Brocade® SANnav™ Management Portal Installation and Migration Guide, 2.1.0x

Installation Guide
28 August 2020

Table of Contents

Copyright Statement

Copyright © 2020 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Brocade, the stylized B logo, Fabric OS, and SANnav are among the trademarks of Broadcom in the United States, the EU, and/or other countries. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, to view the licensing terms applicable to the open source software, and to obtain a copy of the programming source code, please download the open source disclosure documents in the Broadcom Customer Support Portal (CSP). If you do not have a CSP account or are unable to log in, please contact your support provider for this information.

Introduction

About This Document

This guide contains detailed steps for installing SANnav™ Management Portal and for migrating from an earlier version of SANnav. The guide also includes information about installing SANnav as an OVA appliance.

Quick installation checklists are provided for users who are familiar with SANnav installation. See SANnav Installation and Migration QuickStart Checklists.

Refer to the following guides for additional information:

- *Brocade SANnav Management Portal User Guide* describes how to monitor and manage your storage area network (SAN) using Brocade SANnav Management Portal.
- *Brocade SANnav Flow Management User Guide* explains how to configure and manage flows using SANnav Management Portal.
- *Brocade SANnav Management Portal REST API and Northbound Streaming Reference Manual* contains definitions of REST APIs you can use to access SANnav Management Portal, including streaming performance and flow metrics to an external server.
- *Brocade SANnav Global View User Guide* describes how to use SANnav Global View to monitor and manage multiple Management Portal instances. SANnav Global View is a separate product.
- *Brocade SANnav Management Portal Release Notes* includes a summary of the new, unsupported, and deprecated features for this release.

Contacting Technical Support for Your Brocade® Product

If you purchased Brocade product support from a Broadcom OEM/solution provider, contact your OEM/solution provider for all your product support needs.

- OEM/solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information on this option, contact Broadcom or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.

For product support information and the latest information on contacting the Technical Assistance Center, go to https://www.broadcom.com/support/fibre-channel-networking/. If you have purchased Brocade® product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7.

Online	Telephone
For nonurgent issues, the preferred method is to log in to myBroadcom at https://www.broadcom.com/mybroadcom. (You must initially register to gain access to the Customer Support Portal.) Once there, select **Customer Support Portal** > **Support Portal**. You will now be able to navigate to the following sites: • **Knowledge Search**: Clicking the top-right magnifying glass brings up a search bar. • **Case Management**: The legacy MyBrocade case management tool (MyCases) has been replaced with the Fibre Channel Networking case management tool. • **DocSafe**: You can download software and documentation. • **Other Resources**: Licensing Portal (top), SAN Health (top and bottom), Communities (top), Education (top).	Required for Severity 1 (critical) issues: Please call Fibre Channel Networking Global Support at one of the numbers listed at https://www.broadcom.com/support/fibre-channel-networking/.

Document Feedback

Quality is our first concern. We have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission or if you think that a topic needs further development, we want to hear from you. Send your feedback to documentation.pdl@broadcom.com. Provide the publication title, publication number, topic heading, page number, and as much detail as possible.

SANnav Installation and Migration QuickStart Checklists

These checklists are provided for experienced users who are familiar with SANnav installation. For all other users, start with Installation Overview.

Installation Checklist

The following table provides a quick checklist for installing SANnav.

#	Item	Description
1	Ensure that your server meets the requirements for SANnav installation. Upgrade the OS if you are running an unsupported version.	System and Server Requirements for SANnav Management Portal
2	Review and comply with the installation prerequisites.	Installation Prerequisites
3	Ensure that the required ports are open in the firewall.	Firewall Requirements for SANnav Management Portal
4	Configure the firewalld backend if you are using CentOS / RHEL 8.0 or higher.	Configuring the Firewalld Backend for CentOS and RHEL 8.0 or Higher
5	Download the SANnav software package to the folder where you want to install the application.	NOTE: Do not create the SANnav installation folder with a space in the name; otherwise, installation will fail.
6	Untar the .gz file.	`tar -xvzf <package_name>.gz` The resulting directory is referred to as <install_home> throughout the rest of the checklists.
7	Install SANnav.	`<install_home>/bin/install-sannav.sh`
8	Check the server status.	`<install_home>/bin/check-sannav-status.sh`

Migration Checklist

The following table provides a quick checklist for migrating from an earlier version of SANnav.

#	Item	Description
1	Back up the current SANnav installation before you start the migration process.	Refer to the *Brocade SANnav Management Portal User Guide* for instructions.
2	Ensure that your server meets the requirements for SANnav installation. Upgrade the OS if you are running an unsupported version.	System and Server Requirements for SANnav Management Portal
3	Review and comply with the installation prerequisites.	Installation Prerequisites
4	Ensure that the required ports are open in the firewall.	Firewall Requirements for SANnav Management Portal
5	Configure the firewalld backend if you are using CentOS / RHEL 8.0 or higher.	Configuring the Firewalld Backend for CentOS and RHEL 8.0 or Higher
6	Download the SANnav software package to the folder where you want to install the application.	NOTE: Do not create the SANnav installation folder with a space in the name; otherwise, installation will fail.
7	Untar the .gz file.	`tar -xvzf <package_name>.gz`

#	Item	Description
8	Install SANnav.	`<install_home>/bin/install-sannav.sh`
9	Check the server status.	`<install_home>/bin/check-sannav-status.sh`

SANnav OVA Installation Checklist Using vCenter

The following table provides a quick checklist for installing SANnav as an appliance using vCenter.

#	Item	Description
1	Review and comply with the installation prerequisites.	Installation Prerequisites for the SANnav Management Portal Appliance
2	Download SANnav OVA (.ova file) to the location from which you want to import to ESXi / vCenter.	The time taken to deploy SANnav OVA to the host depends on the network speed between the location to which the OVA is downloaded and the ESXi.
3	Deploy the SANnav OVA package.	Log in to vCenter and deploy the OVF template. Refer to Installing the SANnav Management Portal Appliance Using vCenter.
4	Power on the VM, and then log in as "sannav" user.	When SANnav OVA is deployed, it configures the network of the VM and makes customizations based on user input. After successful network configuration, the VM reboots. Wait for the VM to reboot before logging in.
5	Install SANnav.	After you log in to the VM, the SANnav installation script starts automatically.
6	Check the server status.	`<install_home>/bin/check-sannav-status.sh`

SANnav OVA Installation Checklist Using ovftool

The following table provides a quick checklist for installing SANnav as an appliance using `ovftool`.

#	Item	Description
1	Review and comply with the installation prerequisites.	Installation Prerequisites for the SANnav Management Portal Appliance
2	Download SANnav OVA (.ova file) to the location from which you want to import to ESXi / vCenter.	The time taken to deploy SANnav OVA to the host depends on the network speed between the location to which the OVA is downloaded and the ESXi.
3	Download `ovftool`.	You can download this free tool from https://code.vmware.com/web/tool/4.3.0/ovf.
4	Deploy the SANnav OVA package.	Run the `ovftool` command. Refer to Installing the SANnav Management Portal Appliance Using ovftool.
5	Wait for the VM to come online, and then log in as "sannav" user.	When SANnav OVA is deployed, it configures the network of the VM and makes customizations based on user input. After successful network configuration, the VM reboots. Wait for the VM to reboot before logging in.
6	Install SANnav.	After you log in to the VM, the SANnav installation script starts automatically.
7	Check the server status.	`<install_home>/bin/check-sannav-status.sh`

Installation Overview

The SANnav application uses a script-based installation. You must run the scripts that are provided in the `<install_home>` directory to install the application. All the scripts for the SANnav application must be executed in the bash shell.

NOTE
SANnav Management Portal and SANnav Global View are two different software products. You cannot install both software products on the same physical host or virtual machine (VM). You can, however, install Management Portal and Global View on different VMs in the same host, if the host has enough resources.

NOTE
For switches that are running Fabric OS versions lower than 8.2.2, port 22 is required for SANnav Management Portal to use the internal firmware repository and SCP and SFTP servers. See Installation Prerequisites for additional details.

If there is a firewall between the client and the server or between the server and the SAN, you must open a set of ports for SANnav to function properly. The list of ports is provided in Firewall Requirements for SANnav Management Portal.

If the installation script detects that an earlier version of SANnav is running, you are prompted whether you want to migrate your data to the new version.

After installation, if you choose to move SANnav from one server or VM to another, you must first release the current license. This process is called rehosting a license. Refer to the *Brocade SANnav Management Portal User Guide* for details.

Migration Overview

If you are upgrading SANnav from a previous version, the installation script provides the option of migrating your data. Migrating allows you to keep all user-configured data, customized data, and historic data (such as port performance metrics and events) when you upgrade to the latest SANnav version.

Other than being prompted to migrate your data, the migration steps are the same as the installation steps.

When you migrate the data, the following occurs:

- Installation settings (such as port customizations) from the previous installation are preserved. The installation does not prompt you for these settings.
- The license is carried forward to the new installation. After migration, you do not need to apply a new license. If the license is a trial license, after migration the license is valid for the remaining days of the trial period. If the license has expired, the migration is allowed, but you cannot use the new version until you apply a new license.
- The discovered fabrics are rediscovered.
- User-configured data, customized data, and historic data (such as port performance metrics and events) are migrated.
- Imported firmware files and switch SupportSave data are migrated.
- Data-streaming-enabled switches that were streaming data before the migration continue to stream data after migration within 10 minutes of the SANnav server startup.

Note that the following are *not* migrated:

- Capture SuportSave and Maintenance Mode event action policies.
- Events filters (Events and Violations). Note that saved inventory filters are migrated.
- Support data collection files.
- SupportSave files.

Migration Prerequisites

Before you migrate to the new SANnav version, review the following prerequisites.

- Back up SANnav.
  Refer *to the Brocade SANnav Management Portal Use*r Guide for instructions.
- Ensure that the seed switches for discovered fabrics have not reached end of support (EOS).
  If a seed switch has reached end of support, after migration the fabric is unmonitored permanently with the discovery status `Unmonitored: Seed switch is no longer supported`. In this case, you must delete the fabric and rediscover it with a different seed switch. To avoid this scenario, change the seed switch to a supported switch before migration.

OS Upgrade Options

SANnav 2.1.0 and higher do not support RHEL or CentOS 7.6 and lower. If you are running one of these unsupported operating systems and want to migrate to SANnav 2.1.0x, you must first upgrade the OS to one of the supported versions. You cannot migrate SANnav and the OS simultaneously. See Upgrading the OS with SANnav Installed.

Migration Paths

You can migrate from the two previous versions. You cannot migrate from an earlier release to SANnav OVA. The following table lists the software versions and whether migration is supported.

