Brocade® SANnav™ Management Portal Installation and Upgrade Guide, 2.3.x

Installation Guide
April 28, 2023

Table of Contents

Introduction....................4

Contacting Technical Support for Your Brocade® Product....................4

Document Feedback....................5

SANnav Management Portal Installation Overview....................6

SANnav System and Server Requirements....................6

Installing SANnav on a Bare Metal or VM for the First Time....................7

Installing SANnav as Appliance (OVA) for the First Time....................7

Upgrading SANnav in Bare Metal or VM Deployments....................8

Upgrading SANnav in OVA Deployments....................8

Setting Up Disaster Recovery on SANnav....................9

VM and Bare Metal Deployment....................11

Important Considerations for Deployment....................11

Upgrading from an Earlier Release of SANnav....................11

Upgrade Paths for SANnav....................12

Pre-Installation Checks for VM and Bare Metal Deployment....................13

Installation Prerequisites for VM and Bare Metal Deployment....................14

Upgrade Prerequisites....................16

System and Server Requirements for the SANnav Management Portal....................17

Port and Firewall Requirements for SANnav Management Portal....................18

Configuring the Firewalld Backend for RHEL 8.4 or 8.6....................22

Installing SANnav Management Portal....................22

SANnav Installation Prompts and Customizations....................23

Post-Installation for VM and Bare Metal Deployment....................29

Post-Installation Diagnosis....................30

Upgrading the OS with SANnav Installed....................30

Upgrading the SANnav Internal SFTP/SCP Server SSH Key....................31

Uninstalling SANnav....................31

Upgrading to SANnav v2.3.0 (If the OS is Centos or RHEL 7.9)....................32

OVA Deployment....................33

Pre-Installation Checks for OVA Deployment....................33

Installation Prerequisites for the SANnav Management Portal Appliance....................33

System and Server Requirements for the SANnav Management Portal Appliance....................34

Installing the SANnav Management Portal Appliance....................35

Installing SANnav Management Portal on OVA Deployments....................41

Upgrading the SANnav Appliance from 2.2.1....................42

Upgrading the SANnav Appliance from 2.2.2x....................43

Preparing for the SANnav Management Portal Appliance Upgrade.. 43
Deploying the SANnav OVA Package..44
Upgrading the SANnav Management Portal Appliance.. 52
Post-Installation for OVA Deployment.. 53
Recovering from Upgrade Failure of the SANnav Management Portal Appliance..53
Uninstalling the SANnav Management Portal Appliance.. 55
Installation Log File.. 56
Disaster Recovery...57
Requirements for Disaster Recovery...58
Ports That Must Be Open in the Firewall for Disaster Recovery.. 59
Upgrading and Disaster Recovery.. 59
Tasks for Setting Up Disaster Recovery... 60
Setting Up Disaster Recovery on the Primary Node...60
Setting Up Disaster Recovery on the Standby Node...61
Checking the Status of the Disaster Recovery Setup..62
Tasks for Recovering SANnav..62
Recovering SANnav: Planned Failover to the Standby Node..62
Recovering SANnav: Unplanned Failover to the Standby Node..63
Replacing the Standby Node...63
Resetting or Uninstalling Disaster Recovery... 64
Tasks to be Performed After Failover Completes.. 64
Disaster Recovery Impact on Other Features...65
Scripts for Managing the SANnav Server...66
SANnav Management Console.. 68
Checking the Server Health.. 68
Checking the Availability of Linux User ID and Group ID...68
Changing the SSL Self-Signed Certificates... 69
Setting Up a Web Proxy for Internet Connectivity..69
Migrating the SANnav Management Portal from one Server to the Other..70
Required Linux Commands.. 71
Enabling FIPS Mode after SANnav Installation... 73
Changing the SANnav Server IP Address.. 74
Upgrading and SSL Certificates..75
Revision History..76
Documentation Legal Notice.. 77

Introduction

This guide contains detailed steps for installing SANnav™ Management Portal and for upgrading from an earlier version of SANnav. 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 Management Portal Installation Overview.

SANnav Management Portal supports deployment on a virtual machine (VM), on a bare metal physical server, or as an Open Virtual Appliance (OVA). See the following sections to get started:

- VM and Bare Metal Deployment
- OVA Deployment

This guide also includes information about the disaster recovery feature, which allows you to set up a standby server in case the primary server goes down. Disaster recovery is supported only in a VM deployment or OVA. See Disaster Recovery.

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 Global View Installation and Upgrade Guide* contains detailed steps for installing SANnav Global View and for upgrading from an earlier version.
- *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 Management Portal Installation Overview

This chapter provides information on SANnav server requirements and explains detailed procedures to install or upgrade SANnav v2.3.0 on various platforms and deployments (VM, Bare metal, and OVA).

Once the installation or upgrade is complete, you must use SANnav Management Console for typical day-to-day operations.

For detailed information on SANnav utility scripts and their usage, see Scripts for Managing the SANnav Server.

NOTE

The following are some of the common tasks that you may want to perform after installing SANnav.

- Changing the SSL Self-Signed Certificates
- Setting Up a Web Proxy for Internet Connectivity
- Enabling FIPS Mode after SANnav Installation
- Changing the SANnav Server IP Address

SANnav System and Server Requirements

The following are the system and server requirements for SANnav Management Portal v2.3.0.

NOTE
Make sure that you review the following sections in this guide because the information can change for every release.

- System and Server Requirements for the SANnav Management Portal
- System and Server Requirements for the SANnav Management Portal Appliance
- Requirements for Disaster Recovery

The following are the changes in the SANnav requirements for the SANnav v2.2.1x and SANnav v2.2.2x releases compared to SANnav v2.3.0. Read this section before you upgrade SANnav to v2.3.0x.

Changes in the SANnav System Requirements If Upgrading from 2.2.1x

- The Centos 7.9 and RHEL 7.9 operating systems are no longer supported. If your current version of SANnav is 2.2.1x running on Centos or RHEL 7.9, see Upgrading to SANnav v2.3.0 (If the OS is Centos or RHEL 7.9).
- SANnav v2.2.1x OVA cannot be upgraded directly to SANnav v2.3.0x OVA. Perform the inline upgrade to SANnav v2.2.2 before upgrading to SANnav v2.3.0x. For more information, see Upgrading the SANnav Appliance from 2.2.1.
- SANnav v2.3.0 allows users to provide a range of ports for SANnav installation. For more information, see Port and Firewall Requirements for SANnav Management Portal .
- SANnav v2.3.0 has additional prerequisites for Linux UID and GID when installed on a VM or Bare Metal. For detailed information, see Installation Prerequisites for VM and Bare Metal Deployment.

Changes in the SANnav System Requirements If Upgrading from 2.2.2x

- The Centos 7.9 and RHEL 7.9 operating systems are no longer supported. If your current version of SANnav is 2.2.2x running on Centos or RHEL 7.9, see Upgrading to SANnav v2.3.0 (If the OS is Centos or RHEL 7.9).
- SANnav v2.3.0 has additional prerequisites for Linux UID and GID when installed on a VM or Bare Metal. For detailed information, see Installation Prerequisites for VM and Bare Metal Deployment.

Installing SANnav on a Bare Metal or VM for the First Time

If you are installing SANnav for the first time, start with VM and Bare Metal Deployment. Also, review the Pre-Installation Checks for VM and Bare Metal Deployment section to verify that the VM or Bare Metal meets all system requirements.

Perform the following steps to install SANnav Management Portal on a VM or Bare Metal:

- Ensure that your server meets the requirements for SANnav installation. See System and Server Requirements for the SANnav Management Portal.
- Review the installation prerequisites. See Installation Prerequisites for VM and Bare Metal Deployment.
- Install the required Linux commands. See Required Linux Commands.
- Ensure that the required ports are free. Some of these ports need to be opened in the firewall. See Port and Firewall Requirements for SANnav Management Portal.
- If your operating system has firewalld running, ensure it meets the SANnav recommended configuration. See Configuring the Firewalld Backend for RHEL 8.4 or 8.6.
- Start Installing SANnav. See Installing SANnav Management Portal.

Optional:

- For some of the common post-installation tasks that you may be required to perform, see Post-Installation for VM and Bare Metal Deployment.
- For troubleshooting SANnav after installation, see Post-Installation Diagnosis.

Installing SANnav as Appliance (OVA) for the First Time

Before you proceed with the installation of the SANnav Management Portal Appliance, review the Installation Prerequisites for the SANnav Management Portal Appliance section.

> **NOTE**
> Deployment of a SANnav OVA is only supported using the vCenter UI. Deployment of a SANnav OVA is not supported using the ESXi UI.

Perform the following steps before installing SANnav Management Portal Appliance:

- Review the installation prerequisites for the SANnav OVA. See System and Server Requirements for the SANnav Management Portal Appliance.
- Download SANnav OVA (`.ova` file) to the location from where you want to import it to the vCenter.
- Log in to the vCenter UI and deploy SANnav OVA (`.ova` file). The time that it will take to deploy the 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 host. See Installing the SANnav Management Portal Appliance.
- After successfully extracting and deploying the SANnav OVA, power on the VM. During startup, vCenter configures the network of the VM and provides customizations based on the input user that was provided while deploying the OVA. After the successful network configuration, the VM reboots. Wait for the VM to reboot before logging on.
- After a successful reboot, log in to the VM using the default credentials (`root` / `SANnav!@#`) and start installing SANnav. For detailed information, see SANnav Installation Prompts and Customizations and Installing SANnav Management Portal on OVA Deployments.
- Check the SANnav status after installation using the following command:

```
/sannav-home/Portal_<Version>_bldxx/bin/check-sannav-status.sh
```

Optional:

- For some common post-installation tasks that you may be required to perform, see Post-Installation for OVA Deployment.
- For troubleshooting SANnav after installation, see Post-Installation Diagnosis.

