Brocade® SANnav™ Management Portal Installation and Migration Guide, 2.2.0x

Installation Guide
15 December 2021

Table of Contents

Introduction

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.

Within this document, SANnav Management Portal might also be referred to simply as "SANnav".

Quick installation checklists are provided for users who are familiar with SANnav installation. See SANnav Installation and Migration 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 Vision 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 that 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 or solution provider, contact your OEM or solution provider for all your product support needs.

- OEM and 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 or 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 or solution provider.

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

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com. (You must initially register to gain access to the Support portal.) Once registered, log on and then select **Brocade Products**. You can now navigate to the following sites: • **Case Management** • **Software Downloads** • **Licensing** • **SAN Reports** • **Brocade Support Link** • **Training & Education**	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

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; topic heading; publication number and page number (for PDF documents); URL (for HTML documents); and as much detail as possible.

SANnav Installation and Migration Checklists

Checklists are provided for experienced users who are familiar with SANnav installation.

For all other users, start with Migration from an Earlier Release or SANnav Management Portal Deployment.

Installation Checklist

The following table provides a 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.	See System and Server Requirements for SANnav Management Portal.
2	Review and comply with the installation prerequisites.	See Installation Prerequisites.
3	Ensure that the required ports are open in the firewall.	See Port and Firewall Requirements for SANnav Management Portal.
4	Configure the `firewalld` backend if you are using RHEL 8.2 or higher.	See Configuring the Firewalld Backend for RHEL 8.2 or Later.
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 SANnav status.	`<install_home>/bin/check-sannav-status.sh`

Migration Checklist

The following table provides a 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.	See System and Server Requirements for SANnav Management Portal.
3	Review and comply with the installation prerequisites.	See Installation Prerequisites.
4	Ensure that the required ports are open in the firewall.	See Port and Firewall Requirements for SANnav Management Portal.
5	Configure the `firewalld` backend if you are using RHEL 8.2 or higher.	See Configuring the Firewalld Backend for RHEL 8.2 or Later.
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 SANnav status.	`<install_home>/bin/check-sannav-status.sh`
10	Clear the browser cache, and restart the SANnav client (browser).	Close the previous version of the SANnav client (browser), and clear the browser cache before launching the new version of SANnav.

SANnav OVA Installation Checklist

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

#	Item	Description
1	Review and comply with the installation prerequisites.	See 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 location of the ESXi.
3	Deploy the SANnav OVA package.	Log on to vCenter and deploy the OVF template. See Installing the SANnav Management Portal Appliance Using vCenter.
4	Power on the VM, and then log on as the "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 on.
5	Install SANnav.	After you log on to the VM, the SANnav installation script starts automatically.
6	Check the SANnav status.	`<install_home>/bin/check-sannav-status.sh`

SANnav OVA Migration Checklist

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

#	Item	Description
1	Back up the current SANnav installation, and save it in a location outside of the current VM.	Refer to the *Brocade SANnav Management Portal User Guide* for instructions.
2	Review and comply with the installation prerequisites.	See Installation Prerequisites for the SANnav Management Portal Appliance.
3	Stop the SANnav server.	`<install_home>/bin/stop-sannav.sh`
4	Copy the MAC address of the current SANnav VM.	This MAC address must be provided at the time of migration while associating the disk. If you do not manually update the MAC address on the new VM, then the license is not migrated from the previous SANnav installation.
5	Power off the VM.	—
6	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 location of the ESXi.
7	Deploy the SANnav OVA package.	Log on to vCenter and deploy the OVF template. Do not power on the VM after deploying.

#	Item	Description
8	Attach the VMDK file from the earlier version of SANnav as a new disk.	See Attach the VMDK file from the earlier version of SANnav.
9	Modify the MAC address of the new SANnav VM.	See Modify the MAC address of the new SANnav VM.
10.	Power on the VM, and then log on as the "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 on.
11.	Install SANnav.	After you log on to the VM, the SANnav installation script starts automatically.
12.	Check the SANnav status.	`<install_home>/bin/check-sannav-status.sh`

Migration from an Earlier Release

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.

NOTE

- Other than being prompted to migrate your data, the migration steps are the same as the installation steps.
- Before starting migration, you should back up the current SANnav installation.
- Make sure that you have a valid license before starting migration.

When you migrate the data, the following actions occur:

- Installation settings (such as port customizations) from the previous installation are preserved. The installation does not prompt you for these settings.
- The license key is carried forward to the new installation and is converted to a license certificate. After migration, you do not need to apply a new license. See SANnav License Migration for additional details.
- The discovered fabrics are rediscovered.
- User-configured data, customized data, and historic data (such as port performance metrics and events) are migrated. Note that only the most recent one million events and violations are migrated.
- Imported firmware files are migrated.
- Certificates are migrated or regenerated. If a certificate is self-signed, it is replaced with a newly generated self-signed certificate with a 13-month validity. Third-party certificates that are migrated are valid for the remainder of their original validation period.

  Starting in SANnav 2.2.0, a single set of certificates is used for both SANnav client-to-server communication and telemetry data streaming.
  - SANnav server certificate – This certificate is used for SANnav client-to-server communication. If the previous SANnav installation had installed CA signed certificates, they are migrated to the new installation. If the previous installation was using original self-signed certificates, they are replaced with newly generated self-signed certificates. After migration, these certificates are used for both client-to-server communication and telemetry data streaming.
  - Southbound streaming certificate (KAFKA certificate) – This certificate is used for telemetry data streaming from a SAN switch to the SANnav server. This certificate is not migrated. In the new installation, the SANnav server certificate is used for both client-to-server installation and telemetry data streaming.
  - Northbound streaming certificate – This is the public certificate of the external server to which SANnav is streaming telemetry data. This certificate is migrated to the new installation.
- Data-streaming-enabled switches that were streaming data before the migration continue to stream data after the migration within 10 minutes of the SANnav server startup.

Note that the following items are *not* migrated:

- Event action policies.
- Events filters (Events and Violations). Note that saved inventory filters are migrated.
- Events that occurred more than 30 days ago.
- Flows and related flow data.
- 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 User Guide* for instructions.
- Rename all accounts with user names "none" or "na" (case insensitive) prior to migration. SANnav 2.2 does not support these user names.
- 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.
- If you are migrating from a VM or bare metal SANnav Management Portal installation that was restored from a backup that was saved from an OVA installation, make sure that the property **sannav.ova** is set to **false** in the `<install_home>/conf` file. This property must be set to false for the migration to be successful.
- Check the list in Ports Required for SANnav Installation, and ensure that the required ports are free.

OS Upgrade Options

See System and Server Requirements for SANnav Management Portal for the supported operating systems.

If you want to migrate SANnav but you are running an operating system that is unsupported by the new version, 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.

SANnav License Migration

Starting in SANnav 2.2.0, a license certificate (XML file) is used instead of a license key. Any previously issued and installed license keys will not work in SANnav 2.2.0 and higher.

During migration, SANnav sets the existing license key to the "Released (Active)" state. When the new SANnav 2.2.0 is started up, SANnav attempts to connect to the licensing portal and, if successful, converts the existing license key to a new license certificate.

If SANnav cannot connect to the licensing portal, the existing license key is valid for 30 days. During this 30-day period, you must obtain the rehosting key from the SANnav 2.2.0 licensing details page and use this key to generate a new license certificate from the licensing portal.

Note that only the active license key is migrated. Any inactive licenses are not migrated.

If the license is a trial license, after migration the license is valid on the new SANnav version for the remaining days of the trial period.

If the license has expired, the migration is allowed, but you cannot use the new SANnav version until you apply a new license.

Migration Paths

You can migrate from the two previous versions.

The following table lists the software versions and whether migration is supported.

Table 1: Supported Migration Paths for SANnav Management Portal

Current Version	Migration Version	Supported?
SANnav 2.1.1x	SANnav 2.2.0x	Yes
SANnav 2.1.0x	SANnav 2.2.0x	Yes
SANnav 2.0.0x or earlier	SANnav 2.2.0x	No

You cannot migrate from an OVA installation to a VM or bare metal installation. The following table lists the OVA installations and whether migration is supported.

Table 2: Supported Migration Paths for SANnav OVA Installation

Current Version	Migration Version	Supported?
SANnav 2.1.1x OVA installation	SANnav 2.2.0x OVA installation	Yes
SANnav 2.1.0x OVA installation	SANnav 2.2.0x OVA installation	Yes
SANnav VM or bare metal installation	SANnav OVA installation	No
SANnav OVA installation	SANnav VM or bare metal installation	No

If your SANnav server is a dual-stack IPv4/IPv6 deployment, you cannot migrate to an IPv4-only deployment. The following table lists the migration paths for the various SANnav deployments.

Table 3: Supported Migration Paths for SANnav System Configurations

Current Deployment	Migration Deployment	Supported?
SANnav IPv4 deployment	SANnav IPv4 deployment	Yes
SANnav IPv4 deployment	SANnav dual-stack IPv4/IPv6 deployment	Yes
SANnav dual-stack IPv4/IPv6 deployment	SANnav dual-stack IPv4/IPv6 deployment	Yes
SANnav dual-stack IPv4/IPv6 deployment	SANnav IPv4 deployment	No

Features Affected By Migration

The following table lists SANnav features and how they are affected by migration to SANnav 2.2.

Table 4: SANnav Features Affected By Migration

Feature	Effect of Migration
Backup and Restore	• After migration, any backups that were previously taken are not displayed in the **Outputs** list. The list is empty. • If the name of a scheduled backup file contains a space, after migration the space is removed.
Configuration Policies	**Configuration policy definition:** • JSON text representing the Basic configuration and MAPS configuration blocks is parsed and created as block sets and configuration blocks as per the new database schema. • JSON text representing the MAPS policy is parsed and created as a new SANnav MAPS Policy block set. • Policy details information is created as a new policy definition in the database schema. • Switch associations are migrated and created as per the new database schema. • Policy monitoring information is migrated and populated into the new database schema. **Drifts:** • After the policy and block set definitions are migrated, SANnav performs a drift calculation and updates the drifts for all policies.
Dashboards and Reports	The following dashboard widgets are deprecated. After migration, these widgets are empty in any dashboards that contain them. • ISL Port Out Of Range Violations • Port Out Of Range Violations • Target Port Out Of Range Violations For host or storage port report templates, after migration the column name **Symbolic Name** is replaced with **Port Symbolic Name**. For switch report templates, after migration the column names **FCIP** and **FCIP Mask** are renamed **IPFC IPv4 Address** and **IPFC IPv4 Netmask**. Deprecated report widgets are removed from the report template after migration. If the template contains only deprecated widgets, that template is deleted after migration. All user-defined network scopes are deleted after migration. Any template or report that was created with a user-defined network scope defaults to the **All** scope after migration.
Fault Management	• On the **SANnav Email Setup** page, if **All users enabled for notification** was selected for the **Send Test Email** option, after migration the **Test Email** checkbox is cleared. • The email notification option is not migrated. If **Enable Email Event Notifications** was selected on the **Preferences** page, after migration this option is cleared, and you must re-enable notifications. • All forwarding destinations are removed. You must add destinations and filters manually after migration. • Events policies are not migrated. • Events that occurred more than 30 days ago are not migrated.
Filters	Filter definition preferences are updated to have an OR condition after migration.
Flow Management	• Historical statistics of flows, collection aggregation, and flow violations are not migrated. After migration, you must re-enable the collection. • The LUNWWN filter is not supported. After migration, for any reports that use this filter, the filter is ignored. • Some report columns are no longer supported and are removed. • The following flow report widgets are no longer supported and must be removed: — Time Series - Flow Violations — Top Flow Violations — Top Host Port Read Oversubscription — Top SCSI Errors

Feature	Effect of Migration
Health Summary Dashboard	A new health computation parameter, **Default MAPS base policy is enabled**, is enabled by default after migration.
Licensing	See SANnav License Migration for details.
User Management	Any accounts with user names "none" or "na" (case insensitive) must be renamed prior to migration. SANnav 2.2 does not support "none" or "na" as a user name.
Zoning	Offline zones and zone configurations are not visible after migration. You must use the **Save to Switch** option on these offline objects before starting the migration. Tags and descriptions of up to 10,000 zone entities are migrated. Above 10,000 zone entities, the tags and descriptions are lost.