Table 1: SANnav Management Portal Supported Migration Paths

Current Version	Migration Version	Supported?
SANnav 1.1.0x	SANnav 2.1.0x	No
SANnav 1.1.1x	SANnav 2.1.0x	Yes
SANnav 2.0.0x	SANnav 2.1.0x	Yes
SANnav 2.1.0	SANnav 2.1.0a	Yes
SANnav 2.1.0 OVA installation	SANnav 2.1.0a OVA installation	No
SANnav VM or bare metal installation	SANnav OVA installation	No

Starting in SANnav Management Portal 2.1.0, multi-node installation is not supported. If you are migrating from a multi-node installation, first take a backup of the server and restore it to a single node, and then migrate to 2.1.0.

The following table lists various system configurations and whether migration is supported.

Table 2: Supported System Configuration Paths

Current Deployment	Migration Deployment	Supported?
Single-node	Single-node (same host)	Yes
Multi-node	Multi-node (master node, same host)	No
Single-node	Multi-node	No
Multi-node	Single-node	Yes*

*Back up and restore to single-node before migrating.

Upgrading the OS with SANnav Installed

You can upgrade the OS after SANnav is installed using Yellowdog Updater, Modified (YUM) on the same host where SANnav is running. First, stop the SANnav services, perform the upgrade, and then start SANnav services.

NOTE
The YUM upgrade will upgrade to the latest version of the OS.

The following steps apply whether you are upgrading Red Hat Enterprise Linux (RHEL) or CentOS.

1. Go to the `<install_home>/bin` folder and run the following script:

   ```
   ./stop-sannav.sh
   ```

2. Perform the YUM upgrade to the new OS version.

   ```
   yum upgrade -y
   ```

3. Go to the `<install_home>/bin` folder and run the following script:

   ```
   ./start-sannav.sh
   ```

Upgrading the SANnav Internal SFTP/SCP Server SSH Key

SANnav runs its own internal SFTP/SCP server. The SSH key for this server is generated during installation. In SANnav 2.1.0 and earlier versions, this key is a DSA key with a length of 1024 bits. Starting in SANnav 2.1.0a, this key is changed to an RSA key with a length of 2048 bits.

Migration to SANnav 2.1.0a or higher does not replace the existing key from previous installations. After migration, SANnav 2.1.0a or higher still has the old DSA key.

Although not mandatory, it is recommended that you upgrade the SSH key from the old DSA key to the new RSA key for increased security.

For switches running older Fabric OS versions, you must also delete the SSH key of the known host (the SANnav server). Switches that are running the following Fabric OS versions require you to delete the host key:

- Fabric OS 8.2.2, 8.2.2a, and 8.2.2b
- Fabric OS 8.2.1 through 8.2.1d
- Fabric OS 7.4.x

Perform the following steps after you have migrated to SANnav 2.1.0a.

1. Generate a new SSH key on the SANnav server.

   Go to the `<install_home>/bin` folder, and run the following script:

   ```
   ./delete-ssh-key.sh
   ```

   This script stops the SANnav server, deletes the old SSH key pair, and starts the server. A new key pair is generated when the switch Supportsave or firmware download operation is initiated from SANnav.

2. Delete the host key on all switches that are running older Fabric OS versions, as listed previously.
   a) Log in to the switch.
   b) Enter the `sshutil delknownhost` command.

      To delete a specific SANnav server IP address:

      ```
      switch:username> sshutil delknownhost
      IP Address/Hostname to be deleted: <IP address>
      Known Host deleted successfully.
      ```

      To delete all server IP addresses:

      ```
      switch:username> sshutil delknownhost -all
      This Command will delete all the known host keys.
      Please Confirm with Yes(Y,y), No(N,n) [N]: Y
      All known hosts are successfully deleted.
      ```

SANnav Management Portal Deployment

During SANnav Management Portal installation, you are prompted several times to accept default values or provide customized values for various settings. If you are migrating from an earlier version of SANnav, you are not prompted for these customizations, and the settings from the previous installation remain in effect.

The following table lists the installation customization options.

Table 3: SANnav Installation Customizations

Item	Description
Docker installation directory	The default home directory for installing Docker is `/var/lib/docker`, but you can change this to another directory.
Swap space	SANnav requires 16GB swap space. • If there is not enough swap space, the installer prompts you to provide a location in which to create the remainder of the swap space. • If there is no swap space, the installer prompts you to provide a location in which to create the full 16GB of swap space..
IPv6 capability	The default is IPv4 communication between SANnav and the SAN switches. If you have IPv6-capable switches in your data center, you can configure SANnav to use IPv4 and IPv6 communication.
HTTP port 80 to HTTPS redirection	Choose to allow or disallow port 80 to be redirected to port 443 (default) or to another port that you can customize. If you disallow port 80 redirection, the web browser times out when pointed to port 80 and must be explicitly pointed to port 443 or the customized port to be able to log in to SANnav.
Server-to-switch communication protocol	Select an option to configure HTTP or HTTPS connections between SANnav and the SAN switches: • 0 for HTTP (Insecure communication.) • 1 for HTTPS (Secure communication. Requires that you have an IP-provided SSL certificate or self-signed certificate and that your switches are configured for HTTPS.) • 2 for HTTPS then HTTP (First HTTPS is tried, and if that fails, HTTP is used.)
Single sign-on (SSO) options when launching Web Tools	If you launch Web Tools from the SANnav application, SANnav prompts you to provide switch login credentials. You can configure SANnav to automatically log in to the switch when launching Web Tools for switches running Fabric OS 9.0.0 or higher. • 0 for always log in manually. SANnav prompts you for switch login credentials. • 1 to log in with switch credentials. SANnav does not prompt you, but attempts to log in to the switch using the credentials that SANnav used when discovering the switch. • 2 to log in with user credentials. SANnav does not prompt you, but attempts to log in to the switch using the credentials that the user used when logging in to SANnav. For switches running Fabric OS versions earlier than 9.0.0, SANnav always prompts you to log in to the switch when launching Web Tools, regardless of the SSO settings.

Item	Description
Port customization	You can customize ports when installing SANnav Management Portal. To use a default port, that port must be unused and available. The following is the list of default values: • SSH server port is 22. • Client-to-server HTTPS port: Default HTTPS port is 443. • SNMP trap: Default SNMP trap port is 162. • Syslog port: Default syslog port is 514. • Secure syslog port: Default secure syslog port is 6514. **Note:** If you are installing SANnav in IPv6 mode, the following ports are reserved for internal communication. Do not use any of these ports for customization: 5432, 6060, 6061, 7021, 7022, 7051, 7052, 7053, 7054, 7055, 7056, 7060, 7072, 7080, 7082, 7087, 7088, 7089, 7090, 7096, 7099, 7890, 7997, 8021, 8022, 8081, 8082, 8083, 8085, 8200, 9022, 9090, 9091, 9100, 9101, 9200, 9443, 12181, 18081, 19093, 19094, and 19095.
Database password	You can change the default SANnav database (Postgres database) password. You are given the option to proceed with the installation using the default password or to choose a new password for the SANnav database. The default password is "passw0rd" (where 0 is a zero).
SCP/SFTP password	You can change the default SANnav Management Portal SCP/SFTP password. You are given the option to proceed with the installation using the default password or to choose a new password for the SANnav internal SCP/SFTP server. The default password is "passw0rd" (where 0 is a zero).
License auto-renewal	By default, SANnav is configured to automatically retrieve and activate a renewal license when the license expires. You can deactivate automatic license renewal, in which case you must manually apply the license yourself.
Allowing data collection to be sent to Broadcom	SANnav collects usage data for the application. You can decide whether SANnav sends the data to Broadcom to improve user experience in the future.

System and Server Requirements for SANnav Management Portal

You must meet all the system and server requirements before you start the SANnav Management Portal installation.

The following table lists the system and server requirements for deployment of SANnav Management Portal.

> **NOTE**
> The disk space requirement that is listed in the table is for SANnav only. Be sure to account for additional space required by the operating system, for saving files, and for SANnav TAR files and extracted files.

The disk space can be from a direct-attached disk or through a network-mounted disk.

- The default home directory for installing Docker is `/var/lib/docker`, but you can choose another location during installation. Docker must be installed on a local disk.
- The default swap space directory is the "/" directory. If the directory does not have enough space, you can choose a different location during installation.

The required number of CPU cores should be equally distributed over the sockets.

Table 4: System and Server Requirements for SANnav Management Portal Installation

Requirement	Base License or Enterprise License with up to 3000 Ports	Enterprise License with up to 15,000 Ports
Operating system	• Red Hat Enterprise Linux (RHEL): 7.7, 7.8, 8.0, and 8.1 • CentOS 7.7, 7.8, 8.0, and 8.1 Language = English, Locale = US Although RHEL and CentOS 7.7 and 8.0 continue to be supported, it is recommended that you upgrade to RHEL/CentOS 7.8 or 8.1. Note: RHEL and CentOS 7.8 are supported only in SANnav 2.1.0a and higher.	• RHEL: 7.7, 7.8, 8.0, and 8.1 • CentOS 7.7, 7.8, 8.0, and 8.1 Language = English, Locale = US Although RHEL and CentOS 7.7 and 8.0 continue to be supported, it is recommended that you upgrade to RHEL/CentOS 7.8 or 8.1. Note: RHEL and CentOS 7.8 are supported in SANnav 2.1.0a and higher.
Processor architecture	x86	x86
Host type	• Bare metal server • VMware ESXi virtual machine	• Bare metal server • VMware ESXi virtual machine
CPU	16 cores	24 cores
CPU sockets (minimum)	2	2
CPU speed (minimum)	2000 MHz	2000 MHz
Memory (RAM)	48 GB	96 GB
Hard disk space (minimum)	600 GB, distributed as follows: • 450 GB — Installation directory • 120 GB — Docker installation directory • 16 GB of swap space	1.2 TB, distributed as follows: • 1050 GB — Installation directory • 120 GB — Docker installation directory • 16 GB of swap space

Installation Prerequisites

Review and comply with all SANnav installation prerequisites before you unzip the installation file.

NOTE
Use the latest generation processors for better SANnav performance.

Table 5: Installation Prerequisites

Task	Task Details or Additional Information
Gather necessary information and components.	Make sure that you have the following information: • Root user credentials. You must log in to the SANnav server as the root user or a user with root privilege. • The SANnav Management Portalserver IP address.
Uninstall other applications.	SANnav is expected to be installed and run on a dedicated host. If any other application is installed on the host, uninstall it before starting SANnav installation. If you are migrating SANnav, do not uninstall the current SANnav instance.
Uninstall Docker, if already installed.	The SANnav installation installs Docker. If you have a Docker installed other than the Docker that SANnav installs, you must remove it before starting the installation.

Task	Task Details or Additional Information
Ensure that IP network addresses do not conflict with Docker addresses.	SANnav comes with Docker preinstalled. The following IP address ranges are allocated to the Docker virtual interfaces: • 10.11.0.0/24 with Gateway 10.11.0.1 • 172.17.0.0/16 with Gateway 172.17.0.1 • 172.18.0.0/16 with Gateway 172.18.0.1 • 172.19.0.0/16 with Gateway 172.19.0.1 If you are using IPv4, then when choosing your VM IP address and gateway, do not use an address in these ranges. If you do, although the deployment may be successful, the IP address will be unreachable. IPv6 connectivity is not affected.

