Microsoft Windows 32-bit and 64-bit
VxRail Pre-Engagement Questionnaire (PEQ)	4.7.x, 4.5.x
Dell EMC Switch operating system	Dell EMC Networking OS9 Dell EMC Networking OS10
Cisco switch operating system	Cisco NXOS Cisco IOS

Note:

- NVT does not currently validate the Application Centric Infrastructure (ACI) fabric, but can provide valuable information about other components.
- The computer system must support English as the default language.

Generate a JSON file

Optionally, use the VxRail PEQ to generate a JSON file that contains data that NVT requires. Then, import the JSON file into NVT.

1. In a browser, go to Pre-Engagement Questionnaire (PEQ) on Dell EMC Central.
2. Under **Associated Files**, download the VxRail PEQ spreadsheets.
3. Open the PEQ and ensure that the System Engineer (SE), Project Manager (PM), and Solution Architect (SA) update all the information in the PEQ.
4. On the **VxRail Cluster** tab, click **Generate NVT/FDC JSON**, as shown in the following figure:

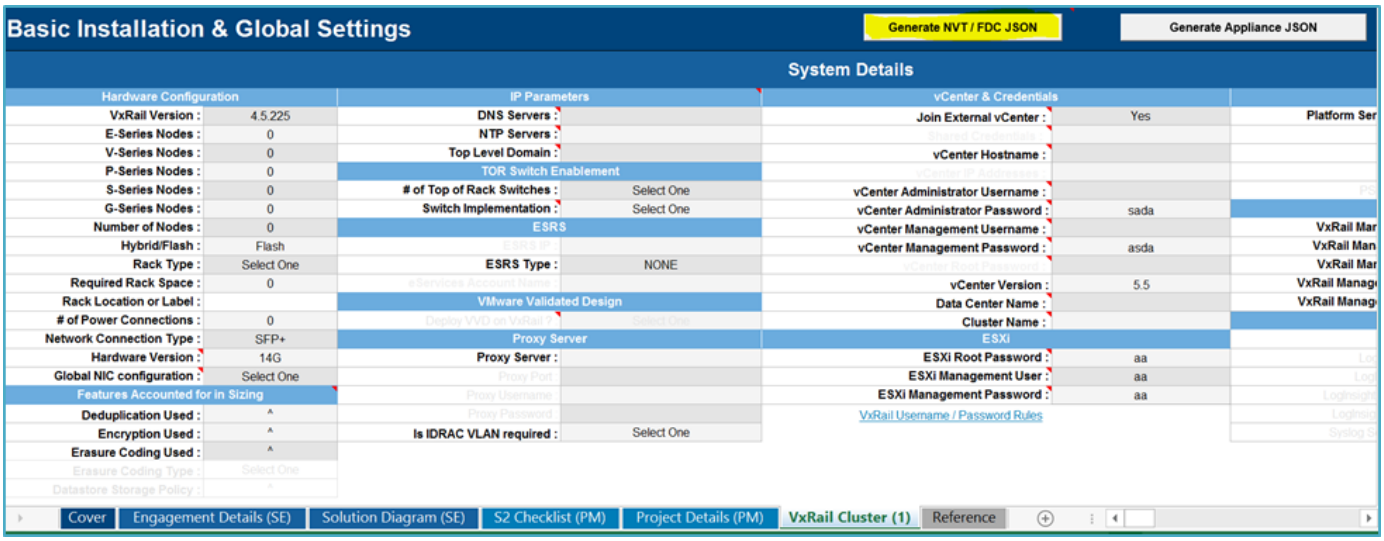

Figure 5. Basic Installation and Global Settings

5. At the prompt, save the JSON file.

Generate a Universal JSON file

Optionally, use the VxRail PEQ to generate a Universal JSON file that contains data that NVT requires. Then import the Universal JSON file into NVT.

1. In a browser, go to Pre-Engagement Questionnaire (PEQ) on Dell EMC Central.
2. Under **Associated Files**, download the VxRail PEQ spreadsheets.
3. Open the PEQ and ensure that the SE, PM, SA, and the cluster update all the information in the PEQ.
4. On the **Cover** tab, click **Create PEQ Data File**, as shown in the following figure:

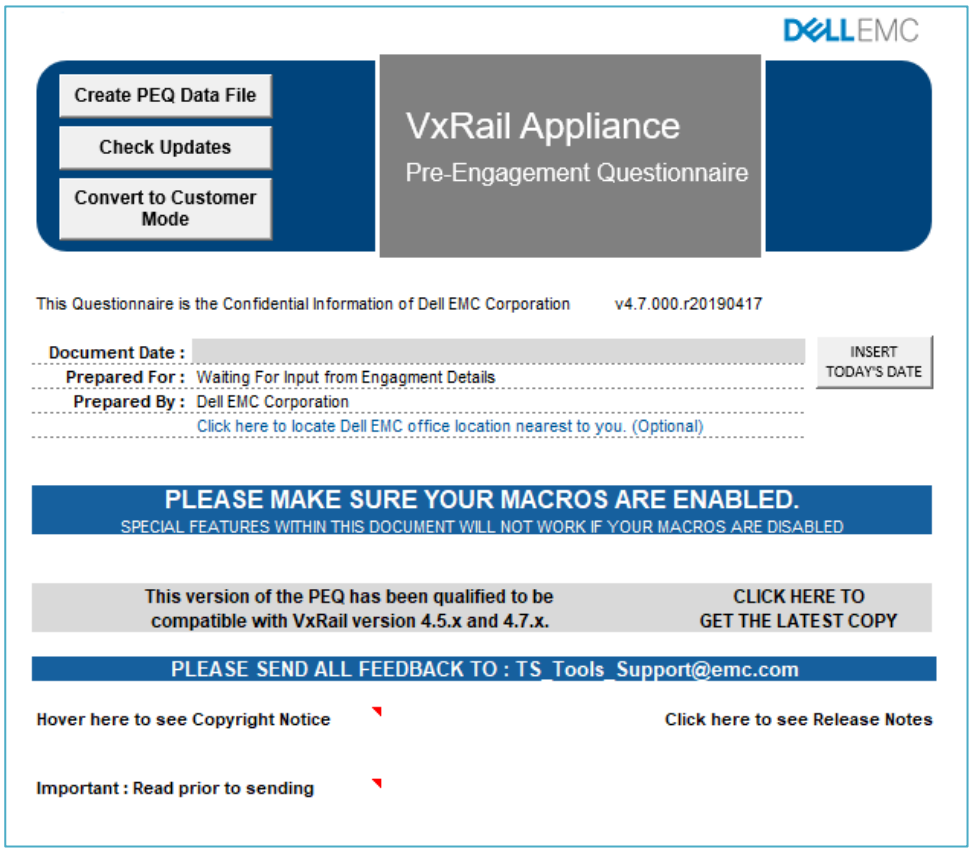

Figure 6. VxRail Appliance Pre-Engagement Questionnaire

5. At the prompt, save the Universal JSON file.

Download and launch NVT

NVT for VxRail is a software and stand-alone application. It does not require any installation.

Download the NVT .ZIP file to a Microsoft Windows workstation in the VxRail management VLAN network where you plan to install the VxRail Appliance.

Download from Dell EMC Central

To download and launch NVT from the Dell EMC Central page:

1. Go to Dell EMC Central.
2. Click **Solutions** on the menu bar.
3. On the **Solutions** page, type `VxRail` in the search field.
4. Hover over **Network Validation Tool for VxRail (NVT)** and click **Download**.
5. Download the NVT .ZIP file.