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 upgrades to the latest version of the OS. If you upgrade to an unsupported OS, the supportability depends on the compatibility of SANnav with that OS. The upgrade is allowed, but requires user agreement.

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.

> **NOTE**
> If you already upgraded the SSH key to the new RSA key in the previous SANnav installation, you do not need to perform these steps.

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:

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 on 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

SANnav Management Portal supports deployment on RHEL or CentOS sesrvers with FIPS mode enabled.

The SANnav Management Portal 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.
- 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 Management Portal to function properly. The list of ports is provided in Port and Firewall Requirements for SANnav Management Portal.

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

After installation, if you choose to move SANnav Management Portal 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.

SANnav Installation Customization

During SANnav 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. Some of the customizations can be changed after installation. See SANnav Management Console for information.

Table 5: SANnav Installation Customizations

Item	Description	Change After Installation?
Docker IP address range	By default, Docker uses an IP address range of 192.168.255.240/28. You can change to another address range during installation.	No
Docker installation directory	The default home directory for installing Docker is `/var/lib/docker`, but you can change to another directory during installation.	No
Swap space	SANnav Management Portal 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.	No

Item	Description	Change After Installation?
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 (dual-stack) communication.	Yes
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 log on to SANnav. **NOTE:** If you disallow HTTP to HTTPS redirection, either during or after installation, Firefox continues to redirect from HTTP to HTTPS. This is due to a limitation in Firefox.	Yes
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.)	Yes
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 on to the switch when launching Web Tools for switches running Fabric OS 9.0.0 or higher. • 0 for always log on manually. SANnav prompts you for switch login credentials. • 1 to log on with switch credentials. SANnav does not prompt you, but attempts to log on to the switch using the credentials that SANnav used when discovering the switch. • 2 to log on with user credentials. SANnav does not prompt you, but attempts to log on to the switch using the credentials that the user used when logging on to SANnav. For switches running Fabric OS versions earlier than 9.0.0, SANnav always prompts you to log on to the switch when launching Web Tools, regardless of the SSO settings. Note that if you enter **2** (log on with user credentials), and if the credentials are managed by LDAP, then SSO does not work. The LDAP passwords are not saved in the SANnav database.	Yes
Preferred IP address for SANnav client and server communication	A list of configured public IP addresses is displayed, from which you can select the preferred IP address. If you select option 0 ("Any"), a SANnav client can be accessed through any configured IP address.	Yes
Preferred IP address for SANnav server and SAN switch communication	A list of configured public IP addresses is displayed, from which you can select the preferred IP address.	Yes
Port customization	You can customize ports when installing SANnav. 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:** See Port and Firewall Requirements for SANnav Management Portal for a list of ports that are reserved for internal communication. Do not use any of these ports for customization.	Yes (SSH port) No (other ports)
Database password	You must provide a password for the SANnav database (Postgres database). There is no default password. The default database user name is "dcmadmin".	Yes

Item	Description	Change After Installation?
SCP/SFTP password	You provide a password for the SANnav internal SCP/SFTP server. There is no default password.	Yes
SANnav security password	This password is used for enhanced security of SANnav infrastructure service components. You must provide a password. There is no default.	No
License autorenewal	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.	Yes
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. You can change this setting during or after installation.	Yes

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 by following the instructions in the installation script.

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

Table 6: 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): 8.4, 8.2, and 7.9 • CentOS 7.9 Language = English, Locale = US **Note:** Future minor versions of RHEL and CentOS are supported, but have not been tested.	
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

Requirement	Base License or Enterprise License with up to 3000 Ports	Enterprise License with up to 15,000 Ports
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 7: Installation Prerequisites

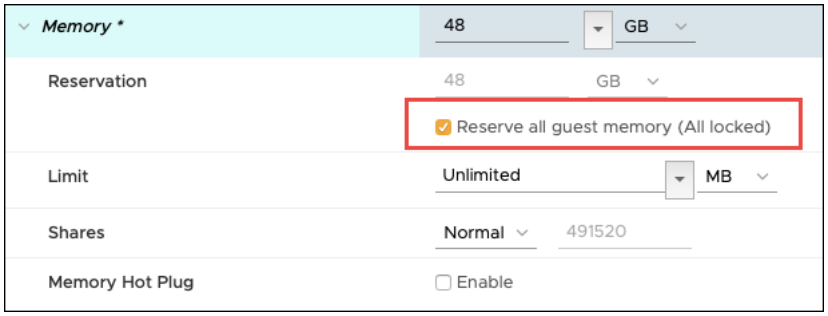
Task	Task Details or Additional Information
Gather necessary information and components.	Make sure that you have the following information: • Root user credentials. You must log on to the SANnav server as the root user or a user with root privilege. • The SANnav Management Portal server IP address.
Uninstall 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.
Ensure that IP network addresses do not conflict with Docker addresses.	SANnav comes with Docker preinstalled. By default, Docker uses an IP address range of 192.168.255.240/28. If you are using IPv4, then when choosing your VM IP address and gateway, do not use an address in this range. If you do, although the deployment may be successful, the IP address will be unreachable. IPv6 connectivity is not affected. The installation script allows you to change the default Docker address range to a different address range.

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 verifying that `ftype=1` . The default Docker installation directory is `/var/lib`.
Set umask.	"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 extract the installation files before setting the umask, you must delete the installation folder, run `umask 0022` , and unzip the files again.

Task	Task Details or Additional Information

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. A best practice is to use the `netstat` command to check if the port is in use.
	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.

Check port 80 availability.	Port 80 must be available if you allow redirection of HTTP port 80 to HTTPS. After installation, port 80 must continue to be available all the time; otherwise, you cannot start (or restart) SANnav.
Check additional port requirements.	See Port and Firewall Requirements for SANnav Management Portal for other ports that must be open.
Allocate memory in the VM.	(Optional) If you are installing SANnav on a VMware-based virtual machine, select **Reserve all guest memory** to ensure that the vitual machine gets all the required memory preallocated. This setting ensures that the memory that you are allocating is not shared with other guests in the ESXi and helps to avoid high memory utilization by SANnav. 
Set the time zone.	Make sure that the time zone of the server is set correctly before starting SANnav installation. If the time zone is set to "n/a", SANnav database installation fails.

Start the `rngd` service.	SANnav relies on the operating system to generate secure random numbers. The server must have the `rngd` service running to avoid performance degradation. Before starting the installation, run the following commands to install `rng` tools and start the `rngd` service in Linux.
	`yum install rng-tools`
	`systemctl start rngd.service`
	`systemctl enable rngd.service`

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. • Enter the `ifconfig` command to verify that the MTU size is at least 1500.

Configuring the Firewalld Backend for RHEL 8.2 or Later

In RHEL 8.2 and higher, the `firewalld` backend defaults to using "nftables" instead of "iptables." Docker does not have native support for nftables.

If you are installing SANnav on RHEL 8.2 or later 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 `firewalld`.

   ```
   systemctl stop firewalld
   ```

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

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

5. Start `firewalld`.

   ```
   systemctl start firewalld
   ```

6. Reload `firewalld`.

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

Installing SANnav Management Portal

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

Ensure that your system meets the requirements listed in System and Server Requirements for SANnav Management Portal.

> **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. Before you unzip the installation file, be sure to review and comply with the prerequisites listed in Installation Prerequisites.
2. 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.

3. 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.

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

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

5. 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.

6. 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.

7. Read and respond to each prompt carefully.

NOTE
Some installation parameters cannot be changed after installation. If you need to change these parameters after installation, you may need to reinstall SANnav.

As the installation proceeds, the script runs a preinstallation 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 15 minutes.

NOTE
After migration, you must clear the browser cache before launching the new version of SANnav.

Uninstalling 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.

Port and Firewall Requirements for SANnav Management Portal

SANnav Management Portal requires certain ports to be available to ensure proper communication and operation.

Ports Required for SANnav Installation

SANnav uses the following ports. Ensure that these ports are free before starting SANnav installation. If you customize any default ports during installation, do not use these ports.