Check operating system requirements.	• Ensure that the operating system can be loaded through a bootable disk or through a PIXe server.
	• Ensure that the `lsof` and `nslookup` packages are installed on the operating system machine. If they are not installed, run the following commands to install them:
	`yum install lsof`
	`yum install bind-utils`

Format the XFS file system.	If you are using XFS as the file system, make sure that you set `d_type=true` while creating the disk. You can verify this by running the command `xfs_info <docker-installation-directory>` and verify that `ftype=1` . The default Docker installation directory is `/var/lib`.
Set umask and ulimit.	• "umask" for the root user must be set to 0022. Enter the following command to set the umask: `umask 0022` You must set the umask before you unzip the installation files. If you extracted the installation files before setting the umask, you must delete the installation folder, run `umask 0022` , and unzip the files again. • Ensure that the ulimit is set correctly. To set the ulimit, edit the `/etc/security/limits.conf` file and add the following limit at the end of the file: `elasticsearch - nofile 65536`

Check port 22 availability.	By default port 22 is used for the internal firmware repository, but you can change this port number during installation. If the port is not available, you must use an external FTP, SCP, or SFTP server for switch supportsave and firmware download functionality.
	For switches running Fabric OS versions earlier than 8.2.2, if you change to a port number other than 22, you must always use an external FTP, SCP, or SFTP server for switch supportsave and firmware download functionality.
	To free port 22 for SANnav Management Portal, perform the following steps:
	1. Edit the `/etc/ssh/sshd_config` file:
	a. Locate the following line:
	`#port 22`
	b. Uncomment the line and change the port number to another, unused port, such as 6022.
	`port 6022`
	Note that whatever port you select must be available and allowed in the firewall.
	2. Restart the SSHD using the following command:
	`systemctl restart sshd`
	The current SSH session remains logged in, but any new sessions must now use port 6022.

Task	Task Details or Additional Information
Check port 80 availability.	Port 80 must be available if you allow HTTP port 80 to HTTPS redirection; otherwise, installation fails. After installation, port 80 must continue to be available all the time; otherwise, you cannot start (or restart) SANnav. If your network utilizes a firewall, there may be other ports that must be open. See the Firewall Requirements for SANnav Management Portal section for details.

Ensure that IPv4 IP forwarding is enabled.	To check whether IPv4 IP forwarding is enabled, enter the following command:
	`/sbin/sysctl net.ipv4.ip_forward`
	If the output is `net.ipv4.ip_forward=1` , forwarding is enabled, and you do not need to make any changes.
	If the output is `net.ipv4.ip_forward=0` , forwarding is disabled, and you must change it as follows:
	1. Enter the following command to set IP forwarding for this session:
	`/sbin/sysctl -w net.ipv4.ip_forward=1`
	2. Edit the `/etc/sysctl.conf` file and add the following lines:
	`# IP Forwarding is enabled for Broadcom SANnav`
	`net.ipv4.ip_forward = 1`

Run additional commands.	• Ensure that the `hostname -i` command resolves to a valid IP address. • The `nslookup` command must be successful for the host name of the physical host and VM.

Configuring the Firewalld Backend for CentOS and RHEL 8.0 or Higher

Starting in CentOS and RHEL 8.0, the firewalld backend defaults to using "nftables" instead of "iptables." Docker does not have native support for "nftables."

If you are installing SANnav on CentOS or RHEL 8.0 or higher and firewalld is enabled, you must change the firewalld backend to use "iptables" instead of "nftables." If you do not make this change, you are not able to discover any switches in SANnav.

Perform the following steps before starting the SANnav installation.

1. Get the active zone details.

   You will need the zone details in the next step.

   ```
   firewall-cmd --list-all
   ```

2. Disable masquerade.

   ```
   firewall-cmd --zone=<ActiveZoneDetails> --remove-masquerade --permanent
   ```

   Where `<ActiveZoneDetails>` is listed in the output of the `firewall-cmd --list-all` command.

3. Stop the firewalld.

   ```
   systemctl stop firewalld
   ```

4. Edit the firewalld configuration file and change `FirewallBackend=nftables` to `FirewallBackend=iptables`.

   ```
   vi /etc/firewalld/firewalld.conf
   ```

5. Start the firewalld.

   ```
   systemctl start firewalld
   ```

6. Reload the firewalld.

   ```
   firewall-cmd --reload
   ```

Installing SANnav Management Portal

Complete these steps to download and install SANnav Management Portal on the server.

Before you unzip the installation file, be sure to review and comply with the system and server requirements and the installation prerequisites that are listed in the following sections:

- System and Server Requirements for SANnav Management Portal
- Installation Prerequisites

> **NOTE**
> If the scripts fail during the installation or startup, uninstall SANnav, reboot the server, and then reinstall SANnav. Do not try to fix the issue and re-run the installation script without first uninstalling the application.

Download and copy the SANnav Management Portal software package to the server. The package contains the SANnav Management Portal tarball.

1. Download the SANnav Management Portal tarball (for example, `Portal_<version>-distribution.tar.gz`) to the folder where you want to install the application.

   > **NOTE**
   > Do not create the SANnav Management Portal installation folder with a space in the name; otherwise, installation fails.

2. Untar the `.gz` file to extract the file to the current location.

   ```
   tar -xvzf Portal_<version>-distribution.tar.gz
   ```

   This step creates a directory with a name similar to `Portal_<version>_bldxx`. This directory is referred to as the `<install_home>` directory in this document.

3. Go to the `<install_home>/bin` directory.

   ```
   [root@RHEL7-10-100 home]# cd Portal_<version>_bldxx/bin
   ```

4. Run the `install-sannav.sh` script to install SANnav Management Portal.

   ```
   [root@RHEL7-10-100 bin]# ./install-sannav.sh
   ```

   If an earlier instance of SANnav Management Portal is installed, the installation script prompts whether you want to continue with migration or exit the installation.

5. If you are prompted about migrating SANnav, enter one of the following options.

   - To proceed with migration, press `Enter`. You are prompted to enter the location of the existing SANnav installation.
   - To exit the installation, press `Ctrl-C`. The script ends. At this point, you can back up the current SANnav instance and restart the installation script. Or you can uninstall the current SANnav instance, and restart the installation script without migrating.

As the installation proceeds, the script runs a pre-install requirements test. If any test fails, the installation exits with error messages. You must fix the reported issues, uninstall the application, and repeat from Step 1. After the diagnostics pass, installation of SANnav Management Portal software continues.

On successful installation of the software, the SANnav Management Portal server starts up. The startup may take up to 20 minutes.

Uninstalling SANnav

You can run a single script to uninstall SANnav. Perform the following steps to uninstall the SANnav application and bring the system back to the original state.

1. Go to the `<install_home>/bin` folder and run the following script:

   ```
   ./uninstall-sannav.sh
   ```

2. After SANnav is uninstalled, restart the server.

Firewall Requirements for SANnav Management Portal

If your network utilizes a firewall between the SANnav Management Portal client and the server or between the server and the SAN, a set of ports must be open in the firewall to ensure proper communication.

The following table lists the ports that must be open in the firewall. These ports are added to the IP tables by default when the SANnav server is running. You do not need to open them in the firewalld if it is enabled and running on the SANnav server.

NOTE
For ports that were customized during SANnav installation, the customized ports must be open in the firewall.

Table 6: Ports That Must Be Open in the Firewall

Port Number	Transport	Inbound/ Outbound	Communication Path	Description
22	TCP	Both	Client --> Server Server <--> Switch	Internal SSH server
80	TCP	Both	Client --> Server Server --> Switch	HTTP port for access from browser to server HTTP port for access from server to switch
161	UDP	Outbound	Server --> Switch	SNMP port
162	UDP	Inbound	Switch --> Server	SNMP trap port
443	TCP	Both	Client --> Server Server --> Switch Server --> vCenter	HTTPS port for secure access from browser to server HTTPS port for secure access from server to switch HTTPS port for secure access from server to vCenter
514	UDP	Inbound	Switch --> Server	Syslog port
6514	UDP	Inbound	Switch --> Server	Secure syslog port
8081	TCP	Inbound	Switch --> Server	Avro schema registry port
18081	TCP	Inbound	Switch --> Server	Avro schema registry insecure port (SANnav 2.1.0a and higher)
19094	TCP	Inbound	Switch --> Server	Secured Kafka port
19095	TCP	Inbound	Switch --> Server	Secured Kafka port

If firewalld is enabled, you must add the SSH service to the trusted zone in the firewalld for the firmware download feature to work. See Configuring a Firewall for SANnav for instructions on how to configure firewalld.

If you configure an external authentication server (LDAP, RADIUS, or TACACS+) or an email server (SMTP), ensure that the SANnav Management Portal server has access to the ports listed in the following table. The default ports are listed in the table, but you can change the default.

Table 7: Ports That the SANnav Server Must Be Able to Access

Port Number	Transport	Inbound/ Outbound	Communication Path	Description
25	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications without SSL or TLS
49	TCP	Outbound	Server --> TACACS+ Server	TACACS+ server port for authentication if you use TACACS+ for external authentication
389	TCP	Outbound	Server --> LDAP Server	LDAP server port for authentication if you use LDAP for external authentication and SSL is not enabled
465	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications with SSL
587	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications with TLS
636	TCP	Outbound	Server --> LDAP Server	LDAP server port for authentication if you use LDAP for external authentication and SSL is enabled
1812	UDP	Outbound	Server --> RADIUS Server	RADIUS server port for authentication if you use RADIUS for external authentication

SANnav Management Portal OVA Deployment

SANnav Management Portal can be installed as a virtual appliance, compatible with VMware ESXi version 6.7.

The SANnav software package contains a SANnav OVA file (.ova), which can be deployed to an ESXi discovered in vCenter, using either of the following methods:

- vCenter user interface
- `ovftool` command

The default installation includes 48 GB memory, which supports the Base License and the Enterprise License with up to 3000 ports. You can upgrade to 96 GB memory to support an Enterprise License with up to 15,000 ports.

The CentOS operating system is bundled with the SANnav virtual appliance. The language is English, and the locale is US.

- CentOS 8.0 (SANnav 2.1.0)
- CentOS 8.1 (SANnav 2.1.0a and higher)

You must have Administrator access to ESXi/vCenter to deploy and install the SANnav virtual appliance.

Migration from a VM or bare metal version of SANnav to SANnav virtual appliance is not supported.

Note that deployment of the SANnav virtual appliance is supported only by VMware infrastructure.

System and Server Requirements for the SANnav Management Portal Appliance

You must meet all system and server requirements before you begin installing the SANnav Management Portal appliance.

SANnav OVA is delivered with base hardware requirements suitable for the Base license or for an Enterprise license with a 3000-port configuration. If you want to use SANnav for a larger port count or a higher configuration, you must edit the hardware specifications before starting installation. The installation procedures include steps for upgrading the hardware.