   The .ZIP file contains the `.exe` file to launch NVT, as well as related documents such as the user guide, the network validation procedure, the security configuration guide, and the firewall configuration requirements.
6. Double-click `VxRail_NVT_v5.3.0_Win.exe` in the .ZIP file to launch NVT.

It might take 30 seconds to open, depending on the host system.

Download from Online Support

To download and launch NVT from Dell EMC Online Support:

1. Go to the following URL:

   https://download.emc.com/downloads/DL90235_Network_Validation_Tool_for_VxRail.zip?source=OLS

2. Click **OK** to open or save the `VxRail_NVT_5.3.0.zip` file.
3. Extract the `VxRail_NVT_5.3.0.zip` file.

   The folder contains the `VxRail_NVT_5.3.0.zip` file, as well as related documents such as the user guide, the network validation procedure, the security configuration guide, and the firewall configuration requirements.

4. Extract the .ZIP file.
5. Double-click `VxRail_NVT_v5.3.0_Win.exe` to launch NVT.

Run NVT

Terms of Use

Read and accept the **Terms of Use**, as shown in the following figure, to continue using the tool for validations:

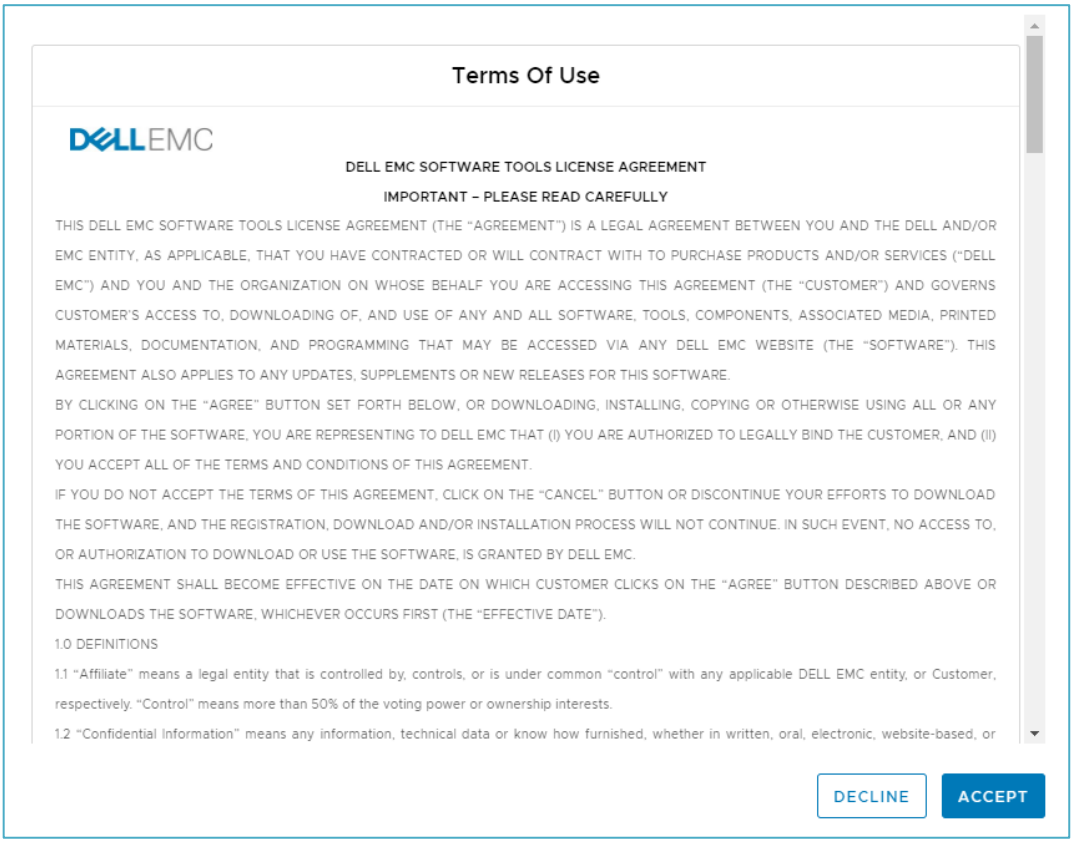

Figure 7. NVT Terms of Use

NVT home page

The NVT home page enables you to select what you want to validate, as shown in the following figure:

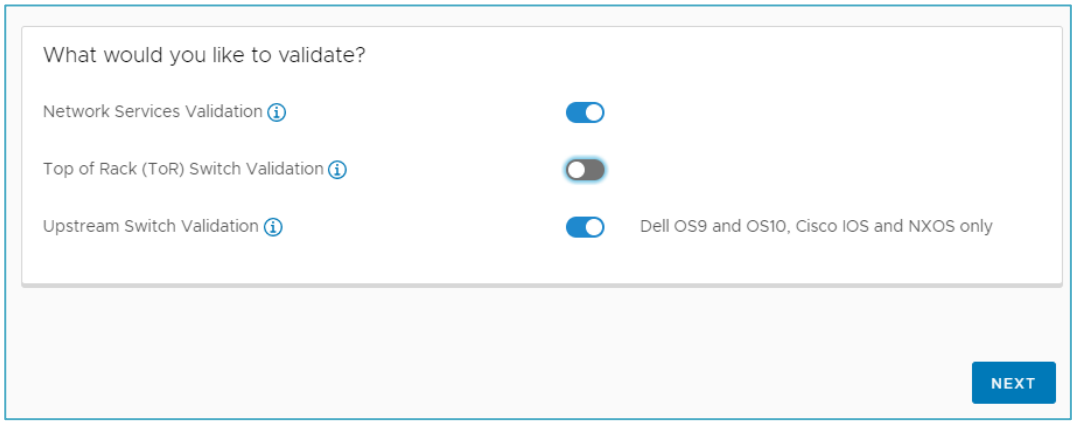

Figure 8. Home Page

1. Enable or disable the following options:
   - **Network Services Validation**—For validation using the ping utility, `nslookup` command, and so on, to validate:
     - DNS, NTP, SRS, default gateway, and IP reachability
     - DNS forward and reverse lookup
     - Reserved IP addresses are not in use
   - **Top-of-rack (ToR) switch validation**—Checks VLAN creation, port mode, permitted VLAN, port channel protocol, LACP port priority, STP mode, bridge priority, and peer link in the ToR switch. NVT requests switch output in the form of a file or access to the switch. Supported switch vendors are Dell OS9, Dell OS10, Cisco NXOS, and Cisco IOS.
   - **Upstream switch validation**—Checks VLAN creation, port mode, permitted VLAN, port channel protocol, STP mode, and bridge priority in the customer upstream switch to which the ToR will be connected. NVT requests switch output in the form of a file or access to the switch. Supported switch vendors are Dell OS9, Dell OS10, Cisco NXOS, and Cisco IOS.

Note: You are not limited to one selection. You can select a combination of these options.

2. Click **Next** to access the pages on which to enter data.

Enter data

Provide data to NVT by:

- Entering data manually
- Importing a JSON file that the VxRail PEQ generates (see Generate a JSON file)
- Importing a file that contains data input from a previous use of NVT. The **Export** button on the validation page enables you to save this data (see Run the validation).