Upgrading SANnav in Bare Metal or VM Deployments

Perform the following steps before upgrading SANnav Management Portal on VM or Bare Metal.

NOTE

- Upgrade to SANnav v2.3.0x is not allowed if the previous SANnav version does not have a valid and not expired license. Upgrade on a trial license is not allowed.
- If the SANnav license in the previous SANnav version is expired and is currently within the 30-day grace period, an upgrade is allowed. However, you cannot log in to the upgraded server until you apply a new license.
- Take a backup of the current SANnav before proceeding with the SANnav v2.3.0x upgrade.
- Take a Supportsave file from the current SANnav v2.3.0 before proceeding with the SANnav upgrade.

NOTE
The Centos and RHEL 7.9 are no longer supported. If your current SANnav installation runs on Centos or RHEL 7.9, see Upgrading to SANnav v2.3.0 (If the OS is Centos or RHEL 7.9).

- Ensure that your server meets the requirements for SANnav installation. See System and Server Requirements for the SANnav Management Portal. If your current version of SANnav is running on an operating system that is not supported by SANnav v2.3.0x, see Upgrading the OS with SANnav Installed.
- Review the installation prerequisites. See Installation Prerequisites for VM and Bare Metal Deployment.
- Install the required Linux commands. See Required Linux Commands.
- Ensure that the required ports are free. Some of these ports must be opened in the firewall. See Port and Firewall Requirements for SANnav Management Portal.
- If your Operating System has firewalld running, ensure it meets the SANnav recommended configuration. See Configuring the Firewalld Backend for RHEL 8.4 or 8.6.
- Start Installing SANnav. See Installing SANnav Management Portal.

Optional:

- If you have Disaster Recovery that is configured before upgrading SANnav, navigate through the Upgrading and Disaster Recovery.
- For some of the common post-installation tasks that may be required to perform, see Post-Installation for VM and Bare Metal Deployment.
- For troubleshooting SANnav after installation, see Post-Installation Diagnosis .

Upgrading SANnav in OVA Deployments

If you are upgrading from SANnav v2.2.1, see Upgrading the SANnav Appliance from 2.2.1 before you proceed to further steps.

NOTE
You can upgrade to the SANnav v2.3.0x OVA if the previous SANnav version license is expired. However, you cannot log in to the upgraded server until you apply a new license.

Perform the following steps before upgrading the SANnav Management Portal Appliance:

- Back up the current SANnav installation and save it in a location outside the current VM. For detailed information, refer to the *Brocade SANnav Management Portal User Guide*.
- Review and comply with SANnav Management Portal Appliance installation prerequisites. See Installation Prerequisites for the SANnav Management Portal Appliance.
- Stop the SANnav server using the following command:

```
/sannav-home/Portal_<version>_bldxx/bin/stop-sannav.sh
```

- Copy the MAC address of the current SANnav VM. This MAC address must be provided at the time of upgrade while associating the disk. If you do not manually update the MAC address on the new VM, the license is not upgraded from the previous SANnav installation. For detailed information on copying a MAC address, see Deploying the SANnav OVA Package.
- Power off the VM.
- Download the SANnav OVA (`.ova` file) to the location from which you want to import to 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 host.
- Deploy the SANnav OVA package.
- Log on to the vCenter and deploy the OVF template. Do not power on the VM after deploying.
- Attach the Virtual Machine Disk (VMDK) file from the earlier version of SANnav as a new disk. See Deploying the SANnav OVA Package.
- Modify the MAC address of the new SANnav VM. See Deploying the SANnav OVA Package.
- Power on the VM, and log in as the root user. When the SANnav OVA is deployed, it configures the network of the VM and provides customizations based on user input. After successful network configuration, the VM reboots. Wait for the VM to reboot before logging in.
- Upgrade the SANnav Management Portal Appliance using the following command:

  ```
  /sannav-home/Portal_<version>_bldxx/bin/install-sannav.sh
  ```

- Check the SANnav status after installation using the following command:

  ```
  /sannav-home/Portal_<Version>_bldxx/bin/check-sannav-status.sh
  ```

Optional:

- For some of the common post-installation tasks that may be required to perform, see Post-Installation for OVA Deployment.
- For troubleshooting SANnav after installation, see Post-Installation Diagnosis.

Setting Up Disaster Recovery on SANnav

Before proceeding with configuring disaster recovery for SANnav, see Requirements for Disaster Recovery.

> **NOTE**
> The system requirements for SANnav Management Portal without Disaster Recovery and with Disaster Recovery are different.

If you are planning to set up Disaster Recovery for SANnav, perform the following steps:

- Complete the installation of the SANnav Management Portal. Disaster Recovery in SANnav v2.3.0x is supported on VMware VM or OVA (new). Disaster Recovery setup is not supported if SANnav is installed on Bare Metal. See Installing SANnav on a Bare Metal or VM for the First Time and Installing SANnav as Appliance (OVA) for the First Time.
- Review the port requirements for the Disaster Recovery feature and open the ports in the firewall. See Ports That Must Be Open in the Firewall for Disaster Recovery.
- Set up Disaster Recovery on the primary node. See Setting Up Disaster Recovery on the Primary Node.
- Set up Disaster Recovery on the standby node. See Setting Up Disaster Recovery on the Standby Node.
- Check the Disaster Recovery setup status. See Checking the Status of the Disaster Recovery Setup.

Optional:

- To recover SANnav when a disaster occurs or to perform a planned failover of the SANnav Management Portal, see Recovering SANnav: Planned Failover to the Standby Node.
- To perform additional tasks after the failover of the SANnav Management Portal, see Tasks to be Performed After Failover Completes.
- For information about the impact of Disaster Recovery on other SANnav features, see Disaster Recovery Impact on Other Features.

VM and Bare Metal Deployment

SANnav Management Portal supports deployment on RHEL servers only. If the FIPS mode is required, it is possible to enable the FIPS mode on RHEL either before or after SANnav is installed.

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.

SANnav VM and bare metal deployment involve the following processes:

1. Pre-installation checks
2. Installation
3. Post-Installation

If you are upgrading SANnav from an earlier release, see Upgrading from an Earlier Release of SANnav for additional information and requirements.

Important Considerations for Deployment

The following information must be considered before SANnav VM and bare metal deployment.

- SANnav Management Portal and SANnav Global View are two different software products. You cannot install both software products on the same physical host or VM. You can, however, install Management Portal and Global View on different VMs in the same host, if the host has enough resources.
- When deploying SANnav as a VM, it is important to understand that the SANnav VM is not a *commodity* standard virtualized Enterprise VM like other applications that may be running in the customer environment. Therefore, software vendors' virtualization tools (such as VMware software tools, Microsoft Hyper V tools, and any other software virtualization tools) are not supported when used to manage the SANnav VM. Instead, use the SANnav tools and scripts to manage the SANnav VM for tasks such as starting, stopping, updating, upgrading, backing up, restoring, and other similar management tasks.
- Using VM snapshots with VMware tools for backing up and restoring the SANnav VM is not supported and not recommended. Instead, use the SANnav backup and restore procedures for these tasks.
- 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 Secure Copy (SCP) and SSH File Transfer Protocol (SFTP) servers. See Installation Prerequisites for VM and Bare Metal Deployment for more details.

Upgrading from an Earlier Release of SANnav

If you are upgrading SANnav from a previous version, the installation script provides the option of upgrading your data.

Upgrading 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 upgrade your data, the upgrade steps are the same as the installation steps.
> - Not all data is upgraded. For example, SANnav backup files and SANnav support data collection files are not upgraded.
> - Make sure that you have a valid license before starting the upgrade.

When you upgrade 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 previously discovered fabrics are rediscovered.
- User-configured data, customized data, and historical data (such as port performance metrics and events) are upgraded. Only the most recent one million events and violations are upgraded.
- Imported firmware files are upgraded.
- Certificates are upgraded or regenerated. See Upgrading and SSL Certificates for more details.
- Data-streaming-enabled switches that were streaming data before the upgrade continue to stream data after the upgrade within 10 minutes of the SANnav server startup.

OS Upgrade Options

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

If you want to upgrade 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 upgrade SANnav and the OS simultaneously. See Upgrading the OS with SANnav Installed.

Upgrade Paths for SANnav

Upgrading to SANnav 2.3.0x is supported on specific SANnav versions.

You cannot directly upgrade from a VM or bare metal installation to an OVA installation. You can, however, back up a VM or bare metal installation and restore to an OVA installation, and then upgrade to an OVA installation. Refer to the *Brocade SANnav Management Portal User Guide* for instructions on backing up and restoring SANnav.

If your SANnav server is a dual-stack IPv4/IPv6 deployment, you cannot change it to an IPv4-only deployment.