The following table lists the hardware requirements for deploying SANnav Management Portal as an appliance.

Note that the supported operating system is different, starting with SANnav 2.1.0a. If you are migrating from SANnav 2.1.0, you can upgrade the operating system after installation, as described in Upgrading the OS with SANnav Installed.

Table 8: System and Server Requirements for the SANnav Appliance

Requirement	Base License or Enterprise License with up to 3000 Ports, Included with SANnav OVA Package	Enterprise License with up to 15,000 Ports
Server package	• VMware ESXi host, 6.7 • ESXi 6.7, discovered in vCenter 6.7 • ESXi 6.5 (supported only with `ovftool`)	• VMware ESXi host, 6.7 • ESXi 6.7, discovered in vCenter 6.7 • ESXi 6.5 (supported only with `ovftool`)
CPU	16 cores	24 cores
CPU sockets	2	2
Memory (RAM)	48 GB	96 GB

The SANnav appliance comes with predefined file system and disk partitions. Two disk partitions are created in the SANnav appliance.

- Operating system and SWAP file
- SANnav installation folder
  This partition is used to store SANnav files and install Docker.

The following table lists the specifications for each partition. The datastore that you are planning to use for SANnav OVA must have a minimum space of 630 GB to meet the space requirements for both partitions.

Table 9: Disk Partitions in the SANnav Appliance

Partition Type	Base License or Enterprise License with up to 3000 Ports, Included with SANnav OVA Package	Enterprise License with up to 15,000 Ports
Operating system and SWAP file	60 GB: • 40 GB for OS • 16 GB for swap space	60 GB: • 40 GB for OS • 16 GB for swap space
SANnav installation folder	570 GB: • 450 GB for SANnav installation • 120 GB for Docker installation	1.2 TB: • 1050 GB for SANnav installation • 120 GB for Docker installation

Installation Prerequisites for the SANnav Management Portal Appliance

Review and comply with all SANnav Management Portal appliance installation prerequisites before importing the OVA file.

Table 10: Installation Prerequisites for SANnav Management Portal Appliance

Task	Task Details or Additional Information
Gather necessary information and components.	You must have default credentials for the root user and SANnav user: • User name = "root", password = "SANnav!@#" • User name = "sannav", password = "SANnav!@#"
If needed, set the preferred IP address.	OVA supports only one IP address. This address is used for both client-to-server and server-to-switch communication. If you want a preferred address for switch-to-server communication, manually set the IP address before starting the installation. Note that you cannot set a nondefault or private IP address for switch-to-server communication.
Decide the IP allocation policy (Static or DHCP) for dual stacks.	The supported IP allocation policy is for both stacks (IPv4 and IPv6) to use Static or both stacks to use DHCP. Using Static for one stack and DHCP for the other stack is not supported.
Ensure that IP network addresses do not conflict with Docker addresses.	SANnav OVA comes with Docker preinstalled. The following IP address ranges are allocated to the Docker virtual interfaces: • 10.11.0.0/24 with Gateway 10.11.0.1 • 172.17.0.0/16 with Gateway 172.17.0.1 • 172.18.0.0/16 with Gateway 172.18.0.1 • 172.19.0.0/16 with Gateway 172.19.0.1 If you are using IPv4, then when choosing your VM IP address and gateway, do not use an address in these ranges. If you do, although the deployment may be successful, the IP address will be unreachable. IPv6 connectivity is not affected.

Installing the SANnav Management Portal Appliance Using vCenter

The default installation includes 48 GB memory, which supports the Base License and the Enterprise License with up to 3000 ports. You can upgrade to 96 GB memory to support an Enterprise License with up to 15,000 ports.

> **NOTE**
> If you are using ESXi 6.5, you must use `ovftool` instead of vCenter. See Installing the SANnav Management Portal Appliance Using ovftool.

Perform the following steps to install SANnav Management Portal Appliance using vCenter.

1. Download the SANnav OVA package to the location from which you want to import to ESXi / vCenter.

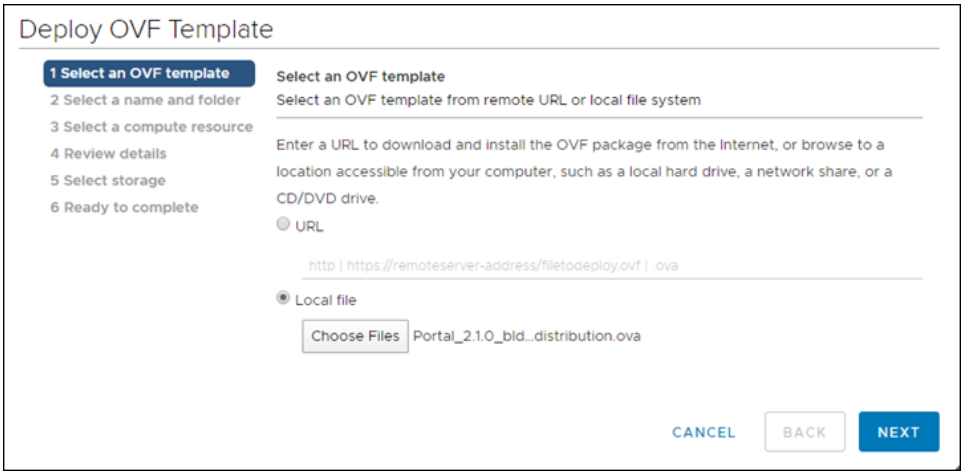
   Note that the time it takes to deploy the SANnav OVA package to the host depends on the network speed between the location to which the OVA package is downloaded and the ESXi.

2. Log in to vCenter, right-click the host on which you want to deploy SANnav, and select **Deploy OVF Template**.

   The following steps correspond to the steps in the vCenter interface. Note that the screenshots are examples to show clarity only. Based on your environment or vCenter license the actual screens may look different.

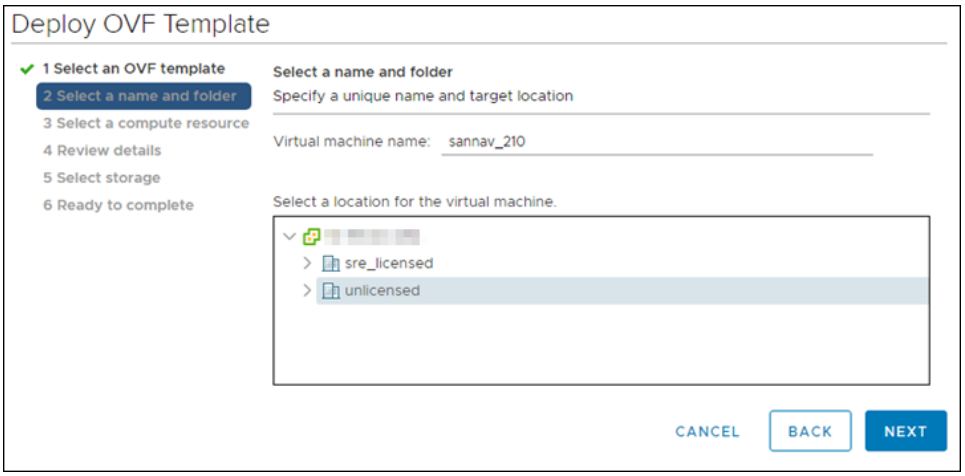
   a) **Select an OVF template**.

   Select the **Local file** option. Click **Choose Files**, navigate to the folder where the SANnav OVA file is downloaded, and select the file. Click **Next**.



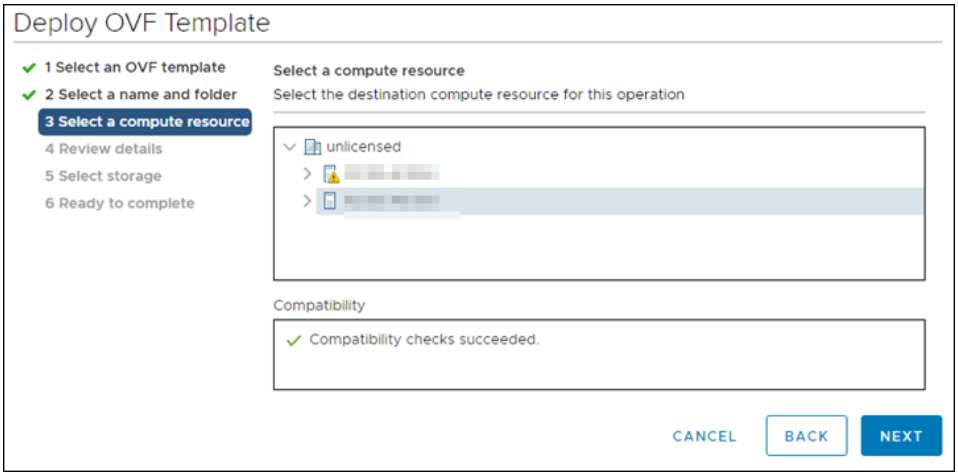
   b) **Select a name and folder**.

   Enter a name for the VM, and select the location (datacenter) to which you want to deploy SANnav. Click **Next**.



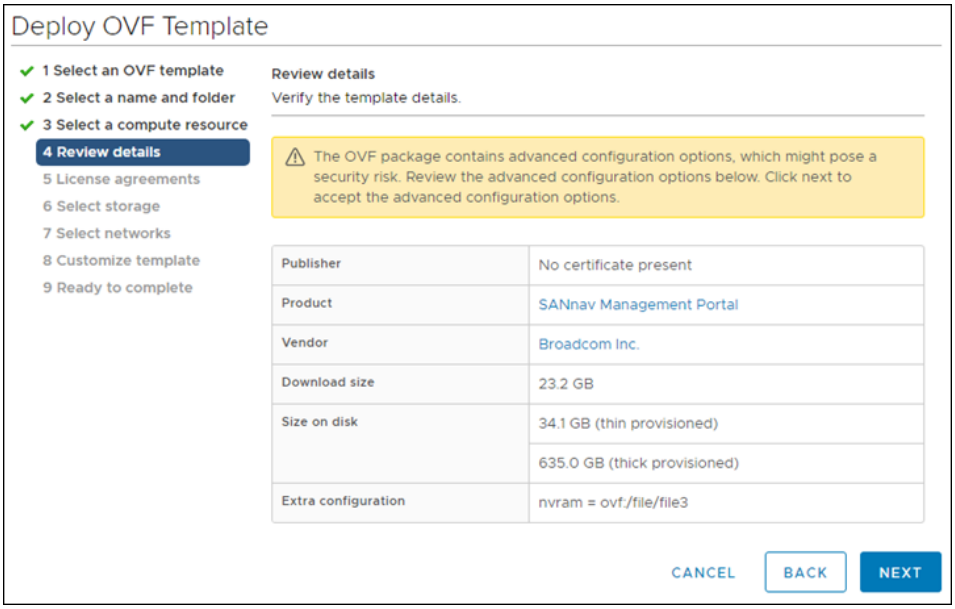
c) **Select a compute resource**.