Table 8: Ports Required for SANnav Installation

Port Number	How the Port Is Used in SANnav	What Happens if the Port Is Not Open	Must Be Open in the Firewall?	Customizable During Installation?
22	Needed for SFTP/SCP.	Switch file transfer operations fail.	Yes	Yes
80	Needed for the SANnav proxy to serve the clients.	The SANnav user interface cannot be accessed using HTTP.	Yes	No
162	Needed for SNMP traps.	SANnav cannot receive traps.	Yes	Yes
443	Needed for the SANnav proxy to serve the clients.	The SANnav user interface cannot be accessed.	Yes	Yes
514	Needed for syslogs.	SANnav cannot receive syslogs.	Yes	Yes
2377	Internal use, for Docker.	Installation fails.	No	No
5432	Internal use, for the database.	Installation fails.	No	No
6060, 6061	Internal use, for the containers.	Installation fails.	No	No.
6514	Needed for secure syslogs.	SANnav cannot receive secure syslogs.	Yes	Yes
7021, 7022, 7051–7057, 7060, 7072, 7080, 7087, 7089, 7090, 7097, 7099, 7100, 7611, 7711, 7890, 7946, 7997	Internal use, for the containers.	Installation fails.	No	No
8021, 8022, 8080, 8081, 8094, 8200	Internal use, for the containers.	Installation fails.	No	No
9090, 9091, 9094, 9097, 9100, 9101, 9300, 9443, 9611, 9711, 9763, 9887, 9888, 9999	Internal use, for the containers.	Installation fails.	No	No
10800–10825	Internal use, for the containers.	Installation fails.	No	No
11111, 11211	Internal use.	Installation fails.	No	No
12181	Internal use.	Installation fails.	No	No
18081, 18082	Schema registry for streaming data from Fabric OS.	Streaming registration fails. Performance data collection fails.	Yes	No
19028	Internal use.	Installation fails.	No	No
19090	Receiving data streams from Fabric OS if the fabric has switches with Fabric OS v8.2.1a.	Installation and performance data collection fails.	Yes	No
19092	Internal use.	Installation fails.	No	No

Port Number	How the Port Is Used in SANnav	What Happens if the Port Is Not Open	Must Be Open in the Firewall?	Customizable During Installation?
19093	Receiving data streams from Fabric OS if the fabric has switches with Fabric OS v8.2.1a.	Installation and performance data collection fails.	Yes	No
19094, 19095	Secure data streaming ports. Receive data streams from Fabric OS if the fabric has switches with Fabric OS v8.2.1b and higher.	Installation and performance data collection fails.	Yes	No
38917	Internal use, for the containers.	Installation fails.	No	No
41185	Internal use, for the containers.	Installation fails.	No	No
42239	Internal use, for the containers.	Installation fails.	No	No
45687	Internal use, for the containers.	Installation fails.	No	No
46537	Internal use, for the containers.	Installation fails.	No	No
47100–47125, 47500	Internal use, for the containers.	Installation fails.	No	No
49112	Internal use, for the containers.	Installation fails.	No	No
55501	Internal use, for the containers.	Installation fails.	No	No

SANnav blocks external access to all nonrequired ports by adding rules in IP tables. After installation, you can close any port that SANnav opened dynamically by executing one of the following commands. In the commands, `protocol` can be either `tcp` or `udp` .

For IPv4:

```
iptables -A SANNAV-CHAIN -i <interface-to-block> -p <protocol> -m <protocol> --dport <port> -j DROP
```

Example: `iptables -A SANNAV-CHAIN -i eth0 -p udp -m udp --dport 2377 -j DROP`

For IPv6:

```
ip6tables -A SANNAV-CHAIN -i <interface-to-block> -p <protocol> -m <protocol> --dport <port> -j DROP
```

Example: `ip6tables -A SANNAV-CHAIN -i eth0 -p udp -m udp --dport 2377 -j DROP`

Ports That Must Be Open in the Firewall

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

If your network utilizes a firewall between the SANnav 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. These ports are added to the IP tables by default when the SANnav server is running. You do not need to open them in `firewalld` if it is enabled and running on the SANnav server.

NOTE

- Ports that were customized during SANnav installation must be open in the firewall.
- The NTP and DNS ports must be open in the firewall.

Table 9: 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.
18081	TCP	Inbound	Switch --> Server	Avro schema registry insecure port (Fabric OS versions lower than 9.0.1). Required to enable Kafka streaming from switches to SANnav.
18082	TCP	Inbound	Switch --> Server	Avro schema registry secure port (Fabric OS 9.0.1 and higher). Required to enable Kafka streaming from switches to SANnav.
19094	TCP	Inbound	Switch --> Server	Secured Kafka port, for IPv4.
19095	TCP	Inbound	Switch --> Server	Secured Kafka port, for IPv6.

If you are using the disaster recovery feature, additional ports must be open in the firewall. See Ports That Must Be Open in the Firewall for Disaster Recovery.

Ports Required for External Authentication

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 10: 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

Port Number	Transport	Inbound/ Outbound	Communication Path	Description
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 can be installed as a virtual appliance, compatible with VMware ESXi versions 6.5 and 6.7.

- Note that deployment of the SANnav virtual appliance is supported only by VMware infrastructure. No hypervisor other than VMware ESXi is supported.
- The SANnav software package contains a SANnav OVA file (`.ova`), which can be deployed to an ESXi discovered in 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.
- CentOS 7.9 is bundled with the SANnav virtual appliance. The language must be English, and the locale must be US.
- 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.

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.

The following table lists the hardware requirements for deploying SANnav Management Portal as an appliance. During installation you select either a **Small** configuration or a **Large** configuration.

If you are migrating from an earlier SANnav version, you can upgrade the operating system before installation, as described in Upgrading the OS with SANnav Installed.

Table 11: System and Server Requirements for the SANnav Appliance

Requirement	Base License or Enterprise License with up to 3000 Ports (Small Configuration)	Enterprise License with up to 15,000 Ports (Large Configuration)
Server package	• VMware ESXi host, 7.x, 6.7, and 6.5 • ESXi 7.x, discovered in vCenter 7.x • ESXi 6.7, discovered in vCenter 6.7 or 7.x • ESXi 6.5, discovered in vCenter 6.7 or 7.x	• VMware ESXi host, 7.x, 6.7, and 6.5 • ESXi 7.x, discovered in vCenter 7.x • ESXi 6.7, discovered in vCenter 6.7 or 7.x • ESXi 6.5, discovered in vCenter 6.7 or 7.x
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 12: Disk Partitions in the SANnav Appliance

Partition Type	Base License or Enterprise License with up to 3000 Ports	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 13: 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: • User name = "root", 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 must use a specific 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. By default, Docker uses an IP address range of 192.168.255.240/28. The installation script allows you to change the default Docker address range to a different address range.

Installing the SANnav Management Portal Appliance Using vCenter

During the installation, you can select a Base or Enterprise configuration. The hardware specifications are configured depending on the selected configuration.

Perform the following steps to install the SANnav Management Portal appliance using vCenter:

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

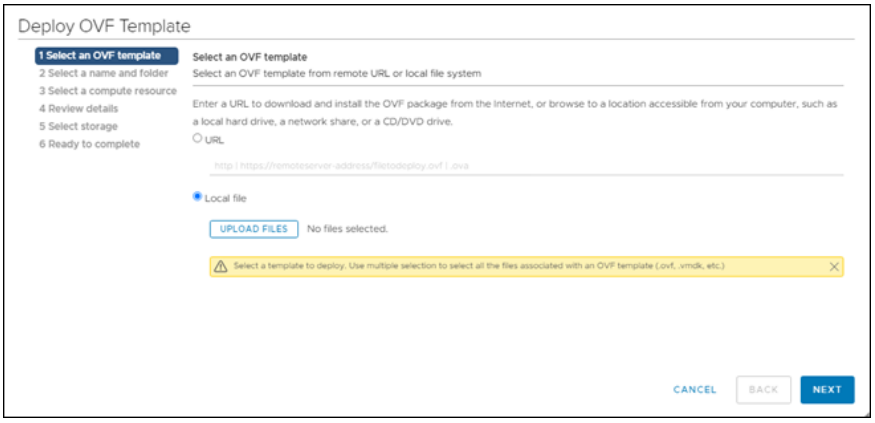
2. Log on to vCenter, right-click the host on which you want to deploy SANnav, and select **Deploy OVF Template**.

   The ESXi host that you select must have enough hardware capability for the configuration (Base or Enterprise); otherwise, OVA deployment fails.

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

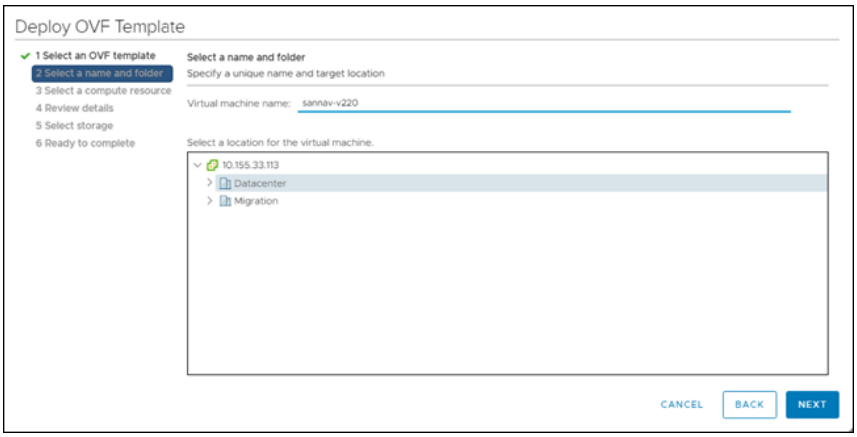
a) **Select an OVF template**.

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



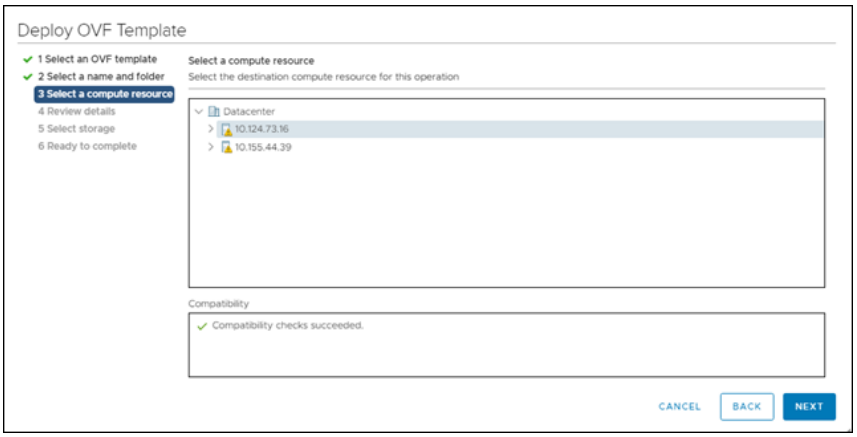
b) **Select a name and folder**.

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



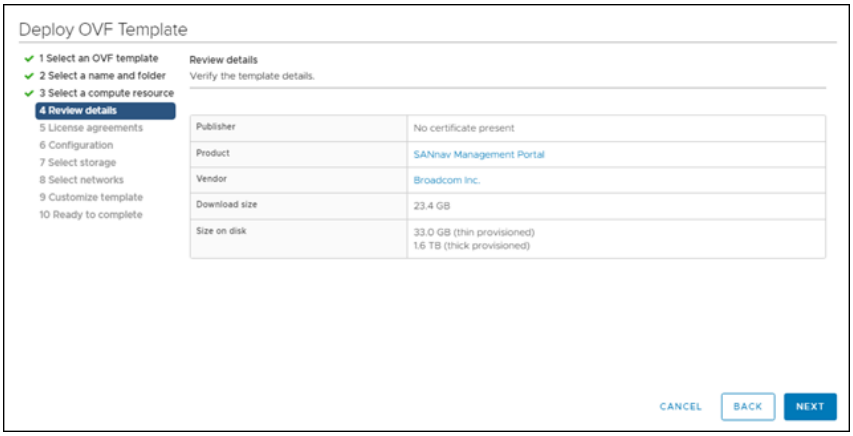
c) **Select a compute resource**.