The following table lists the software versions and whether upgrading to SANnav 2.3.0x is supported.

Table 1: Supported Upgrade Paths for SANnav Management Portal

Current Version	Upgrade Version	Supported?
SANnav 2.2.1x	SANnav 2.3.0x	Yes
SANnav 2.2.2x	SANnav 2.3.0x	Yes
SANnav 2.2.0x or earlier	SANnav 2.3.0x	No

The following table lists the OVA installations and whether upgrade and migration are supported.

Table 2: Supported Upgrade Paths for SANnav OVA Installation

Current Version	Upgrade Version	Supported?
SANnav 2.2.2x OVA installation	SANnav 2.3.0x OVA installation	Yes
SANnav 2.2.1x OVA installation	SANnav 2.3.0x OVA installation	No
SANnav VM or bare metal installation	SANnav OVA installation	No. A full SANnav backup and Restore is required.
SANnav OVA installation	SANnav VM or bare metal installation	No. A full SANnav backup and Restore is required.

The following table lists the upgrade paths for the various SANnav deployments.

Table 3: Supported Upgrade Paths for SANnav System Configurations

Current Deployment	Upgrade 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

Pre-Installation Checks for VM and Bare Metal Deployment

This section outlines the steps that you must take before you start SANnav installation. These steps apply whether you are performing a fresh installation or upgrading from an earlier version.

1. Before you unzip the SANnav installation file, review and comply with all Installation Prerequisites for VM and Bare Metal Deployment.
2. Create a folder where you want to install the application.

   NOTE
   Do not create the SANnav installation folder with spaces in the name; otherwise, installation will fail.
3. Download the SANnav Management Portal tarball to the installation folder.

   The file name is in the format `Portal_<version>-distribution.tar.gz`.
4. Verify the authenticity of the downloaded tarball by validating the MD5 checksum. Run command `md5sum Portal_<version>-distribution.tar.gz` . Match the printed checksum with the MD5 checksum file present in the Broadcom Portal.
5. 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.
6. Check system requirements.

   If you are performing a fresh SANnav installation, you can run the following script to check the requirements before starting the installation:

   ```
   <install_home>/bin/check-sannav-system-requirements.sh
   ```

   The script performs the following checks:

   - Port availability
   - Availability of SANnav required UIDs and GIDs
   - SANnav system requirements
   - Supported operating system and Linux modules
   - SANnav docker dependencies
   - IPtables prerequisites

   The SANnav installation script also performs the same checks.

   If you are upgrading from an earlier release of SANnav, do not run the check-sannav-system-requirements.sh script. Instead, you can perform the checks manually, or you can let the installation script perform the checks.

   See the following sections for additional information:

- Port and Firewall Requirements for SANnav Management Portal
- System and Server Requirements for the SANnav Management Portal
- Required Linux Commands

Installation Prerequisites for VM and Bare Metal Deployment

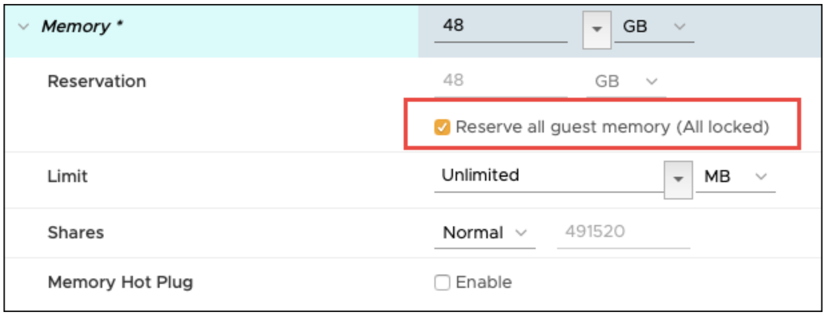
Review and comply with all SANnav installation prerequisites before you unzip the installation file.

Table 4: Installation Prerequisites

Task	Task Details or Additional Information
Gather the necessary information.	Make sure that you have the following information: • Root user credentials or ensure you must have `sudo` privileges. You must log on to the SANnav server as the root user or a user with root privilege (sudo). • The SANnav Management Portal server IP address. • If you want an additional sudo user to manage SANnav, you must execute the `add-user-to-sannavmgr-group.sh` script. For additional information on scripts, see Scripts for Managing the SANnav Server.
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 the SANnav installation. If you are upgrading SANnav, do not uninstall the current SANnav instance.
Uninstall Docker, if it is already installed.	The SANnav installation installs Docker. If you have a Docker installation other than the Docker that SANnav installs, you must remove it before starting the installation. During the boot-up sequence of the Linux, an administrator must ensure that the Docker-mounted file system (for example, `var/lib/docker`) is mounted successfully before `systemctl` Docker service starts. If this is not performed, it may cause issues for SANnav to recover from unexpected hard or cold server reboots.
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.
Disable SELinux, if it is enabled.	SELinux is not supported. If SELinux is enabled, you must disable it before installing SANnav. To disable SELinux, perform the following steps: 1. Log in to your server. 2. Check the current SELinux status by executing the `sestatus` command. 3. To disable SELinux on RHEL or Rocky Linux 8.x, open the `/etc/selinux/config` file in a text editor of your choice and set `SELINUX` to `disabled`. 4. Reboot the Linux server. 5. Verify the SELinux status by executing the `sestatus` and `getenforce` commands.
Ensure the Linux commands are installed in the OS.	Required Linux commands.
Ensure the UIDs, GIDs, usernames, and group names are available in the OS.	• UID:UNAME – 56900:sannavmgr • GID:GNAME – 56900:sannavmgr • UID:UNAME – 1000:sannavstreaming • GID:GNAME – 1000:sannavstreaming For detailed information, see Checking the Availability of Linux User ID and Group ID.

Task	Task Details or Additional Information
Format the XFS file system.	If you are using Extents File System (XFS) as the file system, make sure that you set `d_type=true` while creating the disk. You can verify the XFS file system format by running the command `xfs_info` *`<docker-installation-directory>`* and verifying that `ftype=1` . The default Docker installation directory is `/var/lib`.
Set umask.	The 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.

Check port 22 availability.	By default, SANnav uses port 22 for the internal firmware repository (SCP/SFTP). You can change this port number during installation.
	For switches running Fabric OS versions earlier than 8.2.2x, 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`
	The port that 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. Port 80 is not configurable.
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 virtual 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.  Memory * 48 GB Reservation 48 GB ☑ Reserve all guest memory (All locked) Limit Unlimited MB Shares Normal 491520 Memory Hot Plug □ Enable
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 installation fails.

<table>
<tr><th>Task</th><th>Task Details or Additional Information</th></tr>
<tr><td>Synchronize the server with the NTP server clock.</td><td>For SANnav features (for example, Flow Management) to work properly, make sure that the switch and SANnav server clocks are synchronized. Clock synchronization is mandatory for all switches and the SANnav application server. If the clocks are not synchronized, you may lose flows and their statistics. An application event message alerts you when the SANnav server and the switch are not synchronized.
Use <code>chronyd</code> for synchronizing the clock. For example, to synchronize the SANnav server with the NTP server clock, execute the command <code>chronyd -q "NTPserver"</code> on the SANnav server, where <code>NTPserver</code> is the host name or IP address of the NTP server.</td></tr>
<tr><td>Start the <code>rngd</code> service.</td><td>SANnav relies on the operating system to generate secure random numbers. The server must have the <code>rngd</code> service running to avoid performance degradation. Before starting the installation, run the following commands to install <code>rng</code> tools and start the <code>rngd</code> service in Linux.
<pre>
yum install rng-tools
systemctl start rngd.service
systemctl enable rngd.service
</pre></td></tr>
<tr><td>Run additional commands.</td><td>• Ensure that the <code>hostname -i</code> command resolves to a single valid IP address.
• The <code>nslookup</code> command must be successful for the host name of the physical host and VM.
• Enter the <code>ifconfig</code> command to verify that the MTU size is at least 1500 bytes. For example:
<pre>
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
         inet 10.155.41.231 netmask 255.255.240.0 broadcast 10.155.47.255

         ether 00:50:56:84:6f:dd txqueuelen 1000 (Ethernet)
         RX packets 22218220 bytes 16912208367 (15.7 GiB)
         RX errors 0 dropped 572 overruns 0 frame 0
         TX packets 3040031 bytes 1002844249 (956.3 MiB)
         TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
</pre>
When configuring the VM for SANnav installation, ensure that the MTU size of the network interface is set to 1500 bytes. If the MTU size is not set correctly, SANnav will not receive Historical Performance data. On the VM or server that hosts the SANnav server, change the interface MTU size from 1400 bytes to 1500 bytes.</td></tr>
</table>

Upgrade Prerequisites

Before you upgrade to the new SANnav version, review and comply with the following prerequisites. These upgrade prerequisites are in addition to the installation prerequisites.

NOTE

These upgrade prerequisites apply to all SANnav deployments (VM, Bare Metal, and OVA).

- Back up SANnav. After the backup completes, generate a full support data collection (logs and database, with the **Full** option).

  Refer to the *Brocade SANnav Management Portal User Guide* for instructions.
- Rename all SANnav accounts with user names "none" or "na" (case insensitive) prior to migration. SANnav 2.2.x does not support these user names.