Select the host on which you want to deploy SANnav. Ensure that the host meets the system and server requirements for SANnav. Click **Next**.



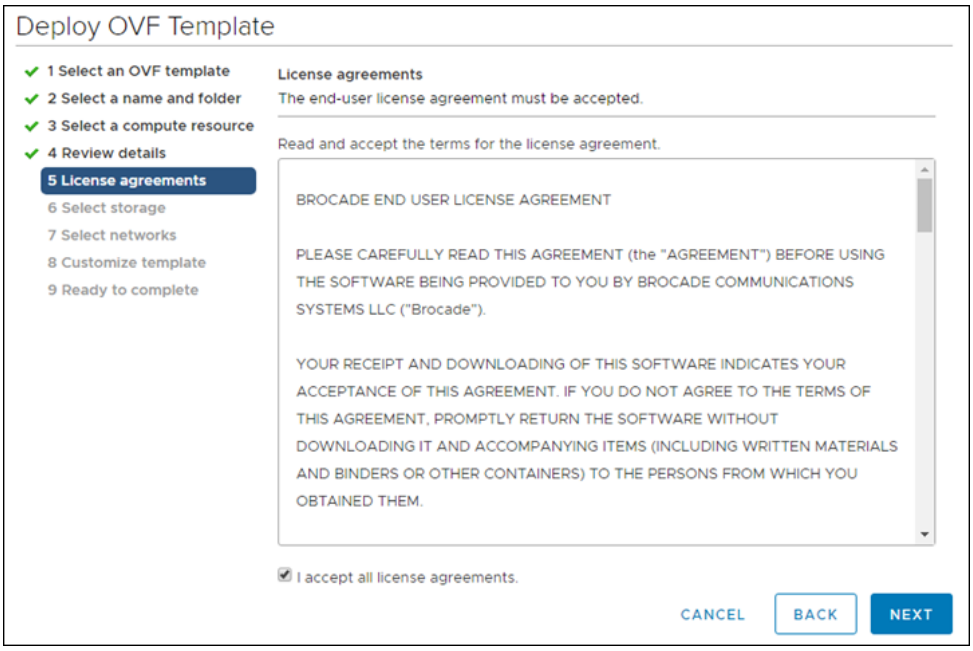
d) **Review details**.

Review details of the installation package, and click **Next**.



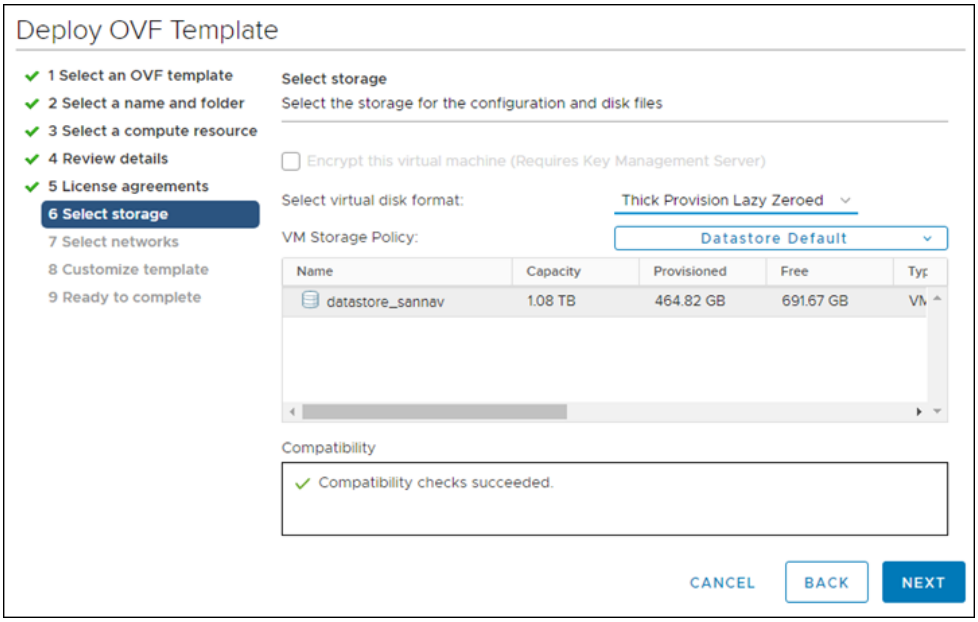
e) **License agreements**.

Select the **I accept all license agreements** checkbox, and click **Next**.



f) **Select storage**.

Select the storage (datastore) where you want to allocate storage space for the SANnav vmdk files. The datastore must have a minimum of 630 GB. Click **Next**.

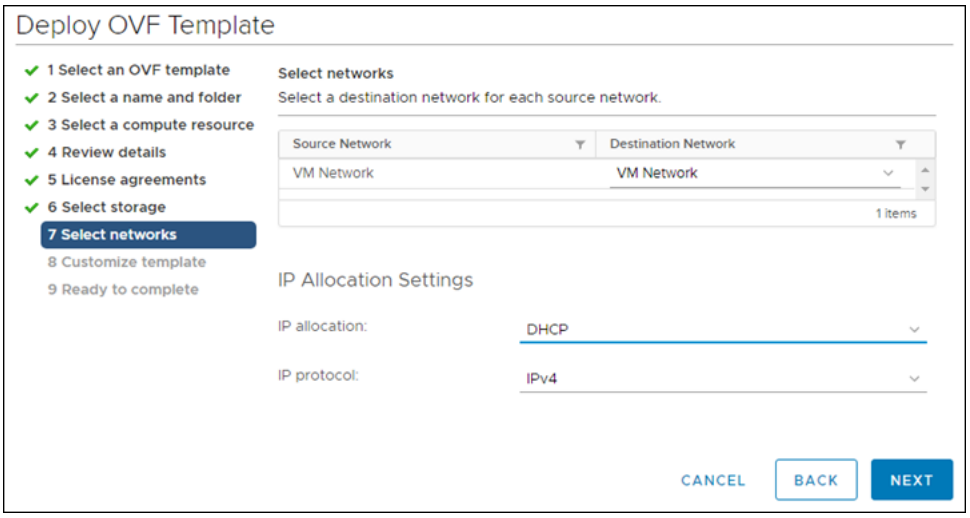


g) **Select networks**.

Choose the IP allocation strategy and IP protocol.

- For **IP allocation**, choose either **DHCP** or **Manual (Static)**.
- For **IP protocol**, choose either **IPv4** or **IPv6**.

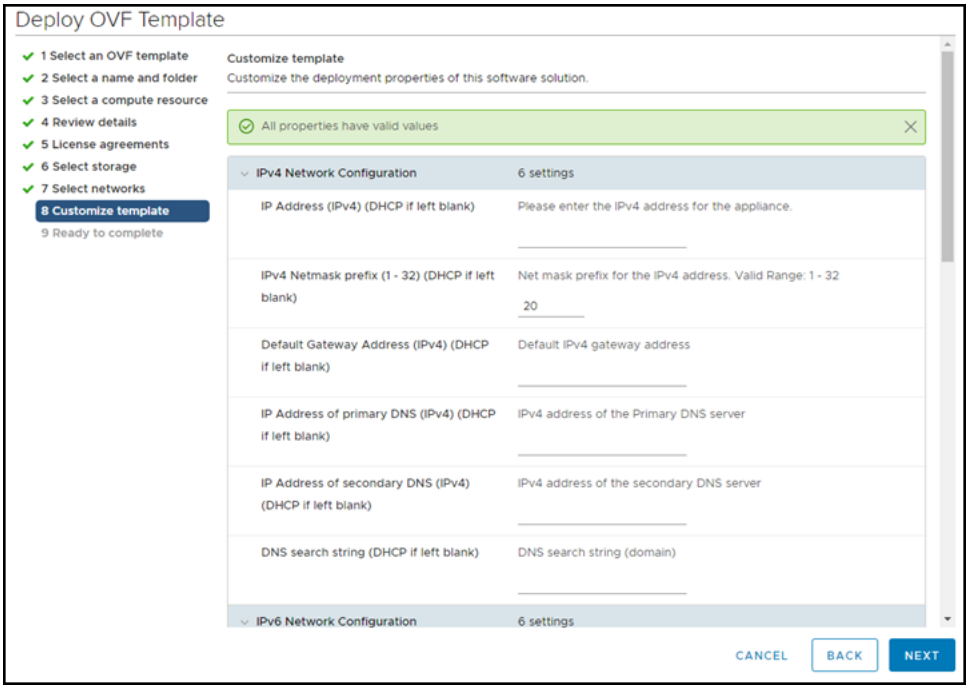
Click **Next**.



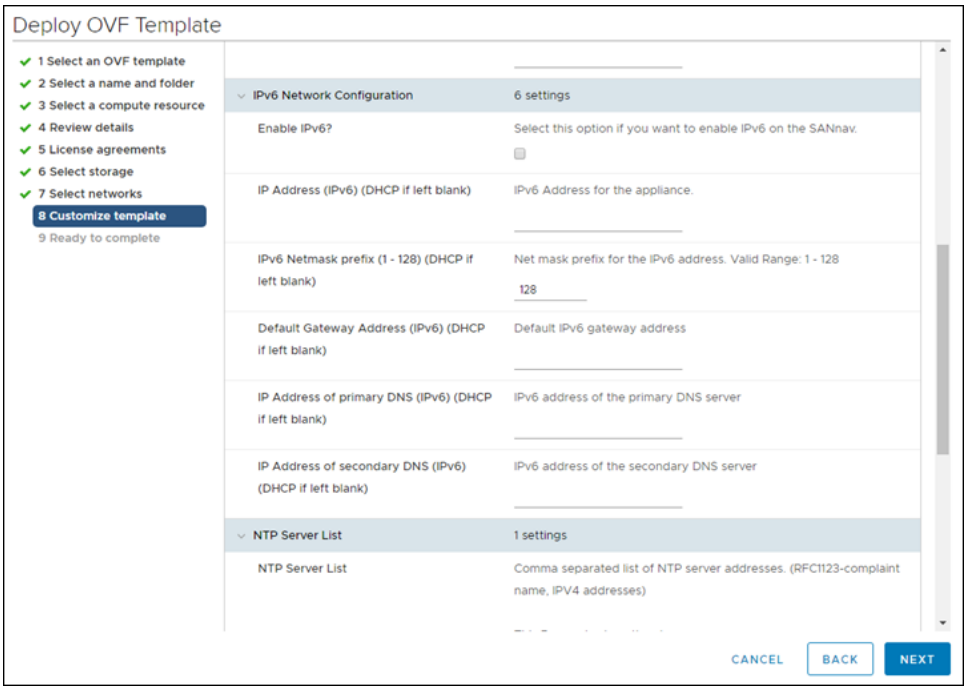
h) **Customize template**.

Provide all values for SANnav customization.

IPv4 Network Configuration. If IP allocation is **DHCP**, leave this section blank. If IP allocation policy is **Manual (Static)**, you must enter the values. Note that the **IP Address of secondary DNS** and **DNS search string** properties are optional.