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



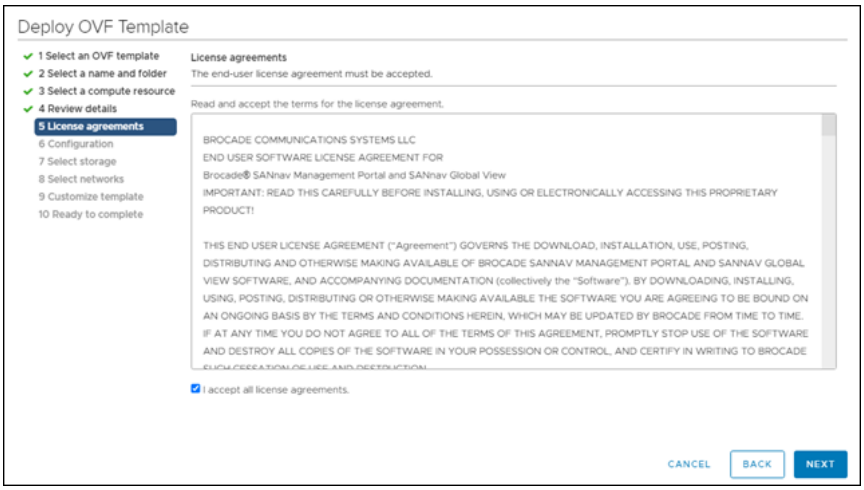
d) **Review details**.

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



e) **License agreements**.

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

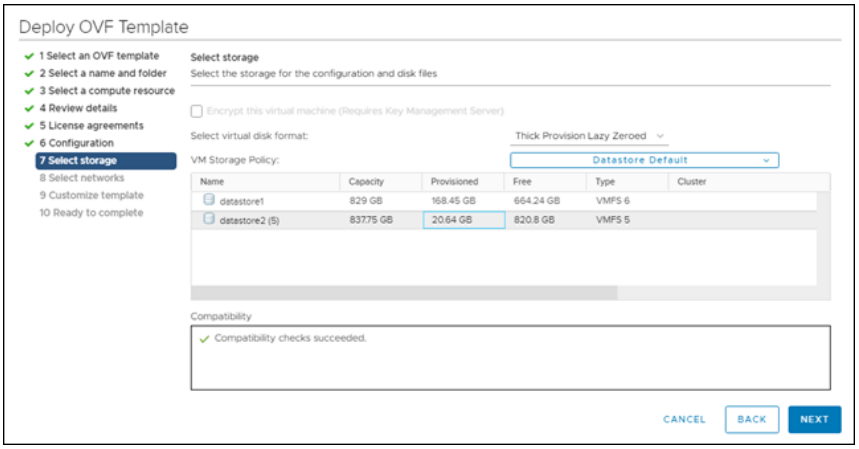


f) **Configuration**.

The **Small** configuration includes 48 GB of memory, which supports the Base License (600 ports) and the Enterprise License (up to 3000 ports). The **Large** configuration includes 96 GB of memory to support an Enterprise License with up to 15,000 ports.

g) **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**.



h) **Select networks**.

Choose the IP allocation strategy and IP protocol:

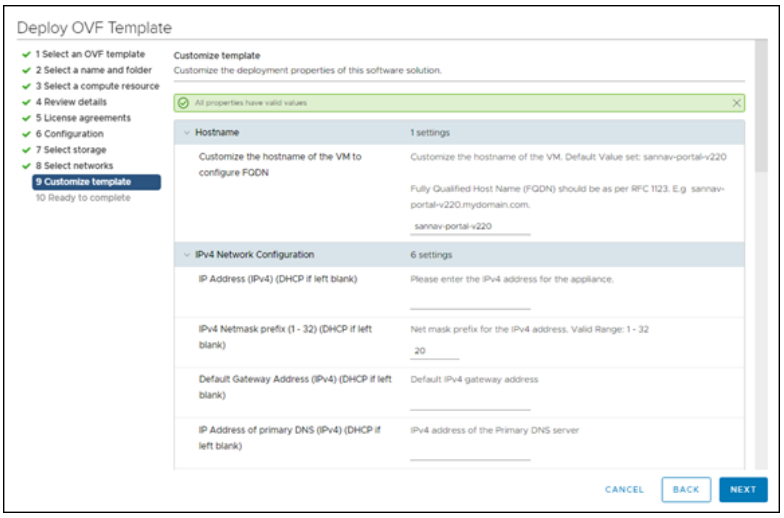
- For **IP allocation**, choose either **DHCP** or **Static - Manual**.
- For **IP protocol**, choose either **IPv4** or **IPv6**.

Click **Next**.

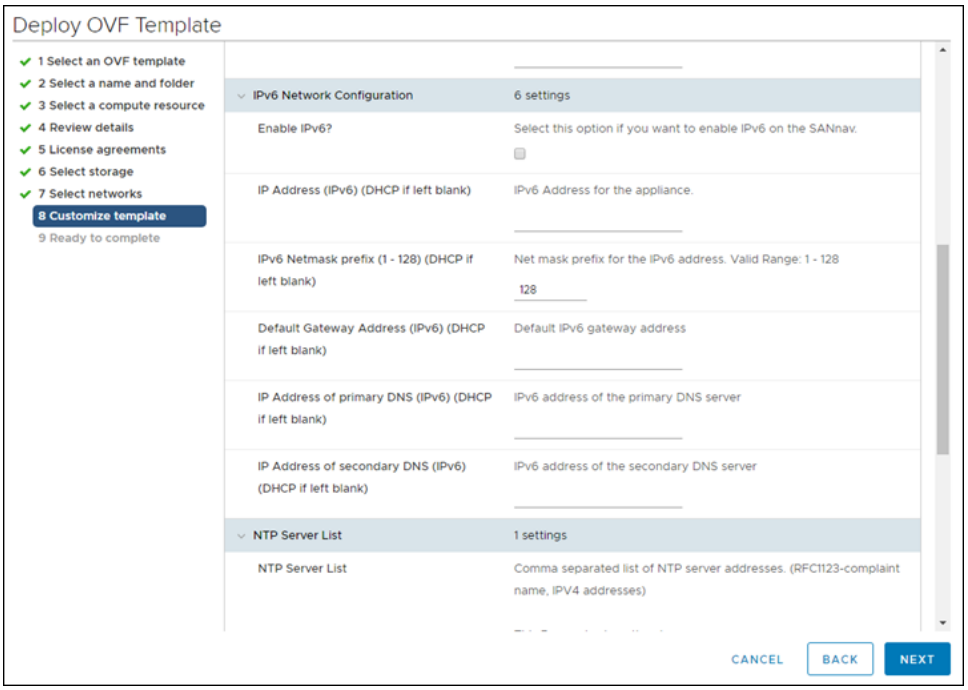
i) **Customize template**.

Provide all values for SANnav customization.

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



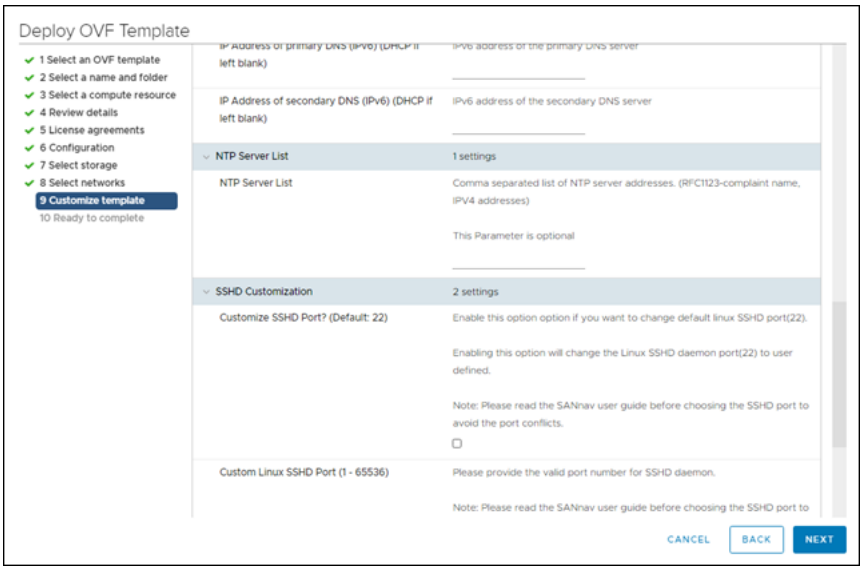
IPv6 Network Configuration: If IP allocation is **DHCP**, leave this section blank. If the IP allocation policy is **Static - Manual**, you must enter the values. Note that the **IP Address of secondary DNS** property is optional.



Host Name: The default host name is set to "sannav-portal-v220". If you want to change this name, you can enter a new name or FQDN.

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.



Application services subnet: This network is used internally. Enter a new IP address range if there are any conflicts with the the default IP address range. The subnet must be at least 28.

Click **Next**.

j) **Ready to complete**.

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

3. After successful network configuration, log in as the root user.

   The SANnav installation script automatically starts. On successful installation, SANnav Management Portal starts on the VM. The startup may take up to 15 minutes.

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

Migrating the SANnav Management Portal Appliance

Before you start the migration, be sure to review and comply with the System and Server Requirements for the SANnav Management Portal Appliance and Installation Prerequisites for the SANnav Management Portal Appliance.

In addition to these requirements, the following prerequisites are specific to migration:

- The ESXi where the SANnav Management Portal appliance is running and where the new SANnav appliance will be deployed should be the same. If this is not possible, then the VMDK file of the current SANnav Management Portal appliance must be accessible from the vCenter datastores.
- At least 630 GB of disk space must be available for deploying the SANnav Management Portal appliance. You can reclaim the disk space that is allocated to the previous version of SANnav Management Portal appliance after you complete the migration and uninstall the earlier version of SANnav.

Perform the following steps to migrate the SANnav Management Portal appliance from a previous version:

1. Back up the current SANnav installation and save it in a location outside of the current virtual machine (VM).
2. Stop the current SANnav server.

   ```
   <install_home>/bin/stop-sannav.sh
   ```

3. Copy the MAC address of the current SANnav VM.

   This MAC address is used during the migration process and is necessary for license migration. If you do not manually update the MAC address on the new SANnav VM, the license is not migrated.
4. Power off the VM.
5. Download the SANnav OVA package to the location from which you want to import to ESXi / vCenter.