To enter data, perform the following steps:

1. Indicate how you plan to provide data to NVT, as shown in the following figure:

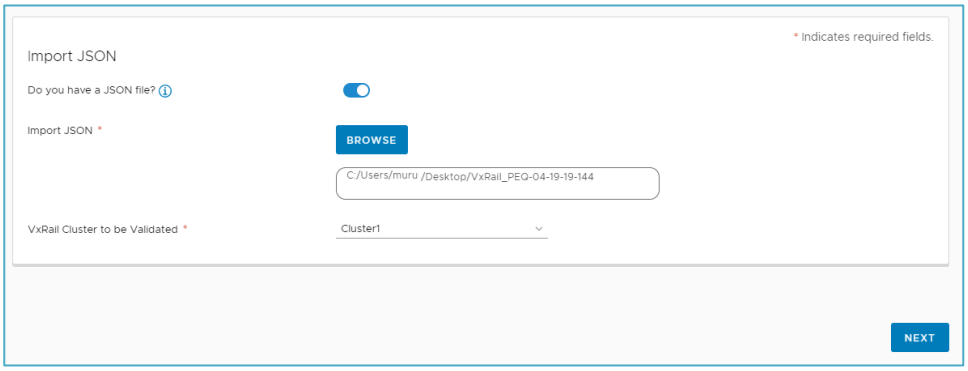

Figure 9. Import JSON window

- If you do not have a JSON file, disable **Do you have a JSON file?** Go to step 3.
- If you generated a JSON file from the VxRail PEQ or saved a file from a previous NVT session, upload it into NVT:
  a. Enable Do you have a JSON file?
  b. Click **Browse,** locate the JSON file, and then click **Open**.

     The JSON file is uploaded into NVT.

2. Click **Next**.

Note: If you upload a Universal JSON file, select the VxRail Cluster that is to be validated.

3. Complete the following pages, which guide you through the steps to enter data into NVT:
   - If you did not use a JSON file, enter the data manually.
   - If you used a JSON file, edit data or enter missing data as necessary.

   The JSON file populates most, but not all, the fields in the following pages.

Enter site information

1. From the main menu, click **Site Information**, as shown in the following figure:

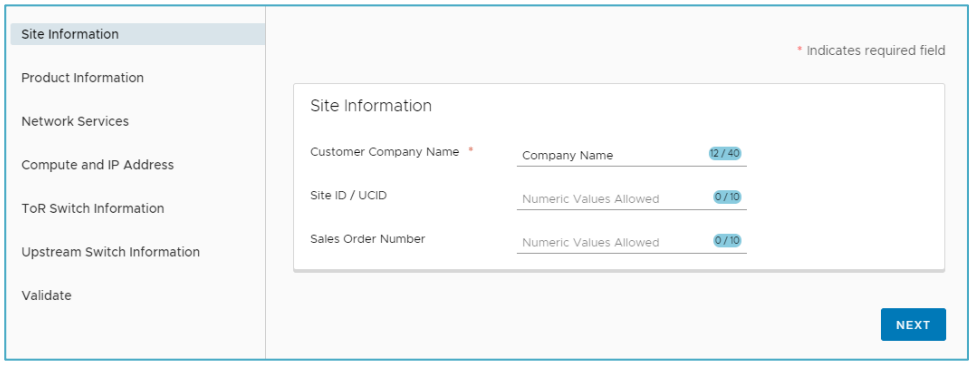

Figure 10. Site Information page

2. Enter the customer details that are described in the following table, and then click **Next**:

Table 4. Site information

Field	Description
Customer Company Name	Enter the name of the company, for example, Dell EMC. **Note:** This field is mandatory. In this version of NVT, site information is not imported from the JSON file.
Site ID or UCID	Enter the site ID or UCID of the VxRail Appliance installation.
Sales Order Number	Enter a sales order number, if applicable.

Enter product information

1. From the main menu, click **Product Information**, as shown in the following figure:

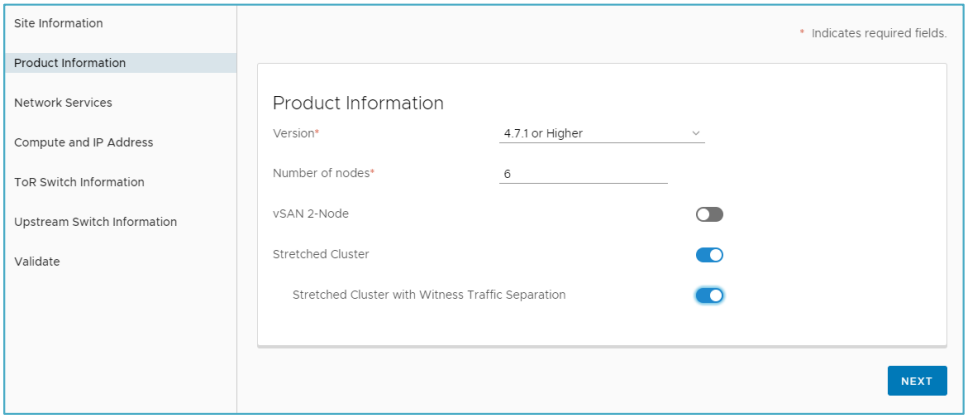

Figure 11. Product Information

2. Enter the product-related information that is described in the following table, and then click **Next**:

Table 5. Product Information fields

Field	Description
Version	Select the VxRail version (4.5.x,r 4.7.0 and 4.7.1 or Higher) from the drop-down menu.
Number of nodes	Enter the number of nodes in the VxRail cluster: 3 to 64. For vSAN, stretched cluster supported configuration is 3 + 3 + 1 to 15 + 15 + 1 (Site 1 Nodes + Site 2 Nodes + Witness).
vSAN 2-Node	Select the product version as 4.7.1 or Higher, and you see vSAN 2-Node.
Stretched Cluster	Select any product version to see the Stretched Cluster option. **Note**: Stretched Cluster and vSAN 2-Node are mutually exclusive, and thus cannot be enabled simultaneously.

Field	Description
Stretched Cluster with Witness Traffic Separation	Select version 4.7.0 or 4.7.1 or Higher and enable **Stretched Cluster**. **Note**: **Stretched Cluster with Witness Traffic Separation** switches are visible only when **Stretched Cluster** is enabled.

Enter server details

1. From the main menu, click **Network Services**, as shown in the following figure:

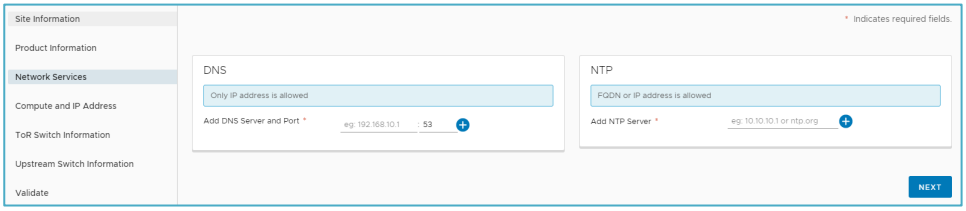

Figure 12. Network services information

2. Enter the DNS and NTP Server details that are described in the following table. Click the plus or minus icons to add or delete DNS and NTP server information.

Table 6. Network services fields

Field	Description
DNS	Enter the IP address of the DNS server. The VxRail IP address and associated hostname must be registered in the DNS server. NVT sends `nslookup` calls to the specified DNS server to verify the VxRail IP address and hostname resolution.
NTP	Enter the FQDN or IP address of the NTP server. The VxRail Appliance must reach the NTP server for time synchronization. NVT sends `w32tm`-equivalent calls to the specified NTP server to verify server accessibility.

NVT validates DNS entries against each DNS server address that is provided on this page. NVT attempts to reach the IP address or FQDN of the NTP servers and provides status after validation.