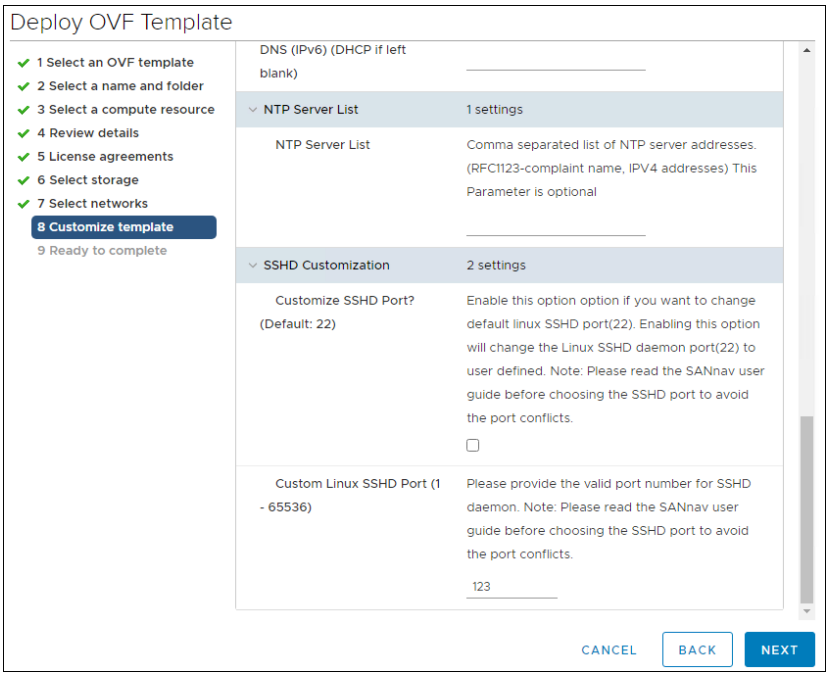


IPv6 Network Configuration: If IP allocation is **DHCP**, leave this section blank. If IP allocation policy is **Manual (Static)**, you must enter the values. Note that the **IP Address of secondary DNS** property is optional.



NTP Server List: To deploy Flow Management in SANnav, you must configure NTP time synchronization on the server. Provide a comma-separated list of NTP servers.

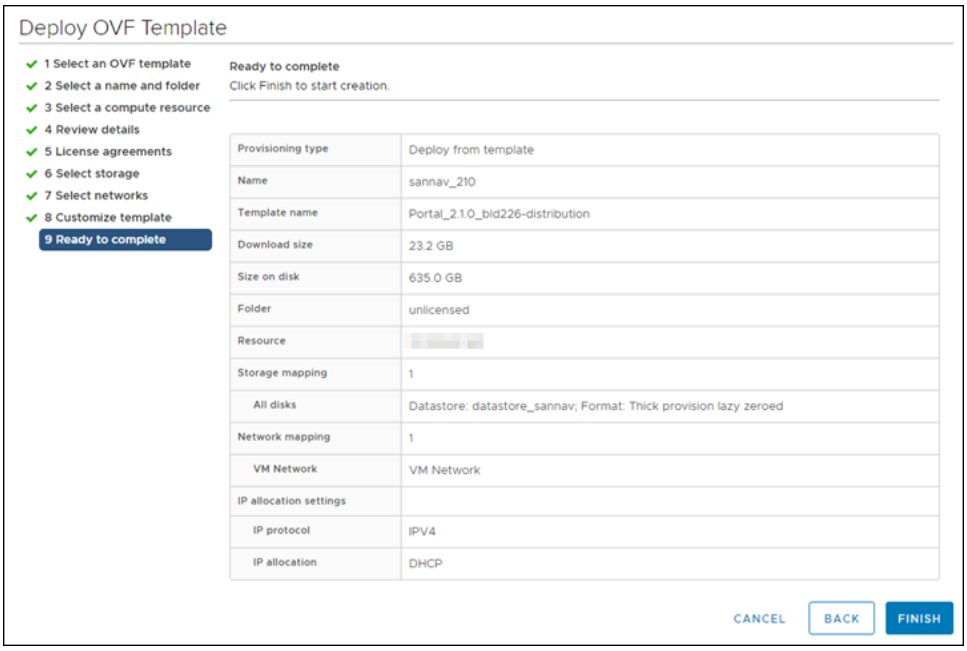
SSHD Customization: By default, port 22 is used for Linux/VM server management. If you want to change this port, select the checkbox and enter the new port number.



Click **Next**.

i) **Ready to complete**.

Review the installation details, and click **Finish**.



3. After successful network configuration, log in as the root user, and ensure that the network is set up accordingly.

   By default, the SANnav OVA installation can accommodate a Base license with up to 600 ports or an Enterprise license with up to 3000 ports.

4. Upgrade the hardware settings if you want to support an Enterprise License with up to 15,000 ports.

   Refer to Expanding Hardware Configurations from 3000 to 15,000 Ports for instructions.

5. Log out as the "root" user, and then log in as the "sannav" user to start the installation.

   The SANnav installation script automatically starts. On successful installation, SANnav Management Portal starts on the VM. The startup may take up to 20 minutes.

After successful installation, you can use the standard scripts to manage SANnav. See Additional Scripts for Managing SANnav.

Installing the SANnav Management Portal Appliance Using ovftool

Before you start importing the OVA package to the host, be sure to review and comply with the system and server requirements and the installation prerequisites that are listed in the following sections:

- System and Server Requirements for the SANnav Management Portal Appliance
- Installation Prerequisites for the SANnav Management Portal Appliance

NOTE

The time that it takes to deploy the OVA package to the host depends on the speed of the network between the location to which the OVA package is downloaded and the target ESXi. For example, a wireless connection can take a long time.

Perform the following steps to install the SANnav Management Portal appliance using ovftool. Contact Technical Support for additional help with this procedure.

1. Download the SANnav OVA package to the location from which you want to import to ESXi / vCenter.
2. Download the Open Virtualization Format tool (`ovftool`).

   VMware OVF Tool is a command line utility to import the OVA. You can download this free tool from: https://code.vmware.com/web/tool/4.3.0/ovf.
3. Deploy SANnav using the `ovftool` command.

   You can deploy SANnav to a VM discovered in vCenter, or you can deploy SANnav to an ESXi directly.

   Run the `ovftool` command using one of the formats in the examples shown in Ovftool Command Examples. For descriptions of the parameters, see Ovftool Command Parameters.

   NOTE
   If the vCenter ESXi password contains special characters, they must be replaced by “%<hexValue>” for each special character. For example, if the password is “Pass!”, when specifying the password in the `ovftool` command, replace this password with “Pass%21”.

   NOTE

   To upgrade the hardware to support an Enterprise License with up to 15,000 ports, include the **--memorySize** and **--numberOfCpus** parameters in the `ovftool` command.

   ```
   --memorySize:<VM_name>=96000
   --numberOfCpus:<VM_name>=24
   ```

   You must also upgrade the hardware settings as described in Step 5.

   At this point, the following occurs:

   1. VM networking is configured.
   2. Docker is configured.
   3. The VM is rebooted.

   VM networking is configured based on the hardware configuration and the options that are provided to the `ovftool` command. If network configuration fails, you must power off the VM, log in to the vCenter to update the network parameters, and then power on the VM to retry the network configuration.
4. After successful network configuration, log in as the root user, and ensure that the network is set up accordingly.

   By default, the SANnav OVA installation can accommodate a Base license with up to 600 ports or an Enterprise license with up to 3000 ports.
5. Upgrade the hardware settings if you want to support an Enterprise License with up to 15,000 ports.

   Refer to Expanding Hardware Configurations from 3000 to 15,000 Ports for instructions.
6. Log out as the "root" user, and log in as the "sannav" user to start the installation.

   The SANnav installation script automatically starts. On successful installation, SANnav Management Portal starts on the VM. The startup may take up to 20 minutes.

After successful installation, you can use the standard scripts to manage SANnav. See Additional Scripts for Managing SANnav.

Ovftool Command Parameters

The following table describes the parameters for the `ovftool` command. All parameters are mandatory, unless otherwise indicated.

Table 11: Ovftool Command Options

Option	Description
`--acceptAllEulas`	Accept the End User License Agreement.
`--disableVerification`	Disable verification of the file.
`--noSSLVerify`	No SSL verification.
`--name`	Name of the virtual machine.
`--X:injectOvfEnv`	Indicates additional parameters.
`--datastore`	Name of the target datastore.
`--network`	Name of the network.
`--ipAllocationPolicy`	Either `dhcpPolicy` or `fixedPolicy`.
`--prop:network.ipv4.01.ipaddress`	IPv4 address that is allocated for this VM.
`--prop:network.ipv4.02.netmask`	Netmask or subnet (1–32).
`--prop-network.ipv4.03.gateway`	IPv4 address of the gateway.
`--prop:network.ipv4.04.dns01`	IPv4 address of DNS server 1.
`--prop:network.ipv4.05.dns02`	(Optional) IPv4 address of DNS server 2.
`--prop:network.ipv4.06.dns_search_string`	(Optional) Search domain string.
`--prop:network.ipv4.07.ntp_server_string`	(Optional) Comma-separated list of NTP server addresses. To deploy Flow Management in SANnav, you must set the NTP server configuration.
`--prop:network.ipv6.01.enable`	(Optional) Indicates whether IPv6 is enabled. Default = False.
If `network.ipv6.01.enable=True` , the following `network.ipv6` parameters are mandatory; otherwise, they are optional.	
`--prop:network.ipv6.02.ipaddress`	IPv6 address that is allocated for this VM.
`--prop:network.ipv6.03.netmask`	Netmask or subnet (1–128).
`--prop:network.ipv6.04.gateway`	IPv6 address of the gateway.
`--prop:network.ipv6.05.dns01`	IPv6 address of DNS server 1.
`--prop:network.ipv6.06.dns02`	(Optional) IPv6 address of DNS server 2.
`--prop:network.sshd.customize`	(Optional) SSHD port customization. Set this option to True if you want to change the Linux default SSHD port 22. Default = False.
`--prop:network.sshd.port`	(Optional) SSHD port customization. If you elect to change the default SSHD port, provide the new port number here. Valid port range is 1–65536. Default = 124.
`--memorySize`	(Optional) Memory size, in MB. Set this option to 96000 to support an Enterprise license with up to 15,000 ports. Default is 48000.
`--numberOfCpus`	(Optional) Number of CPU cores. Set this option to 24 to support an Enterprise license with up to 15,000 ports. Default is 16.
`--powerOn`	Powers on the VM.
`/path-for-sannav-ova-file>/sannav-portal-v210.ova`	Path for the SANnav OVA file.

Option	Description
vi:// <vCenterUserName>:<vCenterPassword>@<vCenterIPaddr>/ <Location of VM>/host/<IPaddr_of_ESXi_Host> --OR-- vi://<ESXiUsername>:<ESXiPassword>@<ESXi_IPaddr>	Inventory path. Use the first format for deploying SANnav to a VM discovered in vCenter. Use the second format for deploying SANnav to ESXi directly.