  Refer to the "Viewing a List of Users" section in the *SANnav Management Portal User Guide*.
- 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 upgrade and 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 upgrade and migration.

System and Server Requirements for the SANnav Management Portal

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

NOTE

- The disk space requirement that is listed in the table is for SANnav only. You must account for the additional space required by the operating system, for saving files, and for SANnav TAR files and extracted files.
- The CPU socket and CPU speed requirements that are listed in the table are validated for SANnav releases prior to SANnav v2.3.0x installation only. Starting with SANnav v2.3.0x, the installation script does not enforce the required CPU sockets and CPU speed requirements. If the CPU sockets and CPU speed do not meet SANnav recommendation, the information is logged and installation continues.

  Failure to meet the recommended number of CPU sockets and the recommended CPU speed may lead to performance degradation on the SANnav server.

The disk space can be from a direct-attached disk or a network-mounted disk. Both Docker and the swap space must be on a direct-attached disk.

- The default home directory for installing Docker is `/var/lib/`, but you can choose another location during installation.
- 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. See SANnav Installation Prompts and Customizations for additional information.

NOTE

- Use the latest generation processors for the better SANnav performance.
- It is recommended that the required number of CPU cores must be equally distributed over the sockets.

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

Table 5: 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 and 8.6. The System Language must be English, and the System Locale must be US. **Note:** RHEL 9.0 is not supported. Check the SANnav Release Notes for information about support for other OS versions.	
Processor architecture	x86	x86
Host type	• Bare metal server • VMware ESXi 7.0 • Hyper-V on Windows Server 2022	• Bare metal server • VMware ESXi 7.0 • Hyper-V on Windows Server 2022
CPU	16 cores	24 cores
CPU sockets (minimum recommended)	2	2
CPU speed (minimum recommended)	2000 MHz	2000 MHz
Memory (RAM)	48 GB	96 GB
Hard disk space (minimum recommended)	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

NOTE
Flow management is supported in a 96GB memory configuration server only.

Port and Firewall Requirements for SANnav Management Portal

SANnav Management Portal requires specific ports to be available to ensure proper communication and operation. Ensure that the required ports are open between the SANnav server and the switches. The ports must be open in the firewalld on the Linux server where SANnav is installed and the network firewall that controls the traffic between the SANnav server and the switches.

Ports Required for SANnav Installation

SANnav 2.3.0x allows users to input a range of hundred ports (default ports 13000 to 13099 for OVA and 12000 to 12099 for VM or bare metal) for SANnav containers to use. All the hundred ports in that range must be free for SANnav to use. The port range cannot be modified after installation.

Additionally, SANnav uses the following ports. Ensure that these ports are also available before starting SANnav installation. If you customize any default ports during installation, ensure that the customized ports are available, and do not use them for other applications.

Table 6: Ports Required for SANnav Installation

Port Number	How the Port Is Used in SANnav	What Happens if the Port Is Not Available	Customizable During Installation?
22	Needed for SFTP/SCP.	Switch file transfer operations fail.	Yes
80	Needed for the SANnav proxy to serve the clients.	The SANnav user interface cannot be accessed using HTTP.	No
162	Needed for SNMP traps.	SANnav cannot receive traps.	Yes
443	Needed for the SANnav proxy to serve the clients.	The SANnav user interface cannot be accessed.	Yes
514	Needed for syslogs.	SANnav cannot receive syslogs.	Yes
6514	Needed for secure syslogs.	SANnav cannot receive secure syslogs.	Yes
2377, 7946	Internal use, for Docker.	Installation fails.	No
5432	Internal use, for the database.	Installation fails.	No
8080	Internal use, for Ignite.	Installation fails.	No
10800–10819	Internal use, for Ignite.	Installation fails.	No
11211	Internal use, for Ignite.	Installation fails.	No
19092, 19093	Internal use, for Kafka	Installation fails.	No
19094 (for IPv4 switches) 19095 (for IPv6 switches)	Needed for receiving data streams from Fabric OS.	Installation fails and performance data collection fails.	No
47100–47119, 47500	Internal use, for Ignite.	Installation fails.	No
18081, 18082	Needed for schema registry for streaming data from Fabric OS.	Installation fails and streaming registration fails. Performance data collection fails.	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 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`

If Firewall is enabled on the server, it must be configured to use iptables instead of the default nftables. See Configuring the Firewalld Backend for RHEL 8.4 or 8.6 for details.

If Firewalld is enabled, all ports are closed by default and SANnav does not open any ports automatically. You must open all required ports (for example, Telemetry, SNMP Traps, Syslog, Secure Syslog, SFTP) manually by entering Firewalld commands. See table *Ports That Must Be Open in the Firewall* in the following section.

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.

NOTE

- The NTP and DNS ports must be open in the external firewall.
- If iptables.service is enabled on the Linux VM or Host, you must open the required ports manually.

NOTE
After successful installation of the SANnav server, you must open the default ports that are listed in the *Ports That Must Be Open in the Firewall* table. If you have customized any of these ports, you must open the customized ports instead of the default ports. You must contact your network administrator to open the ports in the external firewall.

NOTE
In *Ports That Must Be Open in the Firewall* and *Ports That the SANnav Server Must Be Able to Access* tables, in the **Communication Path** column, **Client** refers to either the SANnav user interface or an external REST API session. Unless otherwise specified, **Server** refers to the SANnav server.

After installing SANnav, you can run the following script to check if Firewalld is enabled and whether the required ports are open:

```
<install_home>/bin/sannav-firewall-checker.sh
```

The *Ports That Must Be Open in the Firewall* and *Ports That the SANnav Server Must Be Able to Access* tables list the ports that must be open either in the Firewall or Firewalld depending on the configuration. In the **Communication Path** column, communication coming into the SANnav server is inbound. Communication going out from the server to either a switch or to the SANnav client is outbound. You must open all required ports manually.

The script lists the SANnav required ports and indicates whether they are open or not open in the firewall.

Table 7: Ports That Must Be Open in the Firewall

Port Number	Transport	Inbound/Outbound	Communication Path	Description
22 If port 22 was customized during installation, open its replacement port.	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. This port is not used if HTTP to HTTPS redirection is disabled.
161	UDP	Outbound	Server --> Switch	SNMP trap port.
162	UDP	Inbound	Switch --> Server	SNMP trap port.
443 If port 443 was customized during installation, open its replacement port.	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. This port is not needed if port 6514 is used.
6514	TCP	Inbound	Switch --> Server	Secure syslog port. This port is not needed if port 514 is used.
18081	TCP	Inbound	Switch --> Server	Avro schema registry HTTP port (Fabric OS versions lower than 9.0.1). Required to enable Kafka streaming from switches to SANnav. This port is not needed if port 18082 is used.
18082	TCP	Inbound	Switch --> Server	Avro schema registry HTTPS port (Fabric OS 9.0.1 and higher). Required to enable Kafka streaming from switches to SANnav. This port is not needed if port 18081 is used.
19094	TCP	Inbound	Switch --> Server	Secured Kafka streaming port (required for IPv4 switches).

Port Number	Transport	Inbound/Outbound	Communication Path	Description
19095	TCP	Inbound	Switch --> Server	Secured Kafka streaming port (required for IPv6 switches). This port is not needed if port 19094 is used.

If you are using the disaster recovery feature, additional ports must be open in the firewall.

Ports Required for External Authentication

If you configure an external authentication server (Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), or Terminal Access Controller Access Control System (TACACS+)) or an email server (SMTP), ensure that the SANnav Management Portal server has access to the ports listed in the *Ports That the SANnav Server Must Be Able to Access* table. The default ports are listed in the table, but you can change the default port.

Table 8: 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. Required only if you use email notifications without SSL or TLS.
49	TCP	Outbound	Server --> TACACS+ Server	TACACS+ server port for authentication. Required only if you use TACACS+ for external authentication.
389	TCP	Outbound	Server --> LDAP Server	LDAP server port for authentication. Required only if you use LDAP for external authentication and SSL is not enabled.
465	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication. Required only if you use email notifications with SSL.
587	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication. Required only if you use email notifications with TLS.
636	TCP	Outbound	Server --> LDAP Server	LDAP server port for authentication. Required only if you use LDAP for external authentication and SSL is enabled.

Port Number	Transport	Inbound/Outbound	Communication Path	Description
1812	UDP	Outbound	Server --> RADIUS Server	RADIUS server port for authentication. Required only if you use RADIUS for external authentication.

Configuring the Firewalld Backend for RHEL 8.4 or 8.6

In RHEL 8.4 or 8.6, 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 with `firewalld` is enabled, you must change the `firewalld` backend to use iptables instead of nftables.