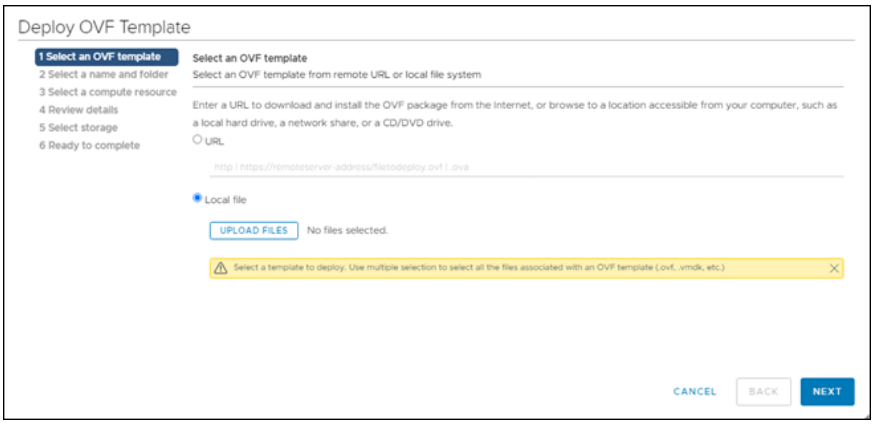
   Note that the time it takes to deploy the SANnav OVA package to the host depends on the network speed between the location to which the OVA package is downloaded and the ESXi.
6. Log on to vCenter, right-click the host on which you want to deploy SANnav, and select **Deploy OVF Template**.

   The ESXi host that you select must have enough hardware capability for the configuration (Base or Enterprise); otherwise, OVA deployment fails.

   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.

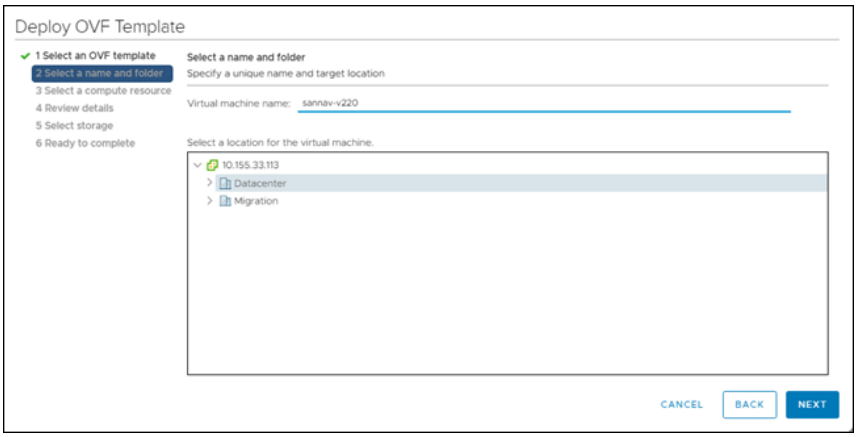
   a) **Select an OVF template**.

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



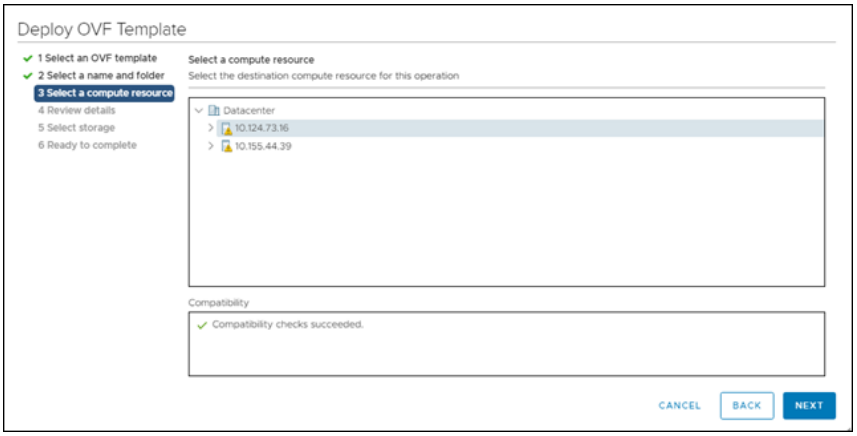
   b) **Select a name and folder**.

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



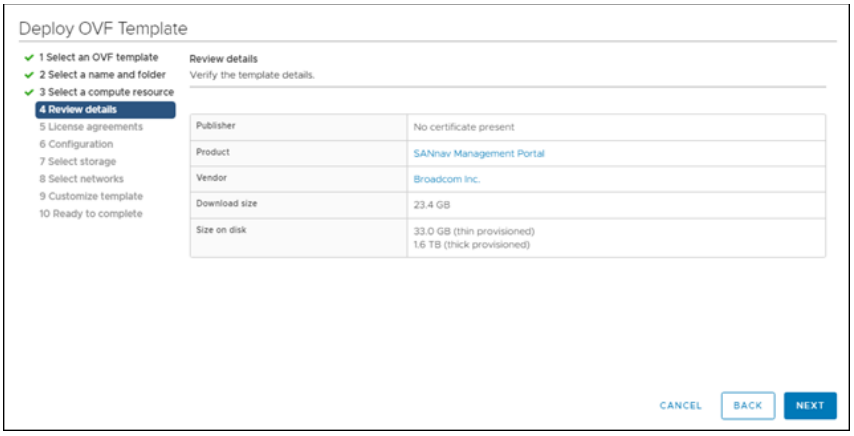
c) **Select a compute resource**.

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



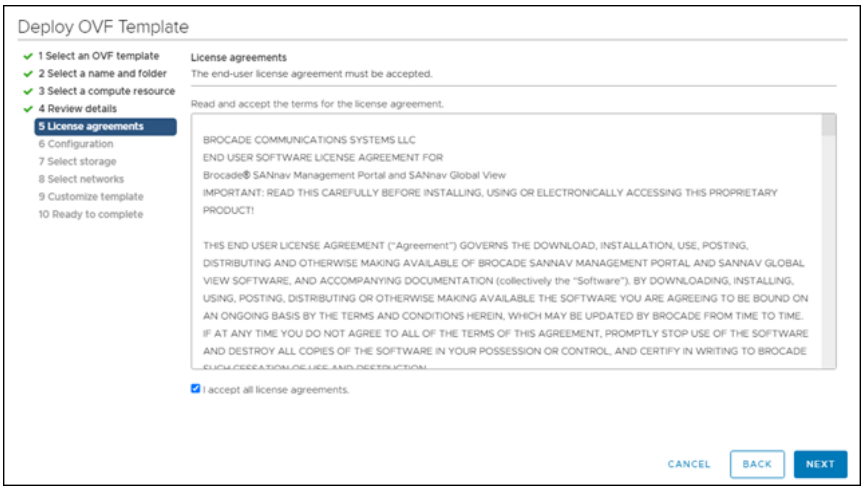
d) **Review details**.

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



e) **License agreements**.

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

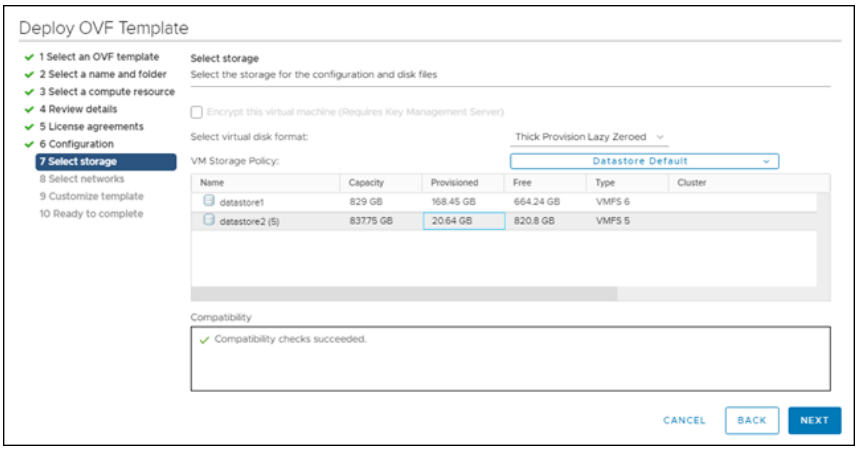


f) **Configuration**.

The **Small** configuration includes 48-GB memory, which supports the Base License (600 ports) and the Enterprise License (up to 3000 ports). The **Large** configuration includes 96-GB memory to support an Enterprise License with up to 15,000 ports.

g) **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**.



h) **Select networks**.

Choose the IP allocation strategy and IP protocol:

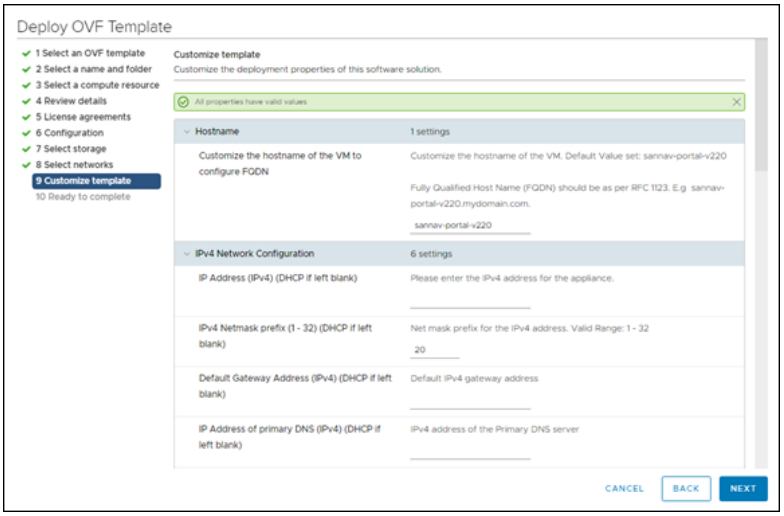
- For **IP allocation**, choose either **DHCP** or **Static - Manual**.
- For **IP protocol**, choose either **IPv4** or **IPv6**.

Click **Next**.

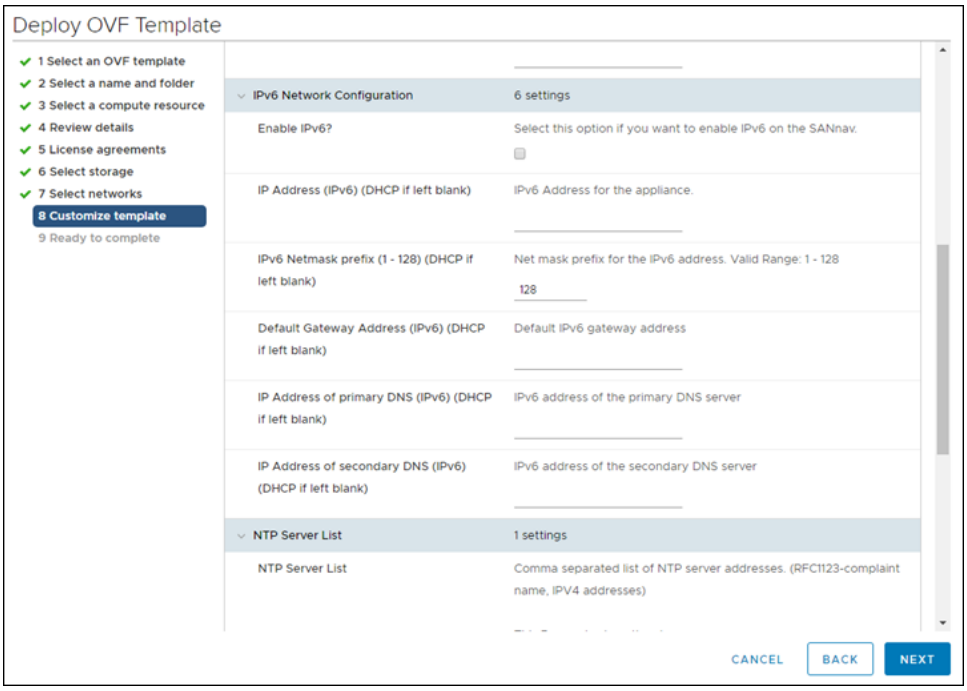
i) **Customize template**.