Enter compute and IP address information

1. From the main menu, click **Compute and IP Address**.
2. At the top of the page, enter the top-level domain name, for example, <*domain*>.com. This domain name is applicable to the following tabs on this page:
   - **ESXi Host Details**
   - **vCenter Details**
   - **Virtual Machine Details**
   - **Witness**

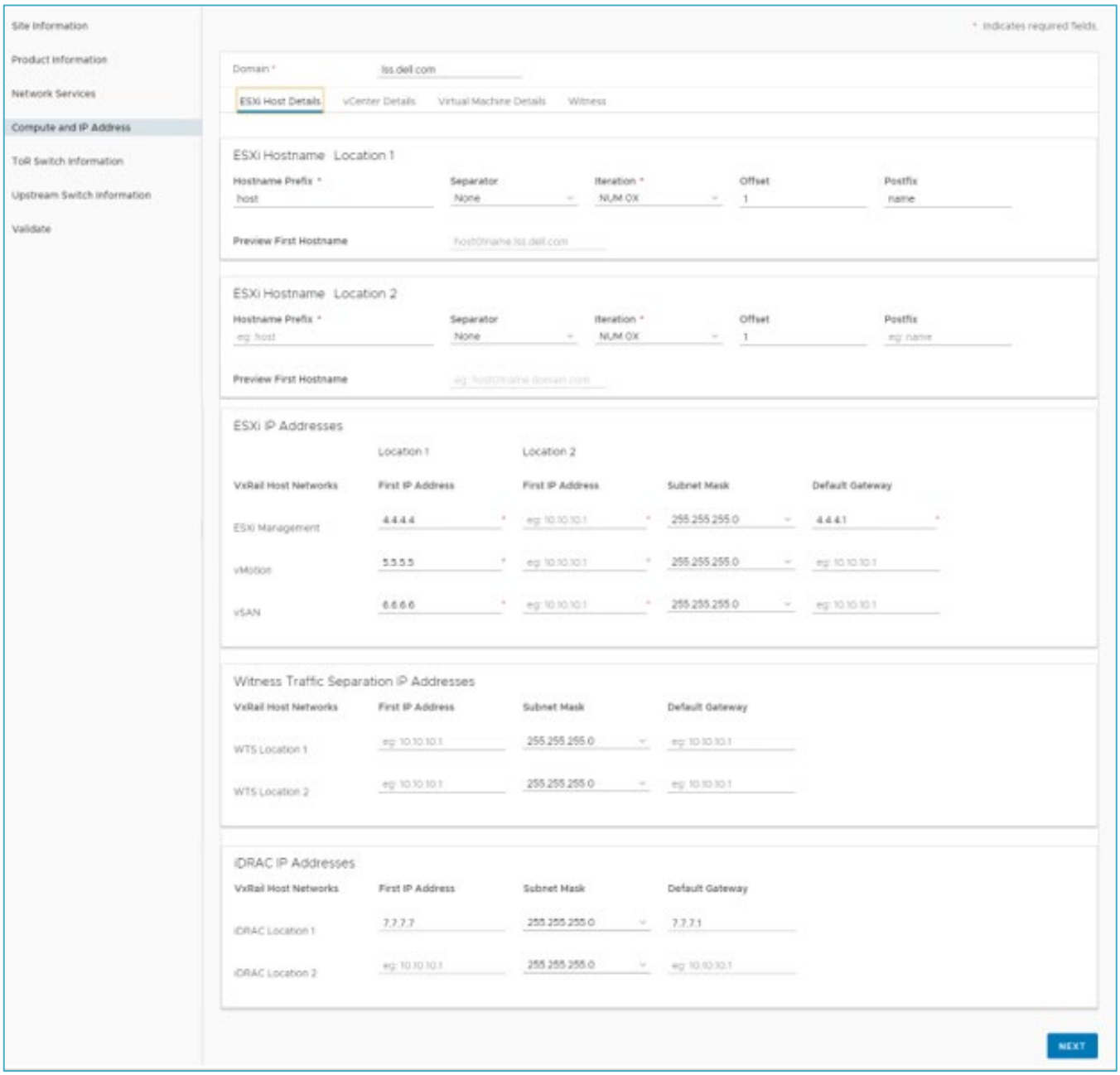

Figure 13. ESXi Host Details

3. To build the hostname of the first node, under **ESXi Hostname**, complete the fields that are described in the following table:

Table 7. Compute and IP Address

Component	Description
ESXi Host Name Location 1	
Hostname Prefix	Provide the hostname prefix.
Separator	Choose - or `None` from the drop-down list.

Component	Description
Iteration	Select one of the following from the drop-down list: • NUM X • NUM 0X • NUM 00X • NUM 000X • ALPHA
Offset	• If the selected iteration is a NUM, the offset must be a number. • If the selected iteration is Alpha, the offset automatically starts with `a`.
Postfix	Enter the postfix.
Preview First Hostname	Preview the first hostname.
ESXi Host name Location 2	The required input for the ESXi Host name location 2 is the same as for the ESXi Host name Location 1.
ESXi IP Addresses	
VxRail Host Networks	Enter the First IP address for Location 1 and Location 2, Subnet Mask, and Default Gateway for VxRail host networks: • ESXi Management • vMotion • vSAN NVT calculates the IP address/hostname for the rest of the nodes by using the number of nodes that is provided on the **Product Information** page.
Witness Traffic Separation IP Addresses	
WTS Location 1	Enter the First IP address, Subnet Mask, and Default Gateway for VxRail host networks WTS Location 1.
WTS Location 2	Enter the First IP address, Subnet Mask, and Default Gateway for VxRail host networks WTS Location 2.
iDRAC IP Addresses	
iDRAC Location 1	Enter the First IP address, Subnet Mask, and Default Gateway for VxRail host networks iDRAC Location 1.
iDRAC Location 2	Enter the First IP address, Subnet Mask, and Default Gateway for VxRail host networks iDRAC Location 2.

4. Click the **vCenter Details** tab.

   The following figure shows the required inputs if you are validating a vCenter that is internal to the VxRail appliance:

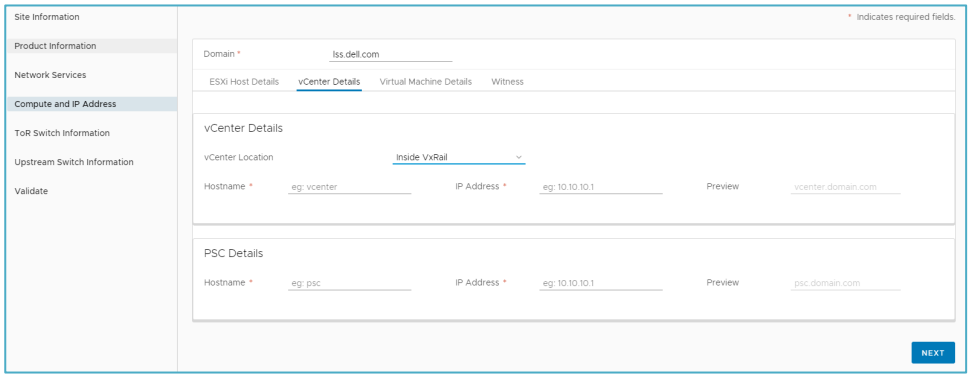

Figure 14. vCenter Details (Inside VxRail)

5. Complete the fields that are described in the following table:

Table 8. vCenter Details (Inside VxRail)

Field	Description
vCenter Location	Select **Inside VxRail.**
Hostname	Enter the vCenter hostname.
IP Address	Enter the vCenter IP address, for example, `10.10.1.1`.
Preview	Preview the vCenter FQDN.
PSC Details	
Hostname	Enter the PSC Hostname.
IP Address	Enter the PSC IP address.
Preview	Preview the PSC FQDN.