If you do not make this change, you will not be 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=<ActiveZoneName> --remove-masquerade --permanent
   ```

   Where *<ActiveZoneName>* 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

After you have finished the pre-installation checks, complete these steps to install SANnav Management Portal.

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

NOTE

- If the scripts fail during the installation or startup, you must uninstall SANnav, reboot the server, and then reinstall SANnav. Do not try to resolve the issue and re-run the installation script without first uninstalling the application.
- If you are installing SANnav Management Portal as a `sudo` user, prefix the script execution with `sudo` . If you want additional `sudo` users to manage SANnav, you can execute the `add-user-to-sannavmgr-group.sh` script. For additional information on scripts, see Scripts for Managing the SANnav Server.

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

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

   ```
   cd Portal_<version>_bldxx/bin
   ```

2. Run the following script to install SANnav Management Portal:

   ```
   ./install-sannav.sh
   ```

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

3. If you are prompted about upgrading SANnav, enter one of the following options:

   - To proceed with an upgrade, 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 upgrading.

4. 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 must uninstall and then 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, restart the server, and repeat this procedure from Step 1. After the preinstallation requirements test pass, installation of the SANnav Management Portal software continues.

   After successful installation of the software, the SANnav Management Portal server starts up. The startup process may take up to 15 minutes.

   NOTE
   The installation takes more time if antivirus software is installed on the host on which SANnav is being installed.

5. Check the SANnav status running the following script:

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

   NOTE

   - After installation, do not modify the name of the installation file and folder permissions in the SANnav installation directory.
   - If you upgraded from a previous version of SANnav, then you must clear the browser cache before launching the new version of SANnav.

SANnav Installation Prompts and Customizations

During SANnav installation, you are prompted several times to accept default values or provide customized values for various settings.

If you are upgrading from an earlier version of SANnav, you are not prompted for these customizations, and the settings from the previous installation remain in effect once upgraded.

The following table lists the installation customization options. Some of the customizations can be changed after installation. See SANnav Management Console for information.

NOTE
For those parameters that cannot be modified after installation (indicated with a **No** in the **Change After Installation?** column), make sure that the values are correct during installation. Changing these parameters (indicated with a **Yes** in the **Customizable in OVA?** column) after installation requires you to uninstall and then reinstall SANnav.

Table 9: SANnav Installation Customizations

Item	Description	Change After Installation?	Customizable in OVA?
Start port for the SANnav installation port range	By default, SANnav uses ports 13000 to 13099 (OVA) and 12000 to 12099 (VM or bare metal) for installation. You can provide a different start port. However, you must make sure that there are 100 ports available from the start port.	No	No
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	Yes (OVA deployment time)
Docker installation directory	The default home directory for installing Docker is `/var/lib/`, but you can change to another directory during installation. Make sure the directory has enough space for SANnav installation.	No	No

Item	Description	Change After Installation?	Customizable in OVA?
Swap space	SANnav Management Portal requires 16GB swap space. The default swap space is the / directory. • If there is not enough swap space in the / directory, 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. The SWAP memory usage by SANnav may reach 100%, which is completely normal. There is no need to reboot SANnav to free this usage. if you are facing any issue like slowness, the issue must be analyzed by SANnav Support Team.	No	No
IPv6 capability	The default communication between SANnav and the SAN switches is IPv4. If you have IPv6-capable switches in your data center, you can configure SANnav to use IPv4 and IPv6 (dual-stack) communication.	Yes	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 redirection is due to a limitation in Firefox.	Yes	Yes

Item	Description	Change After Installation?	Customizable in OVA?
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 a Certificate Authority (CA)-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	Yes

Item	Description	Change After Installation?	Customizable in OVA?
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 logging 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. 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. Use option **0** or **1** in this case. **Option two is deprecated in SANnav v2.3.0x. This option is not available post-v2.3.0 release.**	Yes	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 of the configured IP addresses in the list.	Yes	Yes

Item	Description	Change After Installation?	Customizable in OVA?
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	No
Port customization	You can customize some ports when installing SANnav. The following is the list of ports that you can customize: • 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. Make sure that the ports that you specify (whether default or customized) are unused and available. **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)	Yes (SSH Port) No (Other ports)
Database password	You must provide a password for the SANnav database (Postgres database). There is no default password. When the script prompts for a password, it lists the password policies such as acceptable characters and length. **Note:** Making any changes to the SANnav database manually results in loss of support.	Yes	Yes
SCP/SFTP password	You provide a password for the SANnav internal SCP/SFTP server. There is no default password.	Yes	Yes
SANnav security password	This password is used for the enhanced security of SANnav infrastructure service components.	Yes	Yes

Item	Description	Change After Installation?	Customizable in OVA?
License autorenewal	By default, SANnav is configured to automatically retrieve and activate a renewal license when the license expires. You can deactivate the automatic license renewal, in which case you must manually apply the license yourself. SANnav requires an internet connection for the license autorenewal. If you do not have an internet connection, see Setting Up a Web Proxy for Internet Connectivity.	Yes	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 the user experience in the future. You can change this setting during or after installation. No customer data is sent. Only user clicks are captured. It is recommended to turn on this setting to allow user data to be sent to Broadcom to improve the most used SANnav features in the future.	Yes	Yes

Post-Installation for VM and Bare Metal Deployment

After the SANnav installation completes, you may need to perform some post-installation tasks.

- Check the SANnav status.
  You can check the SANnav any time using the `<install_home>/bin/check-sannav.status.sh` script.
- Run a script to perform post-installation diagnosis (SANnav 2.2.2x and later).
  See Post-Installation Diagnosis.
- Upgrade the OS with SANnav installed.
  If you need to change the OS after installation, see Upgrading the OS with SANnav Installed.
- Upgrade the SANnav internal key.
  If the SSH key for the server is a DSA key, it is recommended that you upgrade to a new RSA key for increased security. See Upgrading the SANnav Internal SFTP/SCP Server SSH Key.
- Uninstall SANnav and bring the system back to its original state.
  See Uninstalling SANnav.
- During the boot-up of the Linux, an administrator must ensure that the Docker-mounted file system (for example, `var/lib/docker`) is mounted successfully before `systemctl` Docker service starts. If this is not performed, it may cause issues for SANnav to recover from unexpected hard or cold server reboots.
  See Installation Prerequisites for VM and Bare Metal Deployment.

Post-Installation Diagnosis

After SANnav 2.3.0x installation, you can run a script to detect problems or drifts in the SANnav prerequisites.

> **NOTE**
> This script is available in SANnav 2.2.2x and later.

The `troubleshooting-sannav.sh` script performs the following operations:

- Checks every required SANnav port to see if it is occupied.
- Checks if the SANnav created Linux UIDs and GIDs are not modified or removed.
- Checks whether the operating system is supported.
- Checks that required Linux commands are available on the server.
- Checks that Docker is up and running. Also checks that the version of Docker that SANnav installed and the current Docker version is the same.
- Checks the following infrastructure functionalities:
  - Service status
  - IPtable-related dependencies
  - Docker write access (`/opt/docker`)
  - SANnav SSL certificate validity
  - Linux systemctl services

To execute the script, issue the following command:

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

Upgrading the OS with SANnav Installed

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

> **NOTE**
>
> - CentOS and RHEL 7.9 are no longer supported when installing or upgrading SANnav. If your current SANnav Management Portal is running on CentOS or RHEL 7.9, see Upgrading to SANnav v2.3.0 (If the OS is Centos or RHEL 7.9).
> - 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 OS upgrade may be allowed but requires explicit user agreement.
> - If Docker or SANnav fails to start after upgrading the OS, check the Technical Service Bulletin or contact technical support.

Perform the following steps to upgrade Red Hat Enterprise Linux (RHEL)

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 2.1.0a and later versions, this key is an RSA key with a length of 2048 bits. In SANnav 2.1.0 and earlier, this key is a DSA key with a length of 1024 bits.

Upgrading SANnav does not replace the existing key from the previous installation. If the previous installation had a DSA key, after the upgrade, SANnav still has a DSA key.

Although not mandatory, it is recommended that you upgrade the SSH key from a DSA key to an 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 upgraded to SANnav v2.3.0:

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 previous 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.
   ```

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 using the `reboot` command.

Upgrading to SANnav v2.3.0 (If the OS is Centos or RHEL 7.9)

If you have a current SANnav that is running on Centos or RHEL 7.9 and you want to upgrade to SANnav v2.3.0, perform the following steps:

1. Take a backup of the SANnav that is running on Centos or RHEL 7.9. For detailed instructions, refer to *Brocade SANnav Management Portal User Guide*.
2. Install the same version of SANnav on the Operating System that is supported by both current and target SANnav. For example, installation of SANnav Management Portal versions 2.2.1, 2.2.2, and v2.3.0 are supported on RHEL 8.4 and 8.6. For detailed instructions, refer to *Brocade SANnav Management Portal User Guide*.

   NOTE
   If you prefer to retain the same IP Address of the SANnav that is installed on Centos or RHEL 7.9, ensure that the backup is moved out of the server and you must shut down the OS.
3. Restore the backup to the newly installed SANnav.
4. Rehost the SANnav license from the older server to the new SANnav. For detailed instructions, refer to *Brocade SANnav Management Portal User Guide*.

OVA Deployment

SANnav Management Portal can be installed as a virtual appliance, compatible with VMware vCenter and ESXi 7.0.

The SANnav software package contains a SANnav OVA file (`.ova`), which can be deployed to an ESXi discovered in vCenter.

During installation, you can select a small or large configuration. The small configuration includes 48-GB memory, which supports the Base License and the Enterprise License with up to 3000 ports. The large configuration includes 96-GB memory to support an Enterprise License with up to 15,000 ports.

Note the following requirements:

- Deployment of the SANnav virtual appliance is supported only by VMware infrastructure. No hypervisor other than VMware ESXi is supported.
- Rocky Linux 8.6 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.
- Dual NIC cards are not supported for OVA installations.