Provide all values for SANnav customization.

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



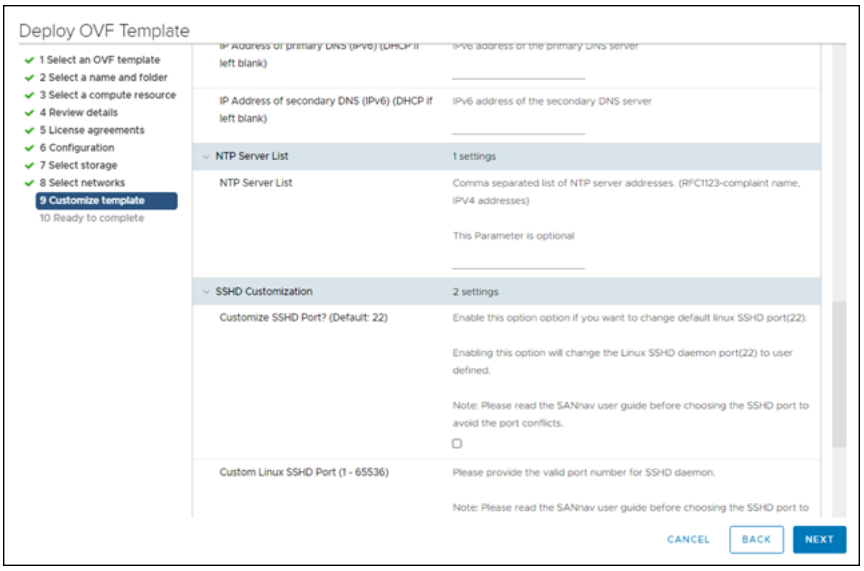
IPv6 Network Configuration: If IP allocation is **DHCP**, leave this section blank. If the IP allocation policy is **Static - Manual**, you must enter the values. Note that the **IP Address of secondary DNS** property is optional.



Host Name: The default host name is set to "sannav-portal-v220". If you want to change this name, you can enter a new name or FQDN.

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.



Application services subnet: This network is used internally. Enter a new IP address range if there are any conflicts with the the default IP address range. The subnet must be at least 28.

Click **Next**.

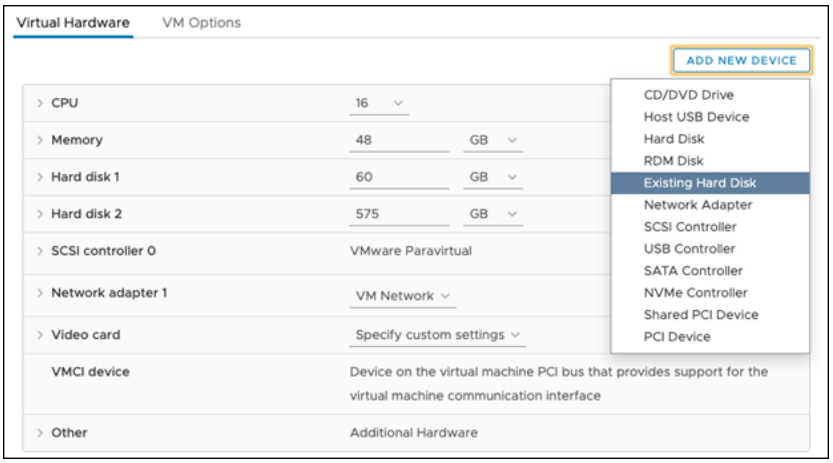
j) **Ready to complete**.

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

NOTE

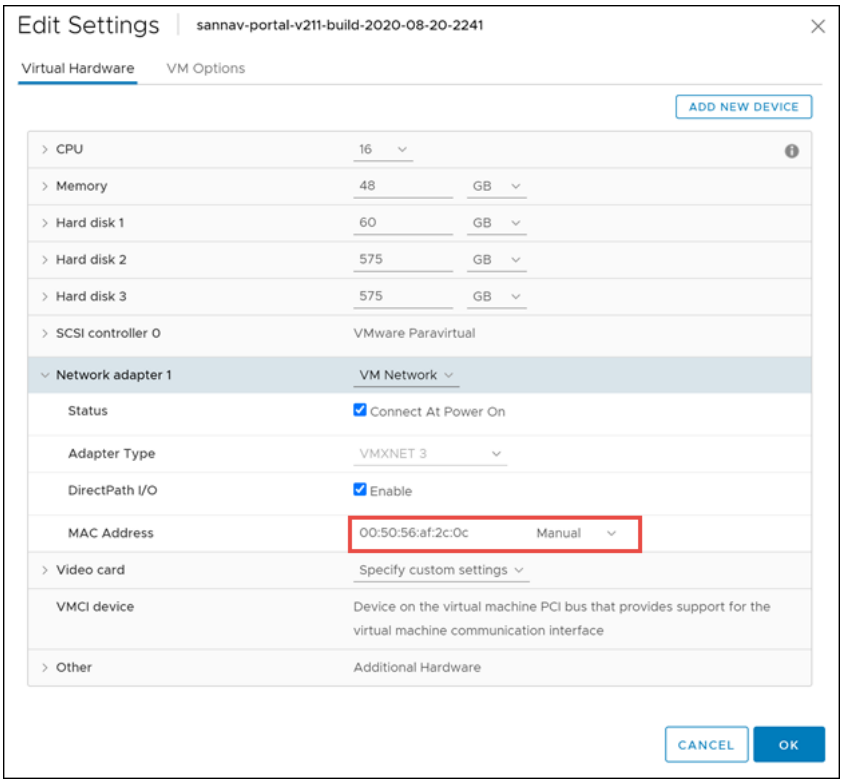
Do not power on the VM at this time.

7. Attach the VMDK file from the earlier version of SANnav as a new disk.
   a) Right-click the newly deployed VM.
   b) Select **Edit Settings > Add New Device > Existing Hard Disk**.



c) Select the datastore in which the VMDK file is stored, and click **OK**.

8. Modify the MAC address of the new SANnav VM.
   a) Right-click the deployed VM and select **Edit Settings**.
   b) Expand the **Network adapter 1** option.
   c) Change the **MAC Address** setting from **Automatic** to **Manual**.
   d) Add the MAC address that you copied earlier from the previous SANnav installation, and click **OK**.



9. Power on the VM.

   After powering on the VM, the SANnav installation script automatically starts if the disk is mounted successfully.

   On successful installation, SANnav Management Portal starts on the VM. The startup may take up to 15 minutes.

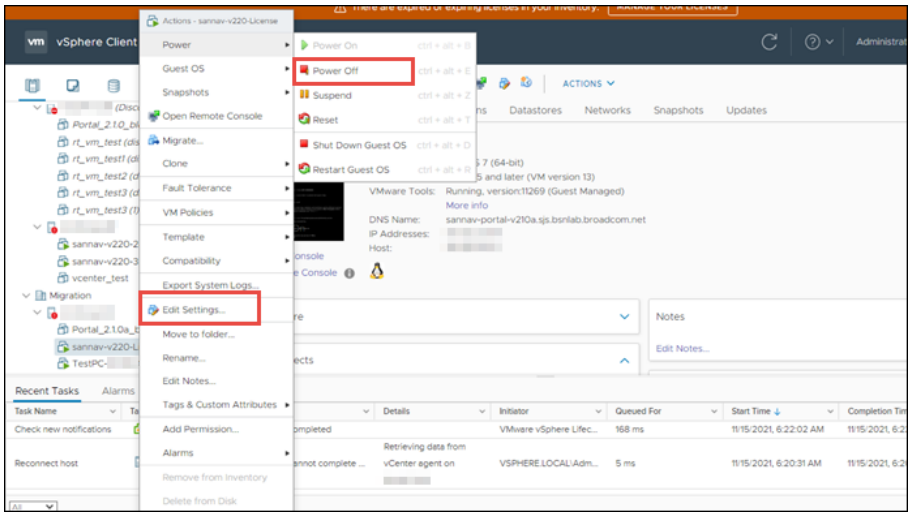
After successful migration, you can use the standard scripts to manage SANnav. See Scripts for Managing SANnav.

If the migration is unsuccessful, see Recovering from Migration Failure of SANnav Management Portal Appliance for instructions on how to return to the previous version.

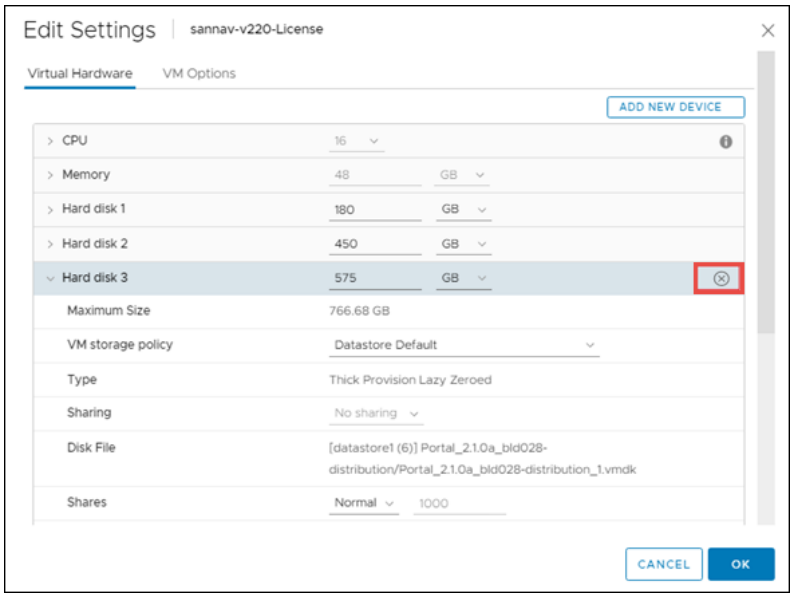
Recovering from Migration Failure of SANnav Management Portal Appliance

If the SANnav Management Portal appliance fails, you can return to the previous version using the following steps:

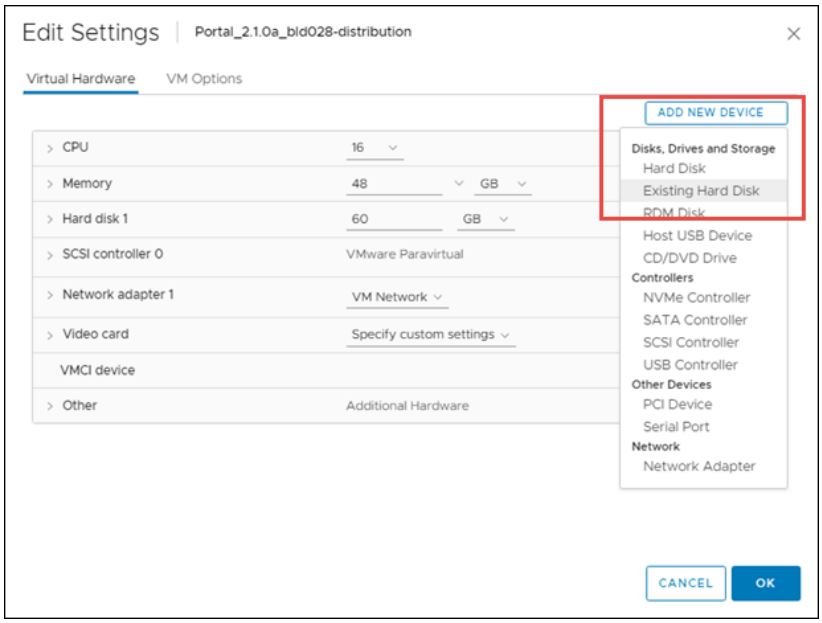
1. Power off the VM, and select the **Edit Settings** option.