The following figure shows the required inputs if you are validating a vCenter that is external to the VxRail appliance:

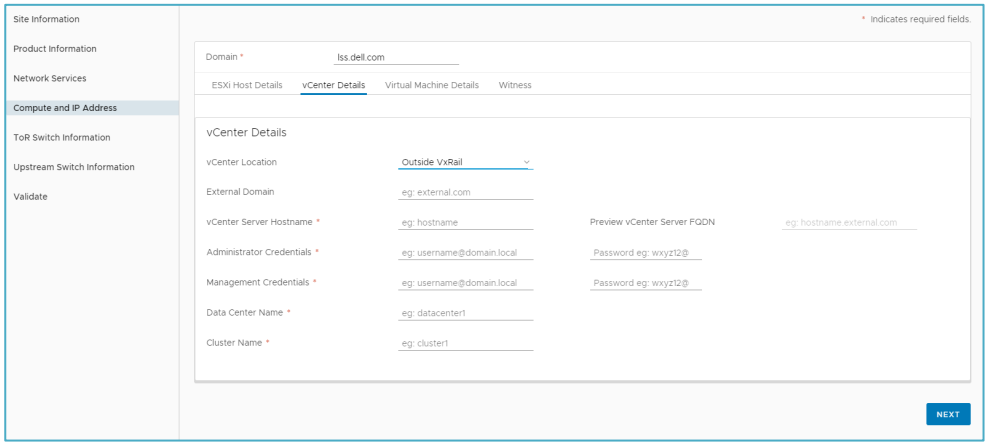

Figure 15. vCenter Details (Outside VxRail)

6. Complete the fields that are described in the following table:

Table 9. vCenter Details: Outside VxRail

Field/option	Description
vCenter Location	Select **Outside VxRail**.
External Domain	Enter the external domain name, for example, `external.com`.
vCenter Server Hostname	Enter the vCenter Server hostname.
Preview vCenter Server FQDN	Preview the vCenter server FQDN, for example, `vxrail01.abc.xyz.com`.
Administrator Credentials	Enter the administrator username and password.
Management Credentials	Enter the management username and password.
Data Center Name	Enter the existing Data Center Name, for example, `datacenter1`.
Cluster Name	Enter a new cluster name, for example, `Cluster1`.

7. Click the **Virtual Machine Details** tab, as shown in the following figure:

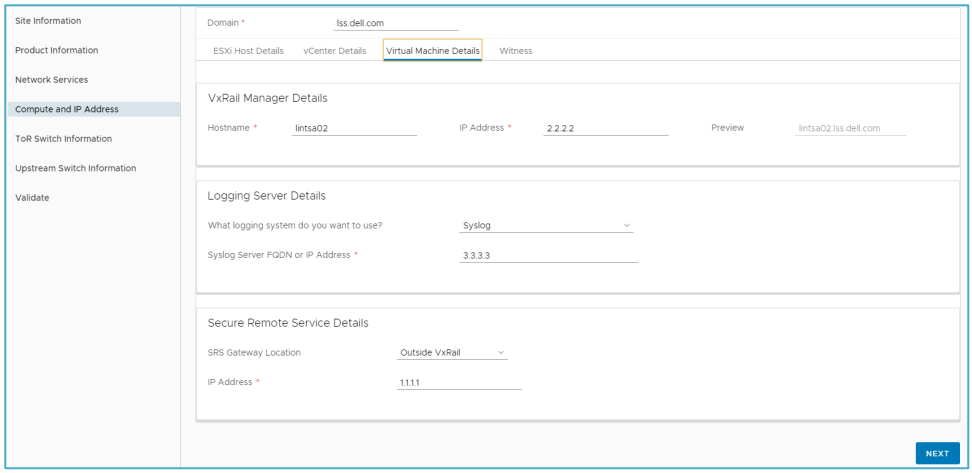

Figure 16. Virtual Machine Details

8. Complete the fields that are described in the following table:

Table 10. Virtual Machine Details

Field/option	Description
VxRail Manager Details	
Hostname	Enter the hostname for the VxRail Manager, for example, `thc02vxrsv01`.
IP Address	Enter the IP address for VxRail Manager.
Preview	Preview the VxRail Manager FQDN, that is, <*hostname*>.<*domain*>. For example, `thc02vxrsv01.pci.local`.
Logging Server Details	
What logging system do you want to use?	Select the logging, which is based on the vCenter selection, from the drop-down list. • If **vCenter Location** is **Inside VxRail**, select one of the following logging options: ▪ **vRealize Log Insight** and enter the hostname and IP address. You can preview the FQDN for vRealize Log Insight, which is <*hostname*>.<*domain*>. ▪ **Syslog** and enter the FQDN or IP address for Syslog server ▪ **None** • If **vCenter Location** is **Outside VxRail**, select one of the following logging options: ▪ **Syslog** ▪ None
Syslog Server FQDN or IP Address	Enter the IP address or FQDN for Syslog Server. For example, `vxrail01.abc.xyz.com` or `10.10.10.1`.

Field/option	Description
Secure Remote Service Details	
SRS Gateway Location	Select the location of SRS Gateway Service details from the drop-down list: • Inside VxRail • Outside VxRail • None
IP Address	Provide the IP address of the SRS server.

9. Click the **Witness** tab to capture the Witness VM details.

   The following figure shows the required inputs if you are validating a witness to the VxRail appliance:

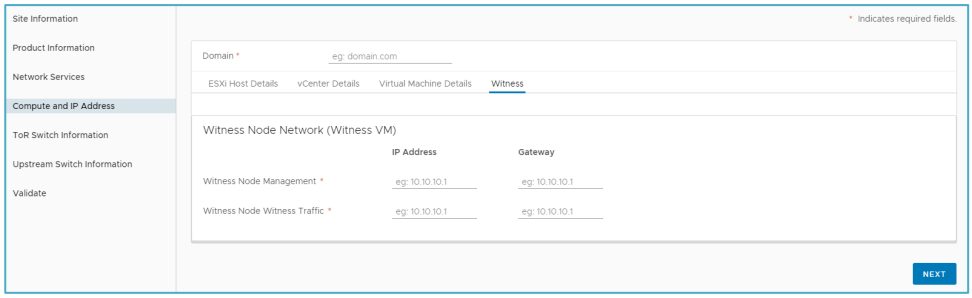

Figure 17. Witness node network (witness VM)

10. Complete the fields described in the following table:

Table 11. Witness node network (witness VM)

Field/option	Description
Witness Node Management	Enter the IP address and Gateway for Witness Node Management. For example, `10.10.10.1`.
Witness Node Witness Traffic	Enter the IP address and Gateway for Witness Node Witness Traffic. For example, `10.10.10.1`.

11. Click **Next** to go to the ToR Switch Information page.

Enter ToR Switch Information

Provide the switch output file and specify the connection. If you import a JSON file that includes the VLAN IDs, those IDs are imported. Otherwise, enter the VLAN IDs manually.