Pre-Installation Checks for OVA Deployment

This section outlines the steps that you must take before you start the SANnav Management Portal Appliance installation. These steps apply whether you are performing a fresh installation or upgrading from an earlier version.

1. Before you download the SANnav OVA, review and comply with all SANnav installation prerequisites.

   See Installation Prerequisites for the SANnav Management Portal Appliance.

2. Check the system requirements.

   See System and Server Requirements for the SANnav Management Portal Appliance.

3. If you are upgrading SANnav, review and comply with the additional upgrade prerequisites.

   See Upgrade Prerequisites.

The next step is to install or upgrade SANnav.

Installation Prerequisites for the SANnav Management Portal Appliance

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

Table 10: Installation Prerequisites for SANnav Management Portal Appliance

Task	Task Details or Additional Information
Gather necessary information and components.	You must have default credentials for the root user: • 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. You cannot set a nondefault or private IP address for switch-to-server communication. **NOTE:** Dual NIC cards are not supported for OVA installations.

Task	Task Details or Additional Information
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.

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.

NOTE
Use the latest generation processors for better SANnav performance.

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, 7.0 • ESXi 7.0, discovered in vCenter 7.0	• VMware ESXi host, 7.0 • ESXi 7.0, discovered in vCenter 7.0
CPU	16 cores	24 cores
CPU sockets (minimum recommended)	2	2
CPU speed (minimum recommended)	2000 MHz	2000 MHz
Memory (RAM)	48 GB	96 GB

The SANnav appliance comes with predefined file system and disk partitions. Three 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 640 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	Description
Operating system and SWAP file	150 GB (16GB SWAP)	150 GB (16GB SWAP)	This partition is used for installing the operating system and a SWAP file creation for SANnav.
SANnav installation folder	490 GB	1090 GB	This partition is used to store SANnav files and install the docker home.

Installing the SANnav Management Portal Appliance

During the installation, you can select a **Small** or **Large** configuration. The hardware specifications are configured depending on the selected configuration.

Perform the following steps to install the SANnav Management Portal appliance using vCenter. If you are upgrading the SANnav Management Portal appliance from 2.2.2x, see Upgrading the SANnav Appliance from 2.2.2x before processing with next steps.

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

   The time that 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.

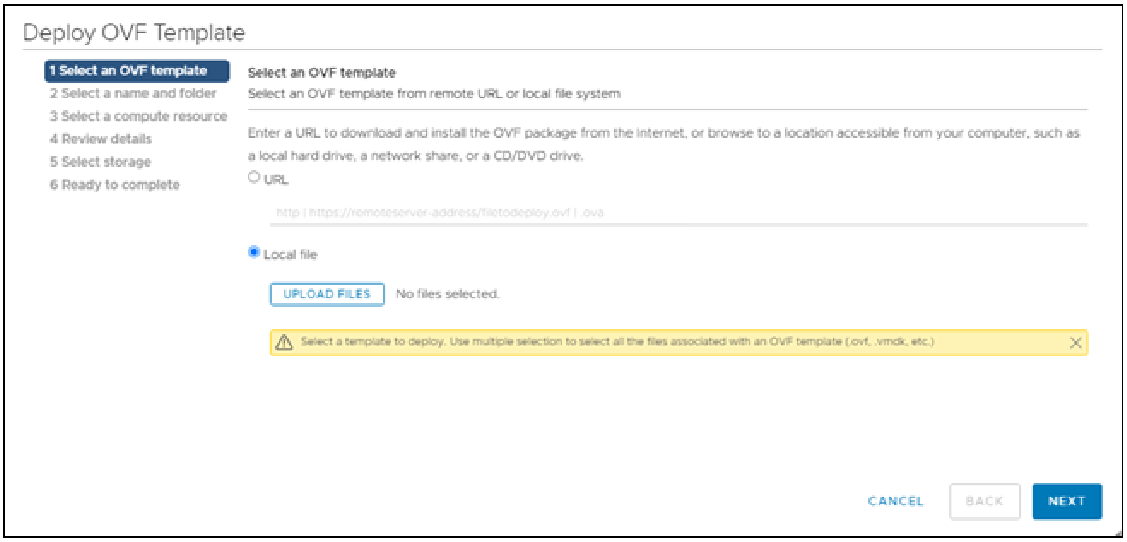
2. Log on to vCenter, right-click the host on which you want to deploy SANnav, and select **Deploy OVF Template**.

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

   NOTE
   The following steps correspond to the steps in the vCenter interface. 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**.



Deploy OVF Template

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

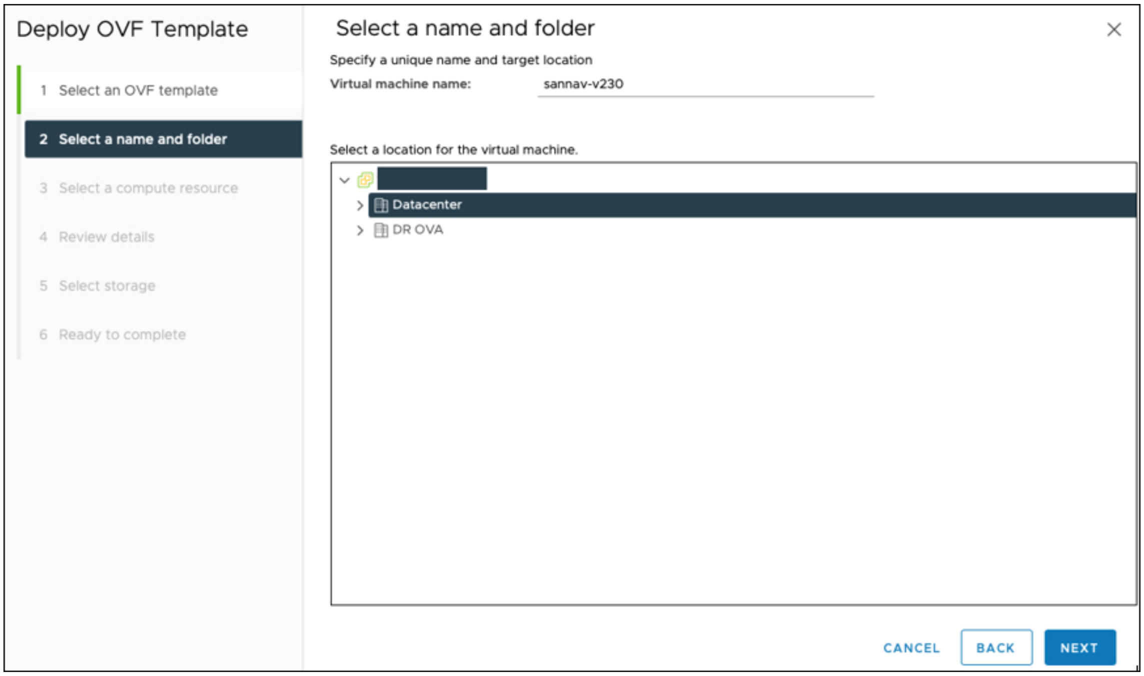
● Local file

UPLOAD FILES No files selected.

⚠ Select a template to deploy. Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

   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**.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a name and folder

Specify a unique name and target location

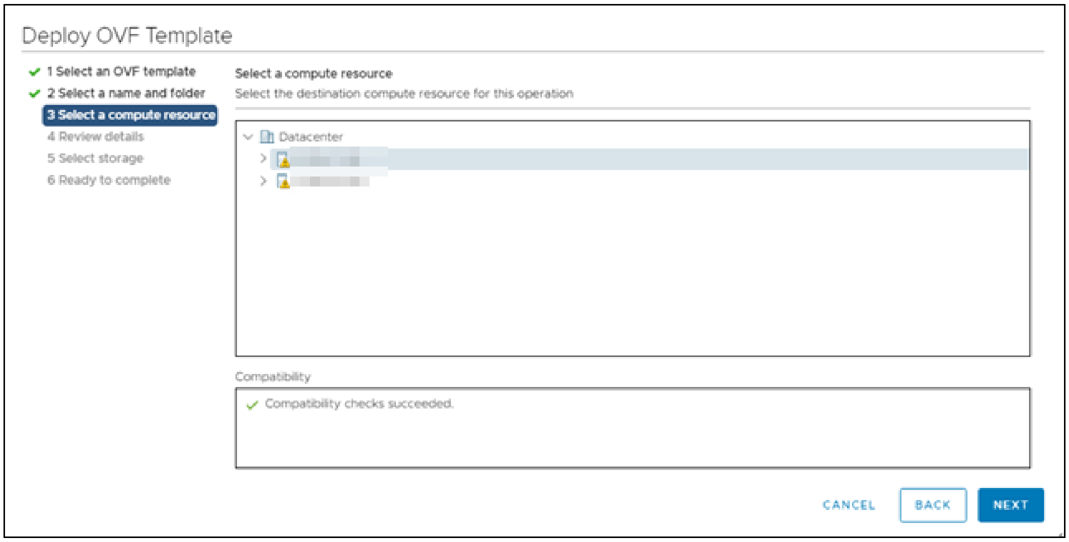
Virtual machine name: sannav-v230

Select a location for the virtual machine.

- [redacted]
  - Datacenter
  - DR OVA

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**.