2. Detach the source hard disk drive (HDD).



3. Attach the HDD to the source server again.



4. Power on the source server.
5. Log on to the source server, go to `<SANnav_home>/bin`, and run the `start-sannav.sh` script.

Uninstalling the SANnav Management Portal Appliance

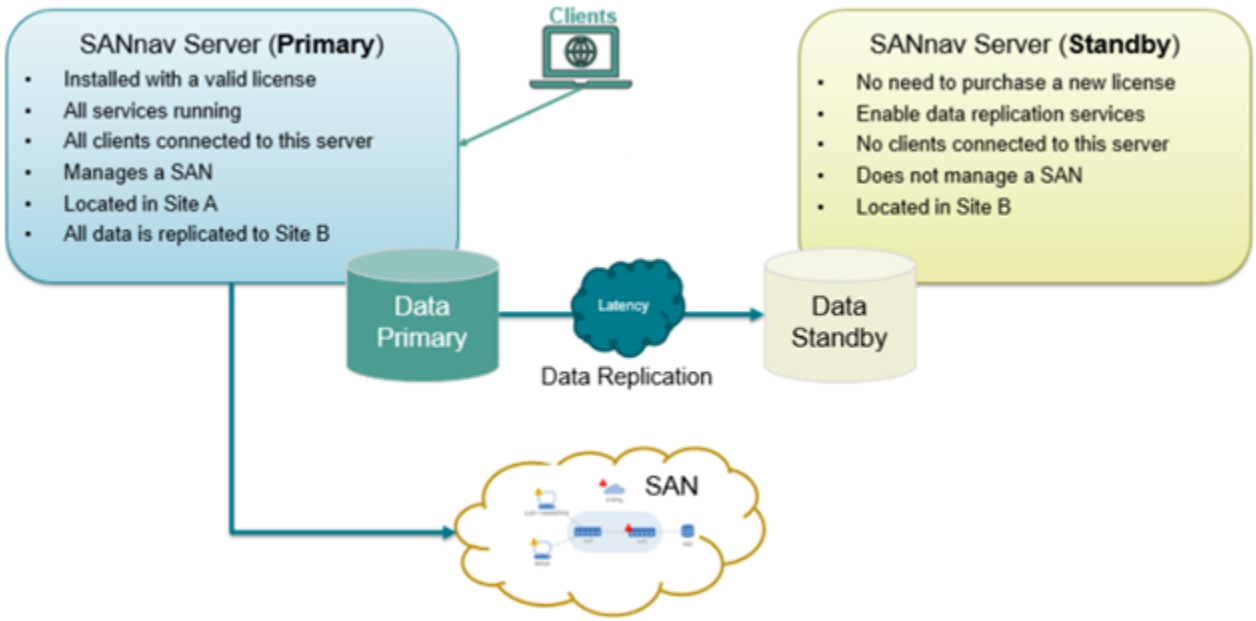
To uninstall the SANnav appliance, perform the following steps.

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

Disaster Recovery

If a system that is running SANnav Management Portal goes down, it can take hours or days to bring up a new system and restore data from a backup. The SANnav disaster recovery feature enables you to install two SANnav servers, a primary and a standby. If the primary server goes down, you can manually fail over to the standby server within minutes.

Figure 1: Disaster Recovery Components



When disaster recovery is enabled, there will be two active VMs with *identical configuration* and reachable to each other over a LAN or WAN:

- The server that currently serves clients and receives telemetry data is called the *primary node*.
- The server that runs only essential services for disaster recover and is responsible for recovery is called the *standby node*.

Data is continuously streamed from the primary node to the secondary node. SANnav synchronizes configuration data every 30 minutes, and a checkpoint timestamp is created. When a failover occurs, the data is restored up to the time of the last successful timestamp.

SANnav performs a health check every 5 minutes. If the peer node is not reachable for a consecutive 10 minutes, you are alerted in the following ways:

- Email notification
- Critical event
- Notification in the notifications panel

You are responsible for identifying the failure of the node and initiating a manual failover. After the failover is initiated, the standby SANnav server should be up and running within 30 minutes.

After the failover completes, the standby server is now the only SANnav server, and you need to set up disaster recovery again. You can set this server as the primary node. For the secondary node, you can reconfigure a new standby node, or you can uninstall SANnav on the previous primary node and set it up as the new standby node.

Requirements for Disaster Recovery

Disaster recovery (DR) is supported for both Basic and Enterprise licenses. Disaster recovery is not available for trial licenses.

Disaster recovery requires two identical active VMs that are reachable over a LAN or WAN. The nodes in the disaster recovery setup are divided into two categories:

- **SANnav DR Primary Node** – The primary node is the active node where SANnav is fully installed and all services are running. When DR is enabled, users can access and stream data to this server.
- **SANnav DR Standby Node** – The standby node is the SANnav node in the remote datacenter or in the same datacenter reachable over a LAN or WAN to the primary node. The standby node has only a subset of services running that are essential for data replication.

Additional requirements:

- The primary and standby nodes must have identical configurations, including the same hardware specifications and operating system versions.
- The primary and standby nodes must have the same SANnav version.
- The primary and standby nodes must have SSH access enabled between them.
- The primary and standby nodes must be synchronized to the NTP server. The nodes can be in different timezones.
- You must have root access or sudo access to the VM on which SANnav is installed.
- The primary and standby nodes must have the same user account, if you are installing SANnav or configuring disaster recovery with a nonroot user account.

The following table lists the system requirements for disaster recovery.

Table 14: System Requirements for Disaster Recovery

Component	Requirement
Operating system	RHEL 8.4 If you have an earlier version of the operating system installed, you can upgrade the operating system and then enable disaster recovery.
Memory	96 GB
Virtualization	VMware VM Bare metal, OVA, and Hyper-V are not supported. If you have an existing version of SANnav installed on bare metal or OVA and you migrate to SANnav 2.2, you cannot enable disaster recovery.
CPUs	24
License	The SANnav primary node requires a Base or Enterprise license. The SANnav standby node does not require a license.
Bandwidth latency between primary and standby servers	Minimum required latency between the primary and standby servers: 100 ms. Minimum required dedicated bandwidth between the primary and standby servers: 100 Mb/s.

Ports That Must Be Open in the Firewall for Disaster Recovery

If you are using disaster recovery, a set of ports must be open in the firewall. These ports are not customizable.

If you set up disaster recovery in two different datacenters and there are firewalls between both datacenters, these ports must be open in both firewalls.

Table 15: Ports That Must Be Open in the Firewall

Port Number	Transport	Inbound/ Outbound	Communication Path	Description
5432	TCP	Both	Server --> Server	Used for data replication.
18022	TCP	Both	Server --> Server	Used for the SSH connection between the primary and standby nodes.
18023	TCP	Both	Server --> Server	Used for REST communication between the primary and standby nodes.
18024	TCP	Both	Server --> Server	Used to calculate the bandwidth between the primary and standby nodes.

Tasks for Setting Up Disaster Recovery

You must perform the following tasks to set up disaster recovery:

- Install SANnav on the primary node and set up disaster recovery.
- Install SANnav on the standby node and set up disaster recovery.
- Set up a web proxy for license rehosting.

In addition, SANnav provides a script that shows you the status of disaster recovery.

Setting Up Disaster Recovery on the Primary Node

Perform the following steps to set up SANnav Management Portal as the primary node:

1. Download and install SANnav Management Portal.
   No change to the installation is required for disaster recovery.
2. After the installation is complete, install the SANnav license.
   The license must be a Basic or Enterprise license. You cannot use a trial license.
3. Go to `<SANnav_home>/bin/dr` and run the following script:

   ```
   setup-dr-primary.sh
   ```

During script execution, you are required to provide the following information:

- The IPv4 address of the standby node. An IPv6 address is not accepted.
- Root or sudo user credentials of the standby node. These credentials are used for setting up passwordless SSH between the primary and standby nodes. The credentials will not be stored in SANnav.

This script performs the following actions:

- Validates the system requirements, IPv4 address, and connectivity to the standby node.
- Copies the required properties, including the IPv4 address of the primary node, to the standby node.
- Copies an SSH key to the standby node.
- Restarts the SANnav server.

The next step is to set up the standby node.

Setting Up Disaster Recovery on the Standby Node

Perform the following step to install SANnav Management Portal and set it up as the standby node.

Go to `<SANnav_home>/bin/dr` and run the following script:

```
setup-dr-standby.sh
```

During script execution, you are required to provide the following information:

- The email server address
- Email To and From addresses

These addresses are not validated during installation, but you have an option to send a test email.

NOTE
If the addresses are incorrect, SANnav will fail to send email if it detects that the standby server is unreachable.

This script performs the following actions:

- Validates the system requirements, IPv4 addresses (primary and standby nodes), and connectivity to the primary node.
- Attempts a handshake with the primary node.

If the requirements are met and a successful handshake with the primary node is established, disaster recovery is enabled on both nodes. The script then takes a full database backup from the primary node to the standby node.

NOTE
The backup can take some time, depending on the size of the database and the bandwidth between the primary and secondary nodes.

After successful completion of the standby node setup, the primary node starts the first data synchronization.

Setting Up a Web Proxy for Internet Connectivity

When SANnav fails over from the primary node to the standby node, the license on the primary node is automatically rehosted to the standby node. For this rehosting to occur, there must be an Internet connection from the VM on which the standby node is installed.