1. From the main menu, select **ToR Switch Information**, as shown in the following figure:

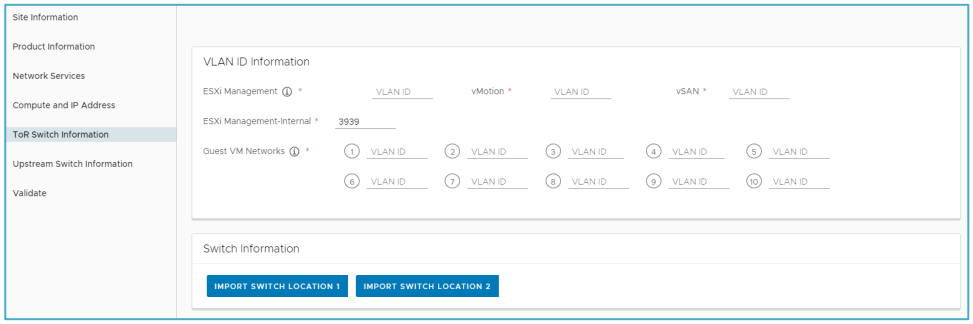

Figure 18. ToR Switch Information

2. Complete the fields that are described in the following table:

Table 12. ToR Switch Information

Field	Description
VLAN ID Information	
ESXi Management	Enter ESXi Management, vMotion, and vSAN VLAN ID as it will be configured on the switch. VLAN 0 is not valid.
ESXi Management-Internal	Provide a valid ESXi Management-Internal VLAN ID within range 1 through 4094.
Guest VM Networks	Provide Guest VM Networks VLAN IDs. **Note:** One VLAN ID is mandatory.
Witness Traffic	Provide Witness traffic VLAN ID.
Switch Information	
Import Switch	Click the **Import Switch** button to import the existing switch file. A maximum of two switches can be added.

Import existing file

The following figure shows the required inputs if you are using the switch Output file:

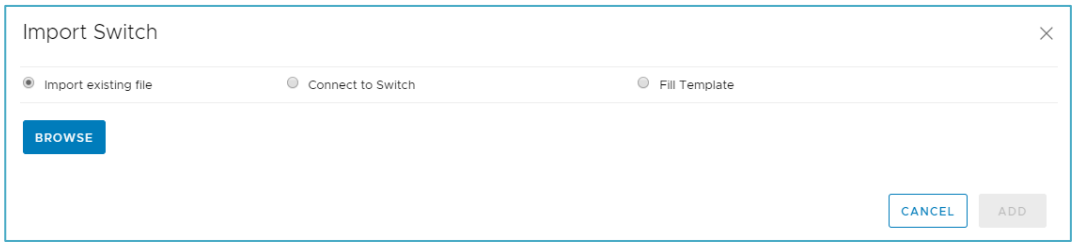

Figure 19. Import Switch

1. Complete the fields that are described in the following table:

Table 13. Import existing file

Field	Description
Switch Output File	If the radio button is selected, you can browse and upload the switch output file from the ToR switch. **Note:** Only Dell OS9, Dell OS10, Cisco IOS, and Cisco NXOS models are supported. If the file is from a supported model but not recognized, see the *Switch Output Collection Guide* in the **Documents** drop-down menu. Ensure that the selected ToR switch models are the same *within and across the sites*.

2. After uploading the switch output file, click the **Add** button. The switch output is displayed, as shown in the following figure:

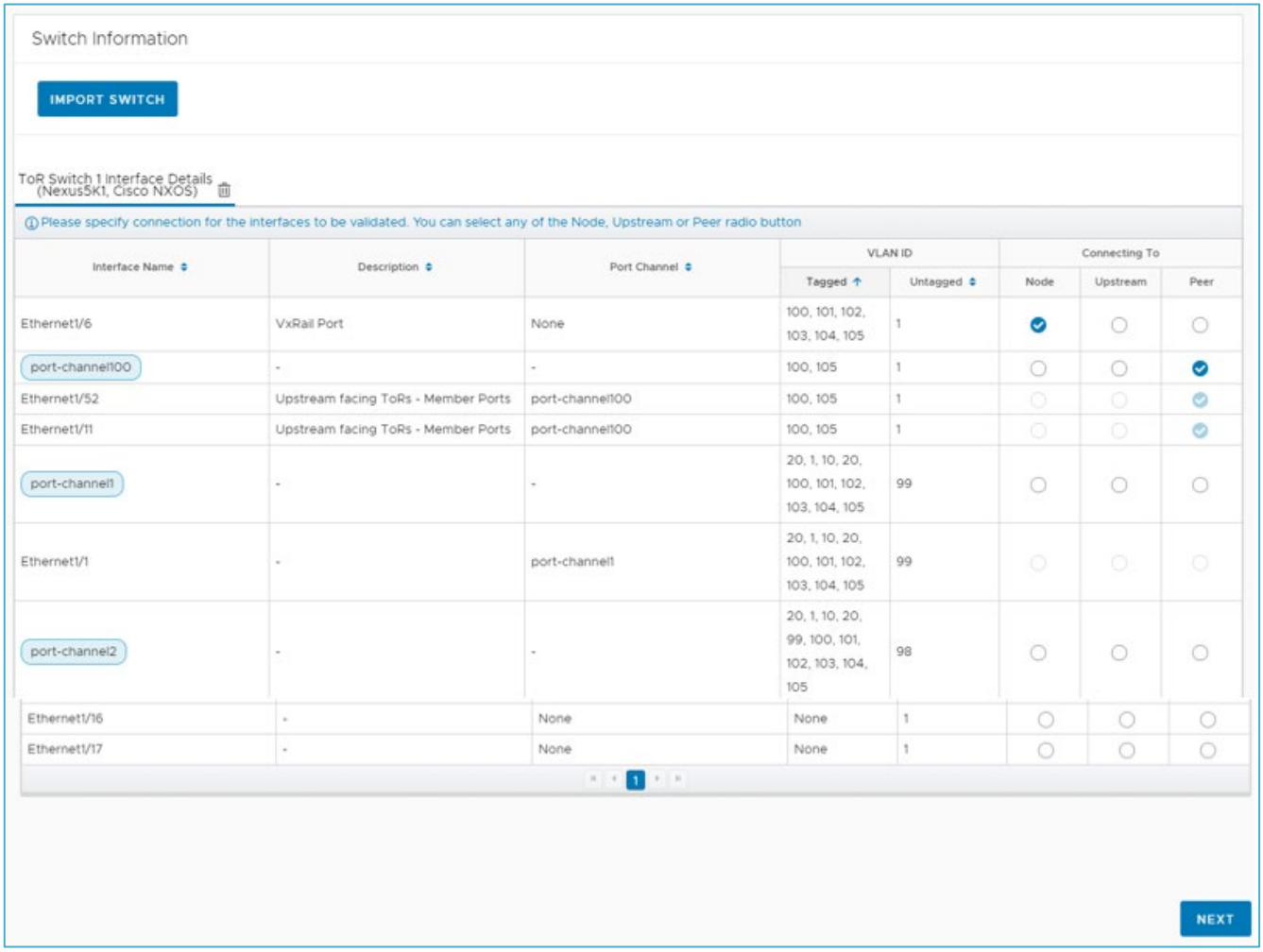

Figure 20. Specifying switch connection

3. To indicate that the interface connects to a node, upstream, or peer switch, click the radio buttons on the right.

If a port is part of a port channel, the connection shows the port channel and all the ports show the same connection.

If a port is not a part of a port channel, the connection is specified for each port.

Note: Validation is performed only for those interfaces for which a connection is specified.

Click the (trash can) icon to remove switch information.

Connect to switch

1. Click **Connect to Switch** to get the Grab Switch command output.

   Here, you can establish connection with the Switch Host.