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

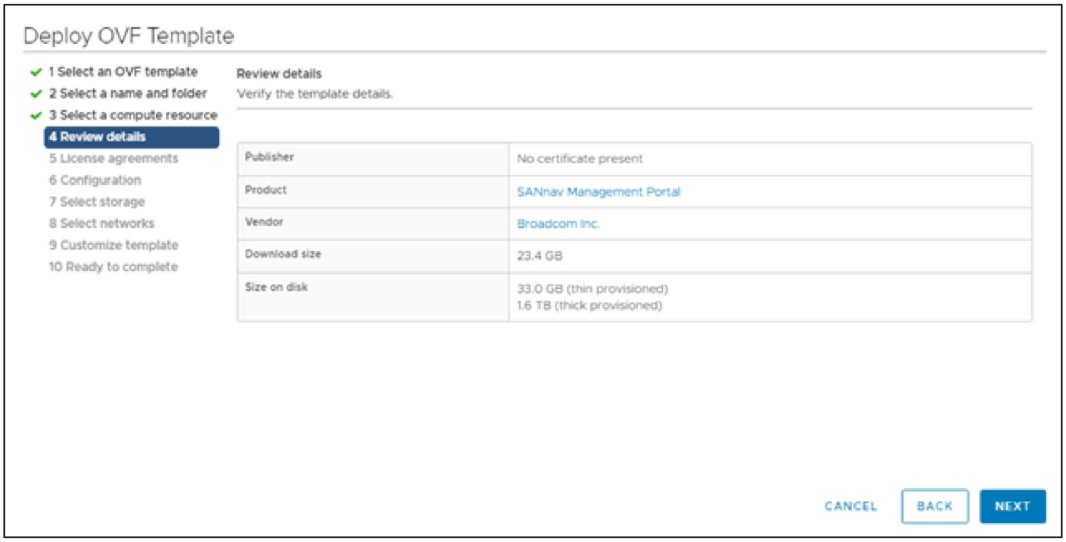
- Datacenter
  - [redacted]
  - [redacted]

Compatibility

✓ Compatibility checks succeeded.

d) **Review details**.

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



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

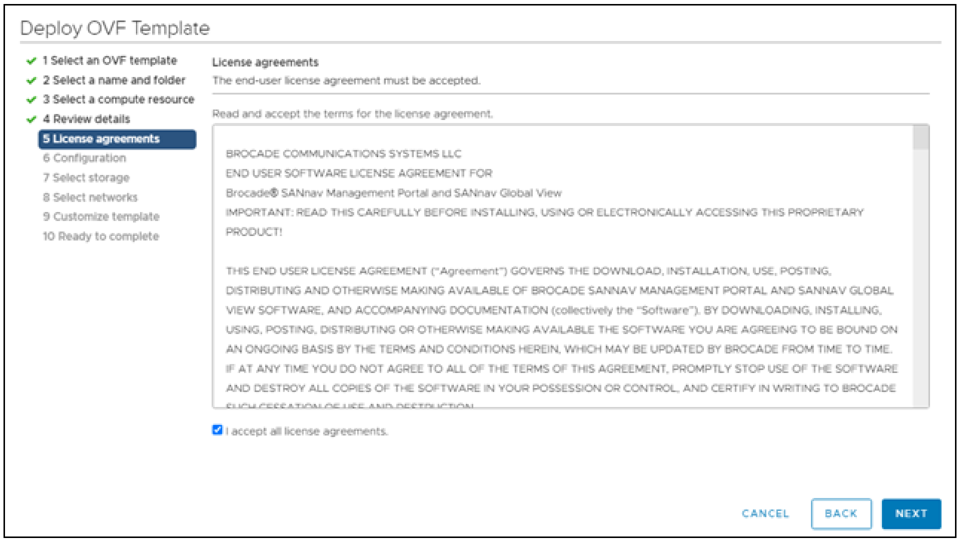
Review details

Verify the template details.

Publisher	No certificate present
Product	SANnav Management Portal
Vendor	Broadcom Inc.
Download size	23.4 GB
Size on disk	33.0 GB (thin provisioned) 1.6 TB (thick provisioned)

e) **License agreements**.

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



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

License agreements

The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

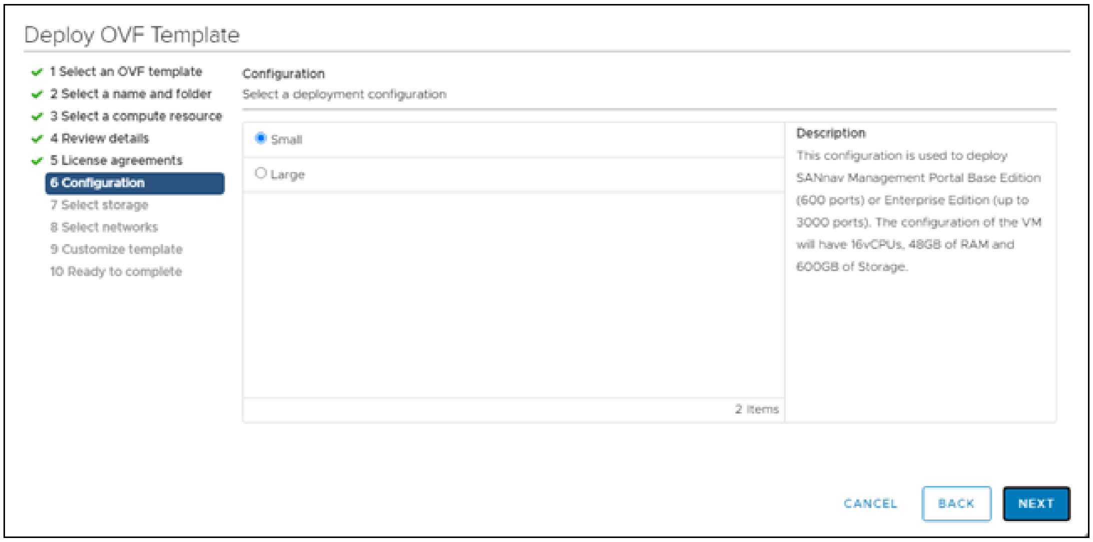
BROCADE COMMUNICATIONS SYSTEMS LLC
END USER SOFTWARE LICENSE AGREEMENT FOR
Brocade® SANnav Management Portal and SANnav Global View
IMPORTANT: READ THIS CAREFULLY BEFORE INSTALLING, USING OR ELECTRONICALLY ACCESSING THIS PROPRIETARY PRODUCT!

THIS END USER LICENSE AGREEMENT ("Agreement") GOVERNS THE DOWNLOAD, INSTALLATION, USE, POSTING, DISTRIBUTING AND OTHERWISE MAKING AVAILABLE OF BROCADE SANNAV MANAGEMENT PORTAL AND SANNAV GLOBAL VIEW SOFTWARE, AND ACCOMPANYING DOCUMENTATION (collectively the "Software"). BY DOWNLOADING, INSTALLING, USING, POSTING, DISTRIBUTING OR OTHERWISE MAKING AVAILABLE THE SOFTWARE YOU ARE AGREEING TO BE BOUND ON AN ONGOING BASIS BY THE TERMS AND CONDITIONS HEREIN, WHICH MAY BE UPDATED BY BROCADE FROM TIME TO TIME. IF AT ANY TIME YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, PROMPTLY STOP USE OF THE SOFTWARE AND DESTROY ALL COPIES OF THE SOFTWARE IN YOUR POSSESSION OR CONTROL, AND CERTIFY IN WRITING TO BROCADE SUCH CESSATION OF USE AND DESTRUCTION

☑ I accept all license agreements.

f) **Configuration**.

The **Small** configuration includes 48 GB of memory, which supports the Base License (600 ports) or 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.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Configuration

Select a deployment configuration

● Small

○ Large

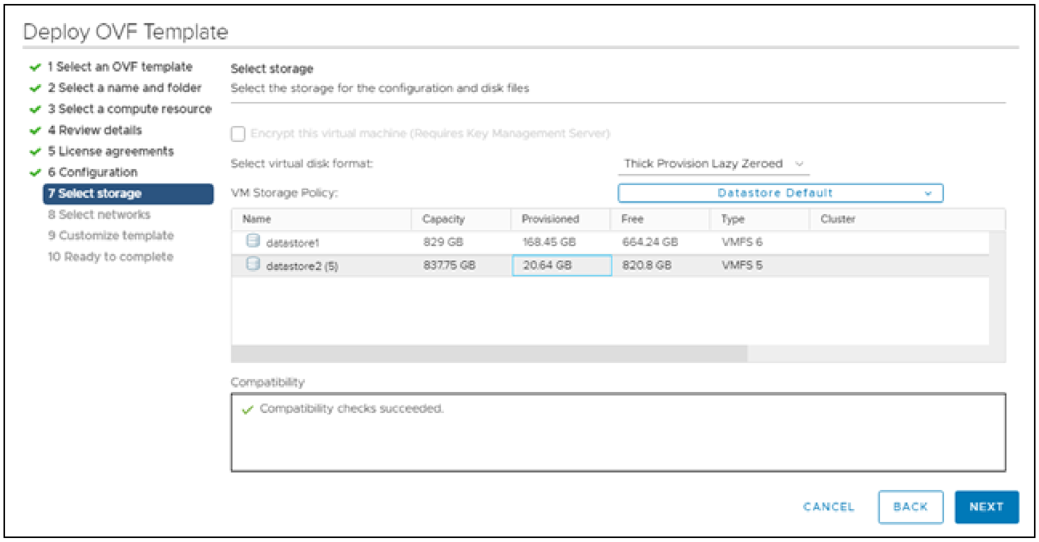
2 items

Description

This configuration is used to deploy SANnav Management Portal Base Edition (600 ports) or Enterprise Edition (up to 3000 ports). The configuration of the VM will have 16vCPUs, 48GB of RAM and 600GB of Storage.