Ovftool Command Examples

Run the `ovftool` command using one of the formats shown here. You can copy this text and replace the parameters that are indicated by angular brackets (< ... >) with your specific values.

The following examples are included here:

- IPv4 Only + DHCP Network Configuration
- IPv4 + IPv6 + DHCP Network Configuration
- IPv4 + Static Network Configuration
- IPv4 + IPv6 + Static Network Configuration
- Configuration Supporting up to 15,000 Ports
- NTP Server Synchronization
- Customized SSHD Port

IPv4 Only + DHCP Network Configuration

The following example deploys SANnav OVA to an ESXi discovered in vCenter.

```
./ovftool --acceptAllEulas --disableVerification --noSSLVerify --name=<Name-of-the-VM> --X:injectOvfEnv --
datastore="<Name-of-the-target-DS>" --network="VM Network" --ipAllocationPolicy="dhcpPolicy" --powerOn <Path-
for-SANnav-OVA-File>/sannav-portal-v210.ova vi://<vCenter_User_Name>:<vCenter_Password>@<vCenter_IPAddress>/
<Location_of_VM>/host/<IP_Address_of_ESXi_Host>
```

To deploy SANnav OVA directly to ESXi, replace the last parameter (the **vi:** parameter) with the following:

```
vi://<ESXi_User_Name>:<ESXI_Pass>@<ESXi_IP_Address>/
```

IPv4 + IPv6 + DHCP Network Configuration

The following example is for deploying SANnav OVA to an ESXi discovered in vCenter.

```
./ovftool --acceptAllEulas --disableVerification --noSSLVerify --name=<Name-of-the-VM> --X:injectOvfEnv
 --datastore="<Name-of-the-target-DS>" --network="VM Network" --ipAllocationPolicy="dhcpPolicy" --
prop:network.ipv6.01.enable=True --powerOn <Path-for-SANnav-OVA-File>/sannav-portal-v210.ova vi://
<vCenter_User_Name>:<vCenter_Password>@<vCenter_IPAddress>/<Location_of_VM>/host/<IP_Address_of_ESXi_Host>
```

To deploy SANnav OVA directly to ESXi, replace the last parameter (the **vi:** parameter) with the following:

```
vi://<ESXi_User_Name>:<ESXI_Pass>@<ESXi_IP_Address>/
```

IPv4 Only + Static Network Configuration

The following example is for deploying SANnav OVA to an ESXi discovered in vCenter. Note that the `network.ipv4.05.dns02` and `network.ipv4.06.dns_search_string` parameters are optional.

```
./ovftool --acceptAllEulas --disableVerification --noSSLVerify --name=<Name-of-the-VM> --X:injectOvfEnv
 --datastore="<Name-of-the-target-DS>" --network="VM Network" --ipAllocationPolicy="fixedPolicy"
 --prop:network.ipv4.01.ipaddress=<IPv4 Address> --prop:network.ipv4.02.netmask=<NetMask> --
prop:network.ipv4.03.gateway=<IPv4 Gateway Address> --prop:network.ipv4.04.dns01=<IPv4 DNS 01 Address>
 --prop:network.ipv4.05.dns02=<IPv4 DNS 02 Address> --prop:network.ipv4.06.dns_search_string=<DNS
 Search String> --powerOn <Path-for-SANnav-OVA-File>/sannav-portal-v210.ova vi://
<vCenter_User_Name>:<vCenter_Password>@<vCenter_IPAddress>/<Location_of_VM>/host/<IP_Address_of_ESXi_Host>
```

To deploy SANnav OVA directly to ESXi, replace the last parameter (the **vi:** parameter) with the following:

```
vi://<ESXi_User_Name>:<ESXI_Pass>@<ESXi_IP_Address>/
```

IPv4 + IPv6 + Static Network Configuration

The following example is for deploying SANnav OVA to an ESXi discovered in vCenter. Note that the `network.ipv6.06.dns02` parameter is optional.

```
./ovftool --acceptAllEulas --disableVerification --noSSLVerify --name=<Name-of-the-VM> --X:injectOvfEnv
 --datastore="<Name-of-the-target-DS>" --network="VM Network" --ipAllocationPolicy="fixedPolicy"
 --prop:network.ipv4.01.ipaddress=<IPv4 Address> --prop:network.ipv4.02.netmask=<NetMask> --
prop:network.ipv4.03.gateway=<IPv4 Gateway Address> --prop:network.ipv4.04.dns01=<IPv4 DNS 01 Address>
 --prop:network.ipv4.05.dns02=<IPv4 DNS 02 Address> --prop:network.ipv4.06.dns_search_string=<DNS
 Search String> --prop:network.ipv6.01.enable=True --prop:network.ipv6.02.ipaddress=<IPv6 Address>
 --prop:network.ipv6.03.netmask=<IPv6 NetMask> --prop:network.ipv6.04.gateway=<IPv6 Gateway
 Address> --prop:network.ipv6.05.dns01=<IPv6 DNS 01 Address> --prop:network.ipv6.06.dns02=<IPv6
 DNS 02 Address> --powerOn <Path-for-SANnav-OVA-File>/sannav-portal-v210.ova vi://
<vCenter_User_Name>:<vCenter_Password>@<vCenter_IPAddress>/<Location_of_VM>/host/<IP_Address_of_ESXi_Host>
```

To deploy SANnav OVA directly to ESXi, replace the last parameter (the **vi:** parameter) with the following:

```
vi://<ESXi_User_Name>:<ESXI_Pass>@<ESXi_IP_Address>/
```

Configuration Supporting up to 15,000 Ports

The default SANnav OVA package supports a Base license an Enterprise license with up to 3,000 ports. To use an Enterprise license with up to 15,000 ports, you must upgrade the hardware (memory and CPU). To upgrade the hardware, include the following parameters in the ovftool command:

```
--memorySize:<VM_name>=96000
--numberOfCpus:<VM_name>=24
```

NTP Server Synchronization

To deploy Flow Management in SANnav, you must configure NTP time synchronization on the server. To do this, include the following parameter in the `ovftool` command:

```
--prop:network.ipv4.07.ntp_server_string=<Comma-separated list of NTP servers>
```

Customized SSHD Port

By default, SANnav uses port 22 for its internal firmware repository, but you can change this port number.

> **NOTE**
> If you change the port number to other than 22, for switches running Fabric OS versions earlier than 8.2.2, you must use an external FTP, SCP, or SFTP server for switch supportsave and firmware download functionality.

To use a port other than port 22, include the following parameters in the `ovftool` command:

```
--prop:network.sshd.customize=<True/False, default:False>
--prop:network.sshd.port=<Valid Port Range 1 - 65536, Default: 124 >
```

Following is an example of IPv4 + IPv6 + Static Network Configuration with the additional parameters for NTP server synchronization and customized SSHD port.

```
./ovftool --acceptAllEulas --disableVerification --noSSLVerify --name=<Name-of-the-VM> --X:injectOvfEnv
 --datastore="<Name-of-the-target-DS>" --network="VM Network" --ipAllocationPolicy=fixedPolicy"
 --prop:network.ipv4.01.ipaddress=<IPv4 Address> --prop:network.ipv4.02.netmask=<NetMask> --
prop:network.ipv4.03.gateway=<IPv4 Gateway Address> --prop:network.ipv4.04.dns01=<IPv4 DNS 01 Address>
 --prop:network.ipv4.05.dns02=<IPv4 DNS 02 Address> --prop:network.ipv4.06.dns_search_string=<DNS
 Search String> --prop:network.ipv4.07.ntp_server_string=<Comma separated list of IPv4 NTP
 servers> --prop:network.ipv6.01.enable=True --prop:network.ipv6.02.ipaddress=<IPv6 Address> --
prop:network.ipv6.03.netmask=<IPv6 NetMask> --prop:network.ipv6.04.gateway=<IPv6 Gateway Address>
 --prop:network.ipv6.05.dns01=<IPv6 DNS 01 Address> --prop:network.ipv6.06.dns02=<IPv6 DNS 02
 Address> --prop:network.sshd.customize=<True/False, default:False> --prop:network.sshd.port=<Valid
 Port Range 1 - 65536, Default: 124 > --powerOn <Path-for-SANnav-OVA-File>/sannav-portal-v210.ova vi://
<vCenter_User_Name>:<vCenter_Password>@<vCenter_IPAddress>/<Location_of_VM>/host/<IP_Address_of_ESXi_Host>
```

Expanding Hardware Configurations from 3000 to 15,000 Ports

If you have purchased an Enterprise license and want to deploy SANnav OVA to discover more than 3000 ports (up to 15,000 ports), you must increase the hardware configurations (memory, CPU, and hard disk). Increasing the configurations must be done during the OVA extraction process and before SANnav installation.

Prerequisites:

- The SANnav OVA package must first be deployed using either vCenter or `ovftool` .

By default, the SANnav OVA image accommodates Base license customers with up to 600 ports or Enterprise customers with up to 3000 ports. For both of these licenses, the VM created when the OVA image is extracted has 48 GB of RAM, 16 cores, and 570 GB of hard disk space.

SANnav OVA contains two virtual machine disk (.VMDK) files.

- VMDK1 (`/dev/sda`) comes with 60 GB of disk space.
- VMDK2 (`/dev/sdb`) comes with 570 GB of disk space.

VMDK2 (`/dev/sdb`) is the SANnav file system that must be expanded to accommodate large port deployment.

1. Power on the SANnav VM and let the network configuration complete.
   If deployed using `ovftool` , the VM is automatically powered on.
2. Power off the SANnav VM.
3. Right-click the VM and click **Edit Settings**.
   Make the following changes:
   - Change **CPU** to 24 cores. Expand the **CPU** section and set cores per socket to **12**.
   - Change **Memory** to 96 GB.
   - Increase **Hard disk 2** to 1300 GB.

4. Save the settings, and power on the VM.
5. Log in to the VM as the "root" user.

   NOTE
   In the following steps, issue the commands from the "/" directory to avoid an error ("`umount: /sannav-portal-v210: target is busy`") when unmounting the disk.

6. Stop and disable the Docker service.

```
systemctl stop docker
systemctl disable docker
```

7. Unmount the current disk partition.

```
umount /sannav-portal-v210
```

8. Edit the `/etc/fstab` file and comment out the following line to avoid accidental mounting of the disk if the VM reboots.

```
#/dev/sdb1   /sannav-portal-v210          ext4    defaults        0 0
```

9. Enter the `fdisk` command to reformat and expand the size of the disk, and then perform the following steps.

```
fdisk /dev/sdb
```

   a) Enter **p** to check the current partition table.
      You can copy the output and save it for reference. The partition that will be updated is `/dev/sdb1`.
   b) Enter **d** to delete the partition.
      SANnav has only one partition, so it is deleted automatically.

```
Command (m for help): d
Selected partition 1
Partition 1 has been deleted.
```

   c) Enter **n** to create a new partition, enter **p** to select the partition type as primary, and enter the partition number (**1**).

```
Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-1363148799, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-1363148799, default 1363148799):

Created a new partition 1 of type 'Linux' and of size 650 GiB.
Partition #1 contains a ext4 signature.

Do you want to remove the signature? [Y]es/[N]o: N

The signature will be removed by a write command.
```

   d) Enter the number of the first sector, or accept the default setting (2048).
   e) For the last sector, accept the default value or enter an appropriate value, such as 1300G.
   f) Enter **N** when prompted to remove the signature.
   g) Enter **w** to save and exit the `fdisk` utility.
      At this point, you might see a message about the kernel using the old table.