2. Verify the host connection details and click **Run Switch Grab**, as shown in the following figure:

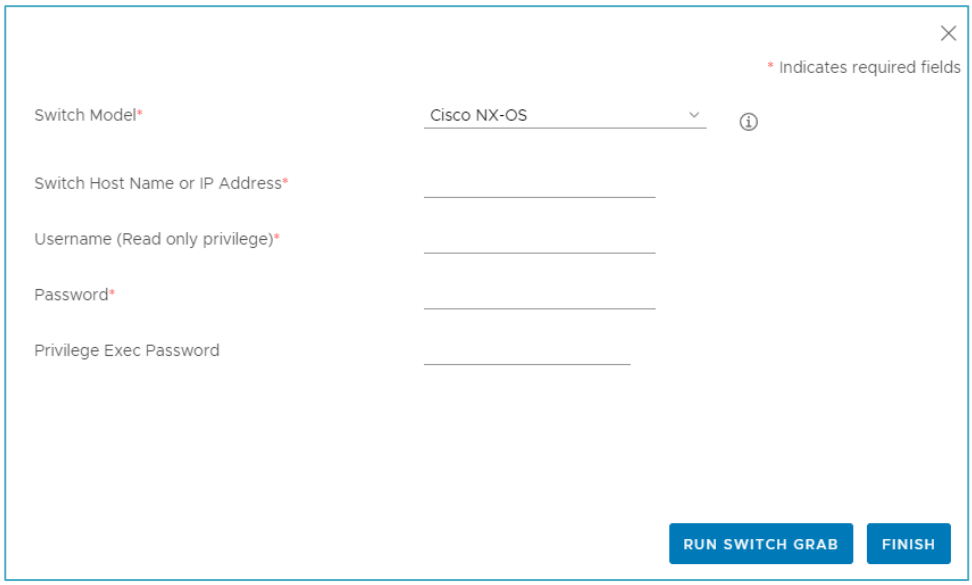

Figure 21. Connect to switch

3. Enter the Switch Grab details that are described in the following table, and then click **Finish**:

Table 14. Launching Grab Switch UI

Field	Description
Switch Model	Select any one of the appropriate switch models from the drop-down menu: ▪ Cisco NX-OS ▪ Cisco IOS ▪ Dell OS9 ▪ Dell OS10 Commands used for the selected Model: Dell OS9 and Dell OS10 – 'show version' and 'show running-config' Cisco IOS and Cisco NX-OS – 'show version', 'show vlan' and 'show running-config'
Switch Host Name or IP Address	Use the hostname or IP address to set the name of the switch.
User Name (Read-Only privilege)	Provide a username that uniquely identifies someone on a system.
Password	Enter the correct password to verify the identity of a user.
Privilege Exec Password	This password protection lets you restrict access to a network.

Fill template

1. Click **Fill Template** to add switch output to the template file, as shown in the following figure:

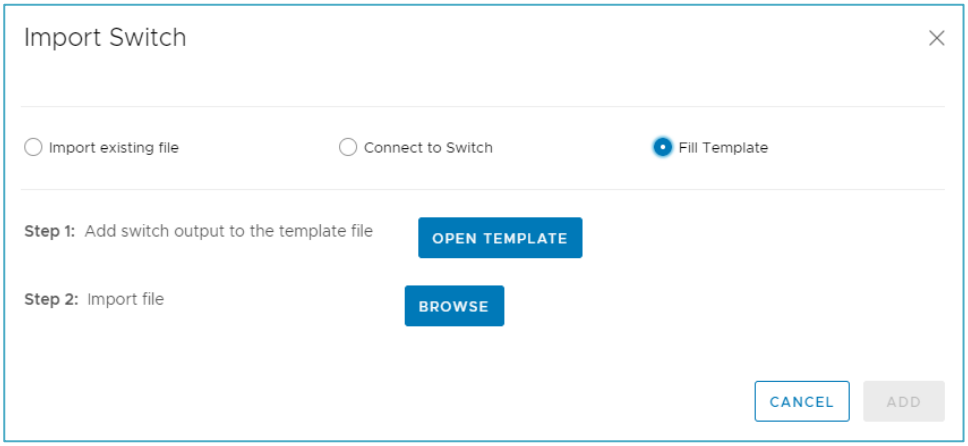

Figure 22. Fill template

2. Complete the fields described in the following table:

Table 15. ToR Switch Output Information

Field/option	Description
Add switch output to the template file	The user can open/update the switch template file to provide the Switch Output File by replacing the command output in switch template file.
Import file	Browse and upload the updated template file. **Note**: The only accepted files are Switch grab output file and the Switch Grab Template, manually populated with switch output and the '`show tech-support`" command output.

Open template

The user can locate each supported switch template in a folder.

The user must manually populate the switch command output in the template. Switch command output needs to be collected from the respective switches.

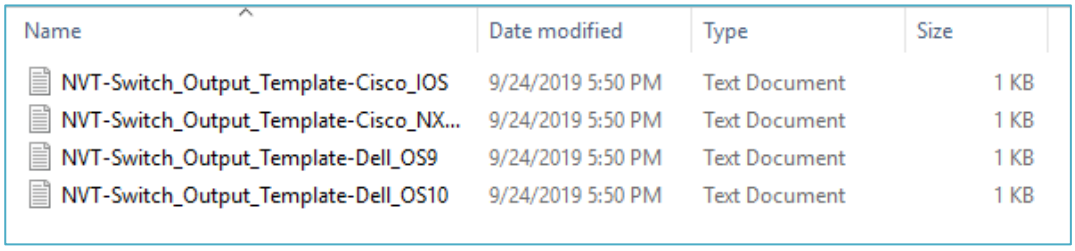

Figure 23. Open switch template

Enter upstream switch information

Validate ESXi Management and Guest VM Network VLANs for upstream switches.

1. From the main menu, click **Upstream Switch Information**, as shown in the following figure:

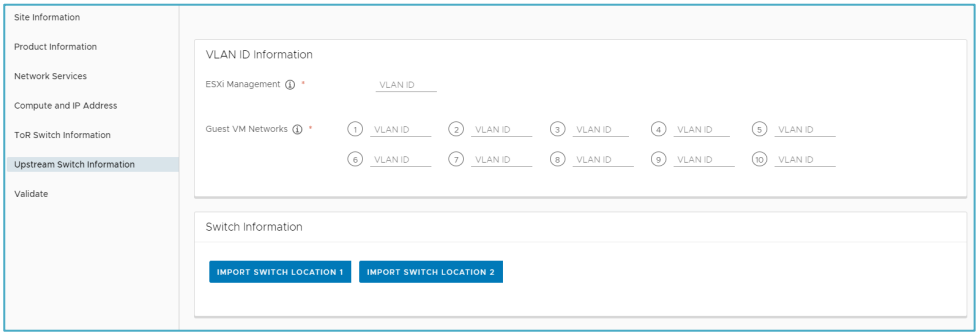

Figure 24. Upstream switch information

The required input for the **Upstream Switch Information** page, and how to provide the switch output file and connections, is the same as for the **ToR Switch Information** page.

2. For information about completing this page, see Enter ToR Switch Information.

Run the validation

Run the validation with or without switch output files. If you do not provide switch connection information or load switch output files, validations that are related to switches do not run.