If you want to configure a proxy from the standby node to connect to the Internet, you can run a script after completing the standby setup. On the standby node, go to `<SANnav_home>/bin` and run the following script:

```
configure-proxy-sh
```

You must provide the following information:

- Proxy address (FQDN or IPv4 address)
- Proxy type (HTTP, HTTPS, or SOCKS)
- Proxy port
- Proxy user name and password, if the proxy is authenticated

Checking the Status of the Disaster Recovery Setup

SANnav provides a script that allows you to check the status of the disaster recovery setup.

Go to `<SANnav_home>/bin/dir` and run the following script:

`show-dr-status.sh`

The script shows the following information:

- The current disaster recovery status (enabled or disabled)
- The date and time of the last successful checkpoint
- Additional information about the status, if applicable

Tasks for Recovering SANnav

Two different tasks are provided for recovering SANnav:

- Planned failover to the standby node
- Unplanned failover to the standby node

After failover, you can create a new standby node so that disaster recovery remains in effect.

Some features require you to perform additional tasks after failover completes.

Unless otherwise specified, all user interactions and configuration are done through CLI scripts and not through the SANnav user interface.

Recovering SANnav: Planned Failover to the Standby Node

You can perform a planned failover from the primary node to the standby node.

The primary and standby nodes can be in different datacenters or in the same datacenter.

1. On the primary node, stop SANnav.

   ```
   <SANnav_home>/bin/stop-sannav.sh
   ```

2. On the standby node, run the following script:

   ```
   <SANnav_home>/bin/dr/failover-sannav.sh
   ```

   The script displays the last successful checkpoint to which the system will be restored. The time shown is the local time of the standby node.

   If a synchronization is in progress, the script waits until the synchronization completes before continuing with the failover.

   The script performs the following actions:

   1. Shuts down disaster recovery on the standby node.
   2. Restores all configuration on the standby node that was synchronized from the primary node.
   3. Rehosts the license onto the standby node:
      a. Deletes the existing SANnav license from the database.
      b. Gets the UUID of the standby node and a rehosting key for the license.
      c. Retrieves a new license certificate from the Broadcom Licensing Portal.
      d. Installs the license certificate on the standby node.
   4. Starts all services on the standby node.

After failover completes, you can log on to the new SANnav server. Note that at this point, the disaster recovery service is disabled. If you want to enable disaster recovery again, see Tasks for Setting Up Disaster Recovery.

Recovering SANnav: Unplanned Failover to the Standby Node

If the primary node suffers nonrecoverable damage, you must perform a failover to the standby node.

If the primary node is not reachable from the standby node for 10 consecutive minutes, the standby node sends you an email notifying you of this situation.

If you receive notification of this situation, perform the following steps:

1. First attempt to log on to the primary node to determine whether this problem is temporary, such as a temporary network connectivity issue.

   Temporary problems can often be fixed by restarting SANnav on the primary node.

2. If the problem is nonrecoverable, follow the instructions in Recovering SANnav: Planned Failover to the Standby Node.

Replacing the Standby Node

You may need to replace the standby node in certain circumstances:

- If the standby node experiences a nonrecoverable hardware failure (unplanned replacement)
- If you want to replace the existing standby node with a new standby node (planned replacement)

Whether planned or unplanned, perform the following steps to replace the standby node:

1. On the primary node, run the following script:

   `<SANnav_home>/bin/dr/replace-standby.sh`

2. Review the confirmation changes, and press **Enter**.

   During script execution, you are required to provide the following information:

   - The IPv4 address of the standby node. An IPv6 address is not accepted.
   - Root credentials of the standby node. These credentials are used for setting up passwordless SSH between the primary and standby nodes. The credentials are not stored in SANnav.

   The script validates the system requirements, IPv4 address, and connectivity to the standby node. The required properties, including the IPv4 address of the primary node, are copied to the standby node.

   A passwordless SSH trust is established between the primary and standby nodes, and an SSH key is copied to the standby node.

   The SANnav server is restarted.

3. Set up the new standby node by following the instructions in Setting Up Disaster Recovery on the Standby Node.

After the new standby node is up and running, the first data synchronization starts. The first data synchronization may take a long time, depending on the amount of data that needs to be replicated.

Tasks After Failover Completes

After the failover (planned or unplanned) completes, and you have verified that the new SANnav node is functioning properly, perform the following tasks to clean up the servers.

Table 16: Tasks to Perform After SANnav Failover Completes

Task	Description
Uninstall SANnav on the previous primary node.	Go to the previous primary node and uninstall SANnav: `<SANnav_home>/bin/uninstall-sannav.sh`
Reconfigure the southbound and northbound configuration from the switches to SANnav.	After failover successfully completes, the SANnav IP address is changed and communication between the switches and SANnav must be reconfigured. Update the IP address of the REST endpoint. Then replace the older SANnav IP address with the new IP address.
Unmonitor and remonitor fabrics.	From the SANnav user interface, unmonitor and then remonitor all fabrics. This will automatically configure SNMP and Syslog registration.
Replace third-party certificates.	If third-party certificates were installed on SANnav, they are not migrated to the new primary node. To replace the certificates, perform the following steps: 1. Procure new SSL certificates that are based on the new host name. 2. On the new primary node, replace the self-generating certificates with these new certificates.

Task	Description
Get a new license, if a license was not automatically generated.	When SANnav fails over from the primary node to the standby node, SANnav automatically generates a rehosting key and retrieves a new license certificate from the Broadcom Licensing Portal. If the Licensing Portal is not reachable, the certificate is not retrieved. In this case, SANnav creates a new Trial license that is valid for 30 days from the day of failover. This 30-day license retains all the capabilities of the original license. An application event, a notification, and a login banner inform you of this 30-day license. When you log on to SANnav Management Portal, click **OK** in the banner. You are redirected to the **Licensing** page where you must provide the new license certificate.
Rediscover SANnav Management Portal in SANnav Global View.	During a failover, SANnav Global View loses connectivity to the primary node. After the failover completes, you must delete the existing SANnav Management Portal instance from SANnav Global View, and you must rediscover the new IP address in Global View.

Disaster Recovery Impact on Other Features

When disaster recovery is enabled, other features may be impacted.

Table 17: Features Affected by Disaster Recovery

Feature	Description
SANnav backup and restore	If disaster recovery is enabled, you can perform a SANnav backup on the primary node. You cannot restore the backup on the primary node. If you perform a backup on the primary node, disaster recovery-related properties are not included in the backup. You cannot take a SANnav backup or restore a SANnav backup on the standby node.
SSL certificates	During SANnav failover, SSL certificates are not migrated to the new node. Instead, the following new SSL certificates are generated: • SANnav server certificate • Southbound streaming certificate (Kafka certificate) • Secure Syslog certificates Third-party certificates are not migrated to the new node.
Supportsave	Supportsave is supported only on the primary node. If you need to collect logs on the standby node (for debugging disaster recovery issues), SANnav provides a script. On the standby node, go to `<SANnav_home>/bin/dr` and run the following script: `collect-dr-supportsave-standby.sh`

Scripts for Managing SANnav

The SANnav installation provides 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 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 in the `<install_home>/bin` folder.

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

Table 18: SANnav User-Executable Scripts

Script	Description
`change-ipv4-installation-to-ipv6.sh`	Changes SANnav from an IPv4 installation to a dual-stack IPv4/IPv6 installation.
`check-sannav-status.sh`	Checks the status of the SANnav server.
`configure-proxy.sh`	Configures a proxy to connect to the Internet.
`install-sannav.sh`	Installs the SANnav server. SANnav should not be running when you run this script.
`manage-high-granular-data-collection.sh`	Enables and disables the SANnav high-granularity, 2-second data collection HFS service. Contact Technical Support before running this script.
`manage-sannav-whitelisting.sh`	Creates and manages a list of IP addresses that are allowed SANnav access. Refer to the *Brocade SANnav Management Portal User Guide* for details.
`merge-files.sh`	Merges files previously split by the `split-file.sh` script.
`reconfigure-sannav-for-96GB.sh`	Changes the memory configuration of the SANnav installation to 96GB, to support 15,000 ports. Before running this script, ensure that the memory capacity of the SANnav host is at least 96GB.
`replace-sannav-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.
`show-sannav-configurations.sh`	Displays SANnav port and server configurations.
`show-sannav-license-information.sh`	Displays the SANnav license serial number and server unique ID (UID).
`show-sannav-open-source-software.sh`	Displays information about open source software used by SANnav.
`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 run this script.
`stop-sannav.sh`	Stops the currently running SANnav server.
`uninstall-sannav.sh`	Uninstalls the SANnav server.

Script	Description
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.

The following scripts lists user-executable scripts that are used for disaster recovery. These scripts are in the <install_home>/bin/dr folder.

Table 19: SANnav User-Executable Scripts for Disaster Recovery

Script	Where to Run	Description
collect-dr-supportsave-standby.sh	Standby node	Collects logs on the standby node that are useful for debugging disaster recovery issues.
failover-sannav.sh	Standby node	Performs a SANnav failover from the primary node to the standby node.
replace-standby.sh	Primary node	Replaces the standby node with a different standby node.
setup-dr-primary.sh	Primary node	Sets up the current SANnav installation to be the primary node.
setup-dr-standby.sh	Standby node	Installs SANnav and sets it up to be the standby node.
show-dr-status.sh	Primary node	Displays whether disaster recovery is enabled and the time and date of the last successful checkpoint.

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.

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.

- Check SANnav status.
- Restart SANnav.
- Stop SANnav.
- Start SANnav.
- Show SANnav configuration.
- Show open source code attribution.
- Update SANnav configuration.

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
```

The following is sample output from 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 from an unhealthy server:

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

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

Changing the SSL Self-Signed Certificates

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

SANnav provides a script that replaces all SSL certificates (SANnav server certificate and KAFKA certificate) at the same time.

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.
- If you intend to use secure syslog, ensure these additional requirements are met:
  - Include the Subject Alternative Name extension in the certificate sign request (CSR) and the SSL certificate that you get from the signing authority.
  - If your VM has a multi-NIC configuration and you chose a non-default IP address for switch-to-server communication during installation, use that IP address in the Subject Alternative Name.

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

```
./replace-sannav-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

This example shows how to set up a firewall using `firewalld`. The 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 the default 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 with the default profile (if this is not done already).

   ```
   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
   ```

Deployment in a FIPS-Enabled Server

SANnav supports deployment on RHEL or CentOS sesrvers with FIPS mode enabled. The SANnav deployment does not take care of enabling FIPS mode as part of installation. You must enable FIPS mode either before or after SANnav installation.

If you enable FIPS mode after installation, the following steps are recommended:

1. Stop the SANnav server.

   You can use the SANnav Management Console script:

   ```
   <SANnav_home>/bin/sannav-management-console.sh
   ```

2. Enable FIPS.
3. Restart the host or VM.
4. Restart SANnav services, if any service fails to start up after the server restart.

Revision History

SANnav-220x-Install-IG100; 15 December 2021

Initial document version.

Copyright Statement


BROADCOM®