10. If the following message is shown, reboot the VM before proceeding to the next step.

```
The kernel still uses the old table. The new table will be used at the next reboot or after you run
 partprobe(8) or kpartx(8).
```

11. Enter the `fdisk -l` command, and check that the size of the `/dev/sdb1` partition has been updated.
12. Perform the following steps to expand the newly created partition to the new size.
    a) Check the disk consistency by entering the `e2fsck -f /dev/sdb1` command.

```
[root@sannav-portal-v210a /]# e2fsck -f /dev/sdb1

e2fsck 1.44.6 (5-Mar-2019)

Pass 1: Checking inodes, blocks, and sizes

Pass 2: Checking directory structure

Pass 3: Checking directory connectivity

Pass 4: Checking reference counts

Pass 5: Checking group summary information

/dev/sdb1: 504/40632320 files (1.0% non-contiguous), 3777622/162529280 blocks
```

    b) Resize the file system to the new size.

```
resize2fs /dev/sdb1 size
```

    where *size* is **1300G**. If you omit this parameter, it defaults to the size of the partition.
13. Edit the `/etc/fstab` file and remount the partition by uncommenting the line that was commented out in Step 8.

```
/dev/sdb1   /sannav-portal-v210          ext4    defaults        0 0
```

14. Remount all disks.

```
mount -a
```

15. Verify that the disk space has increased or has been resized.

```
df -h
```

16. Ensure that the memory is expanded.

```
free mem
```

17. Ensure that the CPU cores are increased.

```
lscpu
```

18. Enable and start the Docker service.

```
systemctl enable docker
systemctl start docker
```

Uninstalling the SANnav Management Portal Appliance

To uninstall the SANnav appliance, perform the following steps.

1. Power off the virtual machine (VM).
2. Delete the VM.

Additional Scripts for Managing SANnav

The SANnav installation provides additional scripts for stopping and starting the server, checking the server status, and more. Run these scripts only if necessary.

The following table lists the user-executable scripts that provide additional ways to customize and manage SANnav. These scripts apply to both standard and OVA installations.

When you run these scripts, SANnav services must be up and running. Exceptions are noted in the table.

All scripts are located in the `<install_home>/bin` folder.

All scripts include a `--help` argument, which shows detailed usage guidelines for the script.

Table 12: SANnav User-Executable Scripts

Script	Description
`add-ldap-server`	Adds the LDAP server host entry to the Docker container host file. Run this script if you are using an LDAP server for authentication.
`change-ipv4-installation-to-ipv6.sh`	Changes SANnav from an IPv4 installation to an IPv6 installation.
`check-sannav-status.sh`	Checks the status of the SANnav server.
`install-sannav.sh`	Installs the SANnav server. SANnav should not be running when you execute this script.
`manage-sannav-whitelisting.sh`	Creates and manages a whitelist of IP addresses that are allowed SANnav access. Refer to the *Brocade SANnav Management Portal User Guide* for additional details.
`merge-files.sh`	Merges files previously split by the `split-file.sh` script.
`replace-kafka-certificates.sh`	Replaces Kafka self-signed certificates with third-party signed certificates.
`replace-server-certificates.sh`	Replaces SSL self-signed certificates with third-party signed certificates.
`restart-sannav.sh`	Stops the currently running SANnav server and then starts it.
`sannav-management-console.sh`	Allows you to perform several actions on the SANnav server without having to access and run scripts individually.
`show-sannav-configurations.sh`	Displays SANnav port and server configurations.
`split-file.sh`	Splits a large SANnav support data collection file into smaller files for faster transmission over the network.
`start-sannav.sh`	Starts the SANnav server after it has been stopped. SANnav should not be running when you execute this script.
`stop-sannav.sh`	Stops the currently running SANnav server.
`uninstall-sannav.sh`	Uninstalls the SANnav server.
`update-events-purge-settings.sh`	Changes the maximum number of days that events are retained or the maximum number of events that are stored in the database.
`update-reports-purge-settings.sh`	Changes the number of days after which reports are automatically deleted.
`update-storage-auto-enclosure-feature.sh`	Enables and disables automatic storage enclosure creation during fabric discovery. By default, this feature is enabled.
`usage-data-collection.sh`	Configures whether collected SANnav usage data is sent to Broadcom.

SANnav Management Console

The `sannav-management-console.sh` script allows you to perform several actions on the SANnav server without having to run individual scripts.

Using this one script, you can perform the following actions:

- Check SANnav status.
- Restart SANnav.
- Stop SANnav.
- Start SANanv.
- Uninstall SANnav.
- Show the SANnav port and server configuration.

Go to the `<install_home>/bin` folder and run the following script:

```
./sannav-management-console.sh
```

You are presented with a list of options from which to choose.

Checking the Server Health

After the installation is complete, you can check the health of the SANnav server using the `check-sannav-status.sh` script. If any of the services is down, it is listed in the script output.

To check the health of the server, go to the `<install_home>/bin` folder and run the following script:

```
./check-sannav-status.sh
```

> **NOTE**
> If any service is found down while checking the server health status, it is automatically started by system-monitor within 20 minutes.

The following is sample output of a healthy server.

```
-bash-4.2# sh ./check-sannav-status.sh
SANnav server is healthy. All the services are currently in running state.
```

The following is sample output of an unhealthy server.

```
-bash-4.2# sh ./check-sannav-status.sh
Following services are currently down or starting
filters-middleware
topology-middleware
```

Changing the Self-Signed Certificates for Client and Server Communication

You can replace the SSL self-signed certificates with third-party signed certificates.

Make sure that the SSL certificate and key files are copied to this host or VM. Go to the `<install_home>/bin` folder and run the following script:

```
./replace-server-certificates.sh
```

When you run this script, SANnav is automatically restarted for the new certificates to take effect.

Changing the Self-Signed Certificates for Kafka Brokers

By default, when SANnav is installed, self-signed certificates for Kafka are generated; these certificates are valid for two years. You can replace the self-signed certificates with third-party signed certificates.

Ensure that the following requirements are met before you run the script:

- The common name (CN) of the certificate must match the fully qualified domain name (FQDN) of the host.
- If you have root and intermediate CA certificates, they must be chained into a single certificate.

Go to the `<install_home>/bin` folder and run the following script:

```
./replace-kafka-certificates.sh
```

When you run this script, SANnav is automatically restarted for the new certificates to take effect. After the server is back up, you must rediscover or unmonitor and then monitor all switches that are registered for telemetry data; otherwise, the new certificates do not take effect.

Configuring a Firewall for SANnav

Perform the following steps to set up a firewall using firewalld. This example uses Red Hat Enterprise Linux (RHEL).

1. Start the firewall using the following command.
   ```
   systemctl start firewalld
   ```
2. Check that the firewall is running.
   ```
   systemctl status firewalld
   ```
3. Enable the firewall automatically after a system reboot.
   ```
   systemctl enable firewalld
   ```
4. Add the SSH service to the trusted zone.
   ```
   firewall-cmd --zone=public --permanent --add-service=ssh
   ```
   If any other default ports are customized, add the services for those ports as well. For example, if you are using HTTPS port 443, enter the following command:
   ```
   firewall-cmd --zone=public --permanent --add-service=https
   ```
5. Add ports using the following commands.
   Note that in the following commands, `public` is the default zone. If your default zone is different, use your default zone for the ports.
   ```
   firewall-cmd --zone=public --add-port=2377/tcp --permanent
   firewall-cmd --zone=public --add-port=7946/tcp --permanent
   firewall-cmd --zone=public --add-port=7946/udp --permanent
   firewall-cmd --zone=public --add-port=4789/udp --permanent
   ```
6. Associate the interface (if this is not done already) with the default profile.
   ```
   firewall-cmd --permanent --zone=public --change-interface=<interface_name>
   ```
7. After the ports are added, use the following command to reload the firewall configuration.
   ```
   firewall-cmd --reload
   ```
8. Verify whether the configuration is correct.
   ```
   firewall-cmd --list-all
   ```

Revision History

SANnav-21x-Install-IG102; 28 August 2020

- In the chapter Migration Overview, the following changes were made:
  - Updated the migration support table to include 2.1.0a.
  - Added the section Upgrading the SANnav Internal SFTP/SCP Server SSH Key.
- In the section System and Server Requirements for SANnav Management Portal, the following changes were made:
  - Added RHEL 7.8 and CentOS 7.8 to the list of supported operating systems. Version 7.8 is supported in SANnav 2.1.0a and higher.
  - Added the requirement that the OS language must be English and the locale must be US.
- In the section Installation Prerequisites, removed the statement about ensuring that the entire physical server must run on a single partition. This is not applicable.
- Added the section Configuring the Firewalld Backend for CentOS and RHEL 8.0 or Higher.
- In the chapter SANnav Management Portal OVA Deployment, the following changes were made:
  - Added support for CentOS 8.1. Version 8.1 is supported in SANnav 2.1.0a and higher.
  - Added the requirement that the OS language must be English and the locale must be US.

SANnav-21x-Install-IG101; 5 August 2020

- Removed references to the `backuprestore/backup` script. This script is not supported from the CLI.
- In Table 3: SANnav Installation Customizations, the following changes were made:
  - Added a list of ports that are reserved for internal communication in IPv6 mode.
  - Clarified the SSO options.
- In the section System and Server Requirements for SANnav Management Portal, the following changes were made:
  - Added a note that additional disk space is required for SANnav TAR files and extracted files.
  - Added the x86 processor architecture to the system requirements.
- In the section Installation Prerequisites, added a prerequisite to ensure that IP network addresses do not conflict with Docker addresses.
- In the section Installation Prerequisites for the SANnav Management Portal Appliance, the following prerequisites were added:
  - Use either Static or DHCP for dual stacks.
  - Ensure that IP network addresses do not conflict with Docker addresses.
- In the section Installing the SANnav Management Portal Appliance Using vCenter, clarified that SSHD customization is for Linux/VM server management.
- Added the section Expanding Hardware Configurations from 3000 to 15,000 Ports.

SANnav-21x-Install-IG100; 30 April 2020

- Added quick installation checklists, for users who are already familiar with SANnav installation.
- Added support for SANnav Management Portal installation as a virtual appliance (OVA).
- Multi-node installation is no longer supported.


BROADCOM®