From the main menu, click **Validate**, as shown in the following figure:

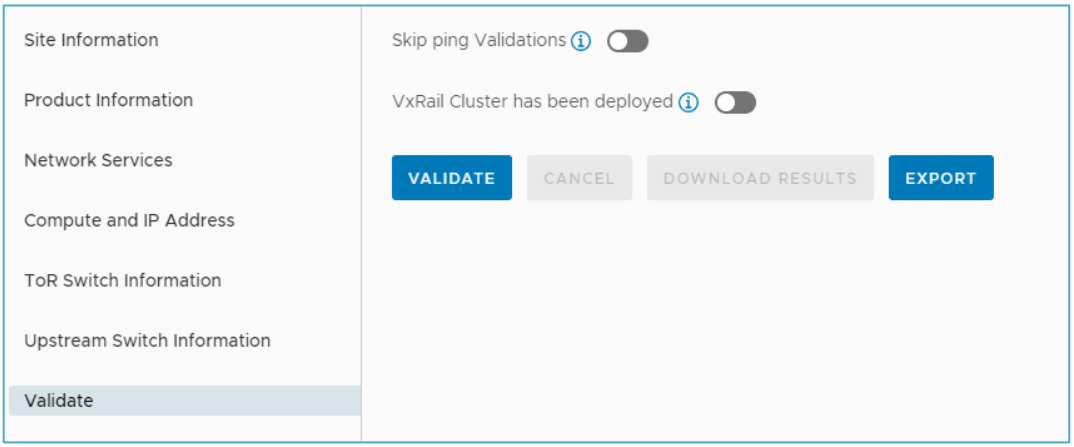

Figure 25. Validation page

The following table describes the functions of each of the buttons that are displayed:

Table 16. Validation button functions

Button	Function
Skip ping Validations	Enable this toggle button before clicking the **VALIDATE** button to skip all the ping tests that test the availability or reachability of the IP address. **Note**: Skip *IP availability* validations and *IP reachability* ping validations. You may want to enable this if a firewall block pings or if pings were previously validated.
VxRail Cluster has been deployed	Enable this toggle button before clicking the **VALIDATE** button for Post deployment IP reachability validations. **Note**: For IP address on the VxRail Cluster, enabling this option changes the *IP availability* validations to *IP reachability* validations.
VALIDATE	To run the validation. The progress bar displays the percentage of the process that is complete and an estimate of the time remaining.
CANCEL	To cancel the validation process.
DOWNLOAD RESULTS	After validation is complete, click this button to generate a report in Excel format.
EXPORT	Click this button to save the JSON file for use when you open NVT again.

Note: If you change any fields, click **VALIDATE** to refresh the results.

After the validation is complete, you can see the validation summary chart, as shown in the following figure:

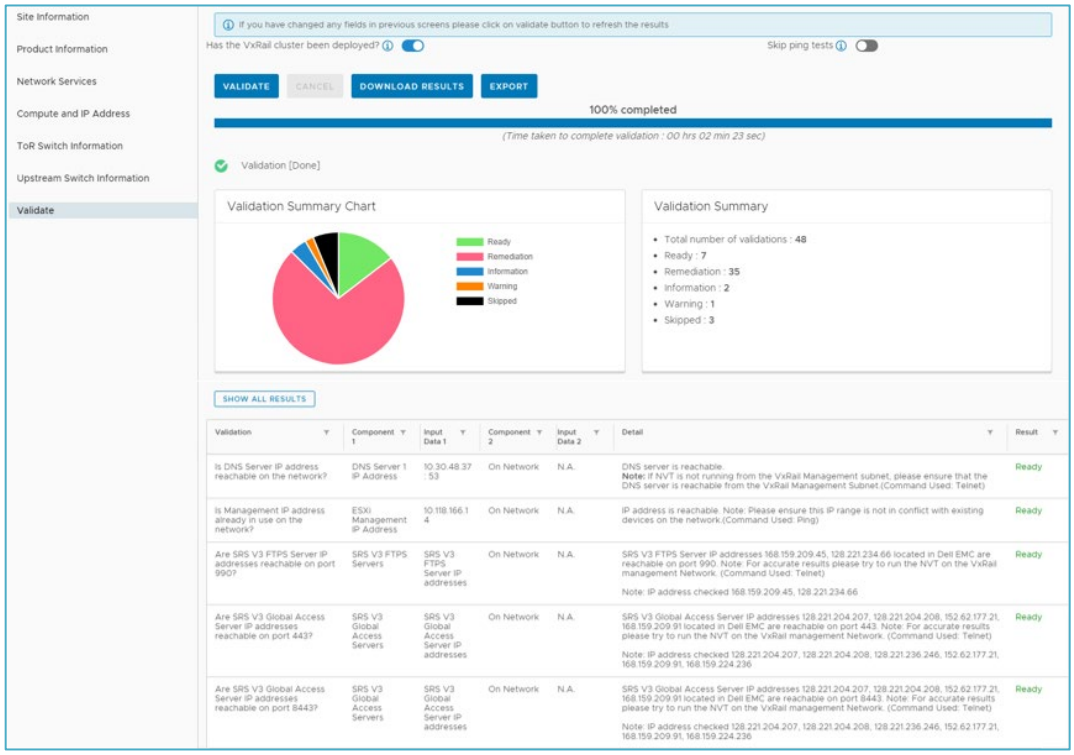

Figure 26. Validation Summary Chart

Validation results include:

- **Ready**—Indicates that the specified configuration follows Dell EMC guidelines for VxRail deployment.
- **Remediation**—Indicates that the specified configuration does not follow Dell EMC guidelines for VxRail deployment. The deployment will not be successful.
- **Information**—Shows configuration information such as STP mode and bridge priority for switches.
- **Warning**—Indicates that the specified configuration does not follow Dell EMC guidelines for VxRail deployment. The deployment might be successful, but the configuration does not use the recommended settings.
- **Skipped**—Indicates that validation was skipped. For example, when an incorrect log file is uploaded for the selected model, the validation results shows that no log file has been uploaded to either the ToR or the upstream page.

Note: The filtering search tool ( ) restricts the search to a certain section of a validation.

Contact Us

For technical support:

- Send an email with diagnostic data to TS_Tools_Support@emc.com.
- Go to Central Help & Support.
- Open a support ticket from Central Help & Support Request Support.

To collect required files for troubleshooting, click **Diagnostic Data** under **Contact Us** on the Masthead Navigation. Send these files to the support team.

Frequently Asked Questions (FAQs)

Where are the log files located?

The default log is at `%AppData%\Roaming\Network Validation Tool for VxRail\logs`. Before contacting support, click **Diagnostic Data** under **Contact Us** on Masthead Navigation.

How do I check NVT-related processes from Windows Task Manager?

Look for **Network Validation Tool for VxRail** in Windows Task Manager.

Does NVT support Application Centric Infrastructure (ACI)?

Currently, you can run NVT, but it validates only the network services and not the ACI fabric.

Is the NVT secure?

The Global Security Office audits all Dell EMC software to ensure that it has no vulnerabilities. The software does not require administrator rights, does not share data, and performs only read-only activities.

References

Dell EMC documentation

The following Dell EMC documentation provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell EMC representative.

- VxRail Networking Solutions at Dell EMC Networking Guides
- *Dell EMC VxRail Network Guide*

Appendix: Tested switch models and operating systems

NVT supports Dell EMC OS9 and OS10, and Cisco NX-OS and IOS switches. The following table lists the switch models and operating systems used for laboratory testing for NVT versions 4.0.400, 4.5, and 4.7:

Table 17. Laboratory switches

Vendor	Switch model	Switch operating system	Switch application
Dell EMC	S4048T-ON	Dell Operating System Version: 2.0	Dell Application Software Version: 9.10 (0.1P6)
Cisco	Cisco Nexus5548 chassis	Cisco Nexus Operating System (NX-OS)	Software • BIOS: Version 3.6.0 • Loader: Version N/A • Kick start: Version 5.2(1) N1(4) • System: Version 5.2(1) N1(4)
Cisco	WS-C3850-12XS	Cisco IOS software, IOS-XE software, Catalyst L3 Switch software	Version 03.07.04E RELEASE SOFTWARE (fc1)