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**.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type	Cluster
datastore1	829 GB	168.45 GB	664.24 GB	VMFS 6	
datastore2 (5)	837.75 GB	20.64 GB	820.8 GB	VMFS 5	

Compatibility

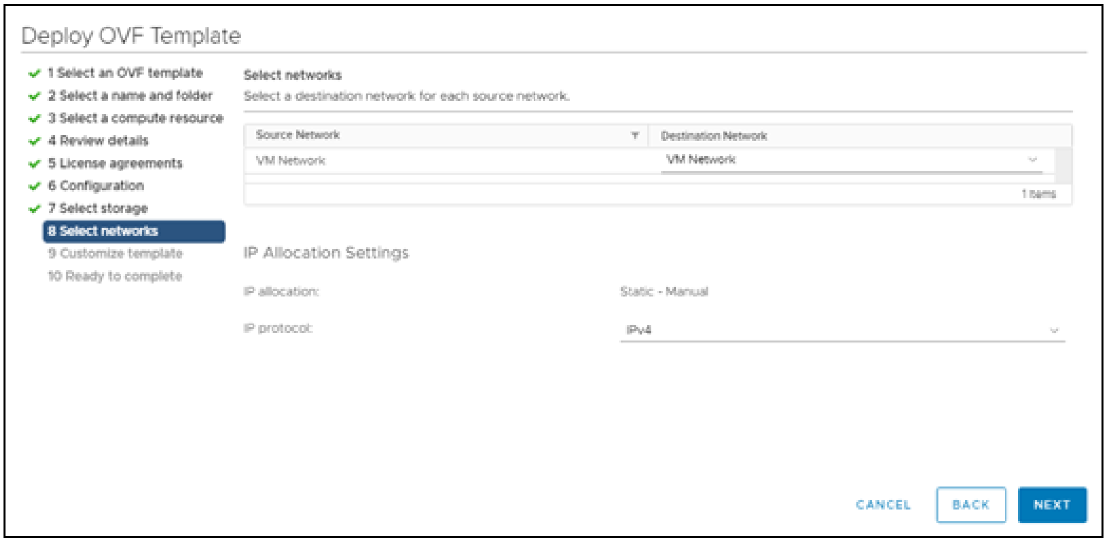
✓ Compatibility checks succeeded.

h) **Select networks**.

Choose the IP allocation strategy and IP protocol:

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

Click **Next**.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

1 items

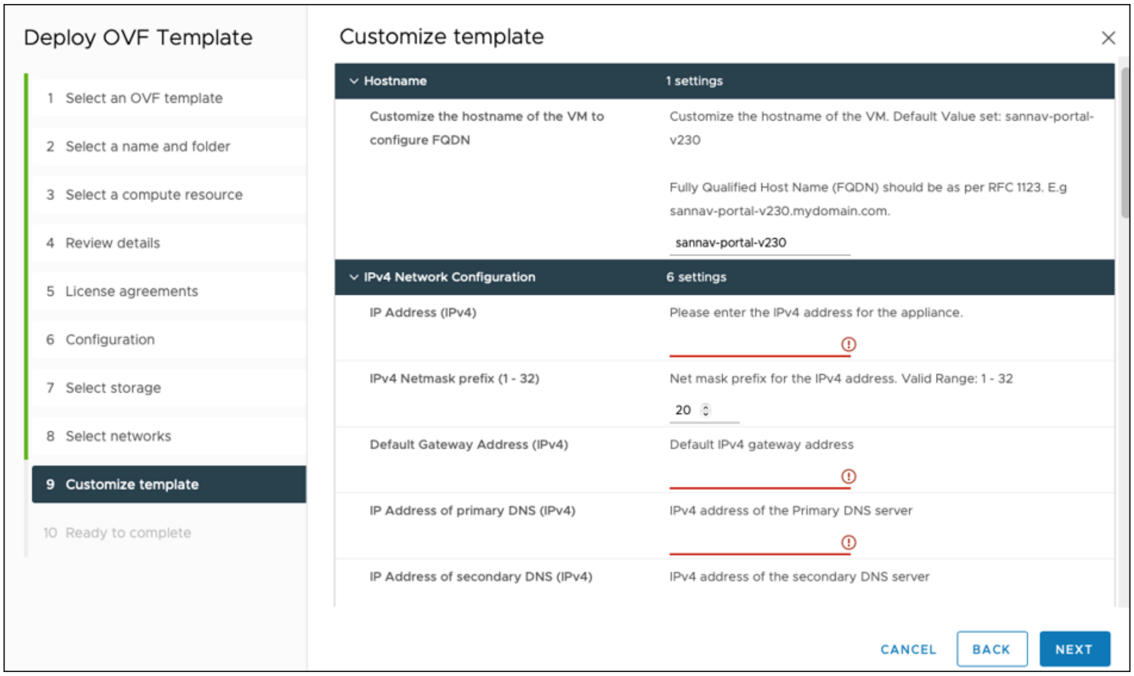
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

i) **Customize template**.

Provide all values for SANnav customization.



Deploy OVF Template

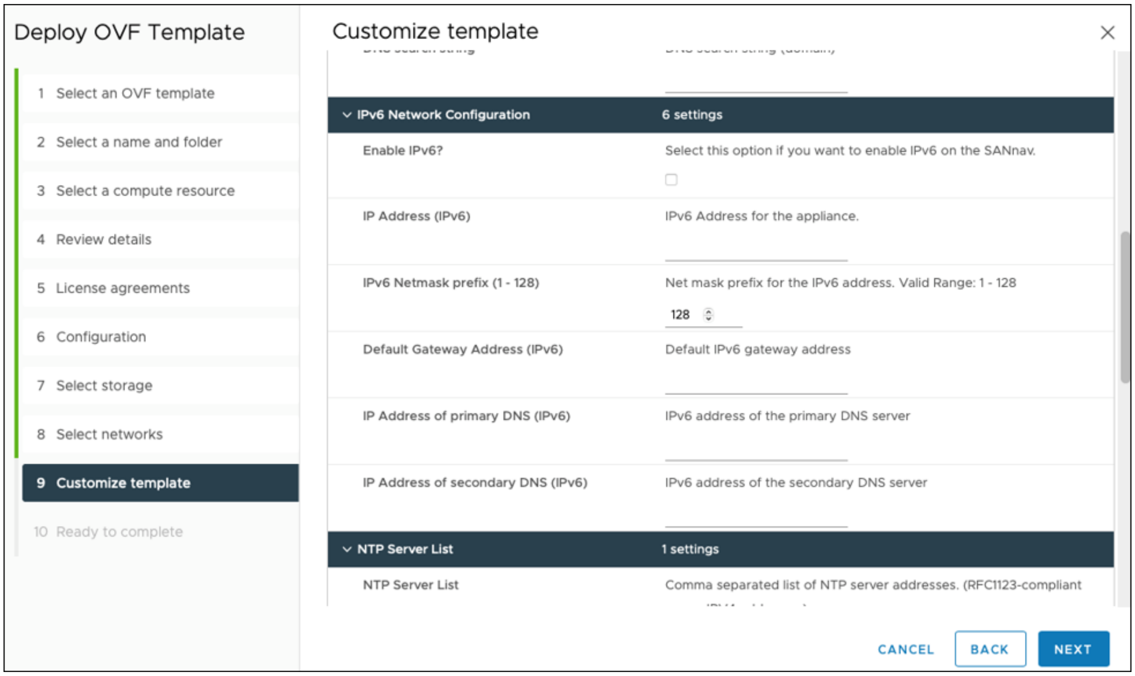
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Customize template

Hostname	1 settings
Customize the hostname of the VM to configure FQDN	Customize the hostname of the VM. Default Value set: sannav-portal-v230 Fully Qualified Host Name (FQDN) should be as per RFC 1123. E.g sannav-portal-v230.mydomain.com. sannav-portal-v230
IPv4 Network Configuration	**6 settings**
IP Address (IPv4)	Please enter the IPv4 address for the appliance.
IPv4 Netmask prefix (1 - 32)	Net mask prefix for the IPv4 address. Valid Range: 1 - 32 20
Default Gateway Address (IPv4)	Default IPv4 gateway address
IP Address of primary DNS (IPv4)	IPv4 address of the Primary DNS server
IP Address of secondary DNS (IPv4)	IPv4 address of the secondary DNS server

IPv4 Network Configuration. SANnav Management Portal appliance does not support DHCP. Only IP Static - Manual allocation policy is supported. The IP Address of secondary DNS and DNS search string properties are optional.

IPv6 Network Configuration: If you choose to enable IPV6 on the SANnav Management Portal appliance, you must enter the values for IPV6 address, Netmask, Gateway, and primary DNS. The IP Address of the secondary DNS property is optional. DHCP for IPV6 configuration is not supported.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

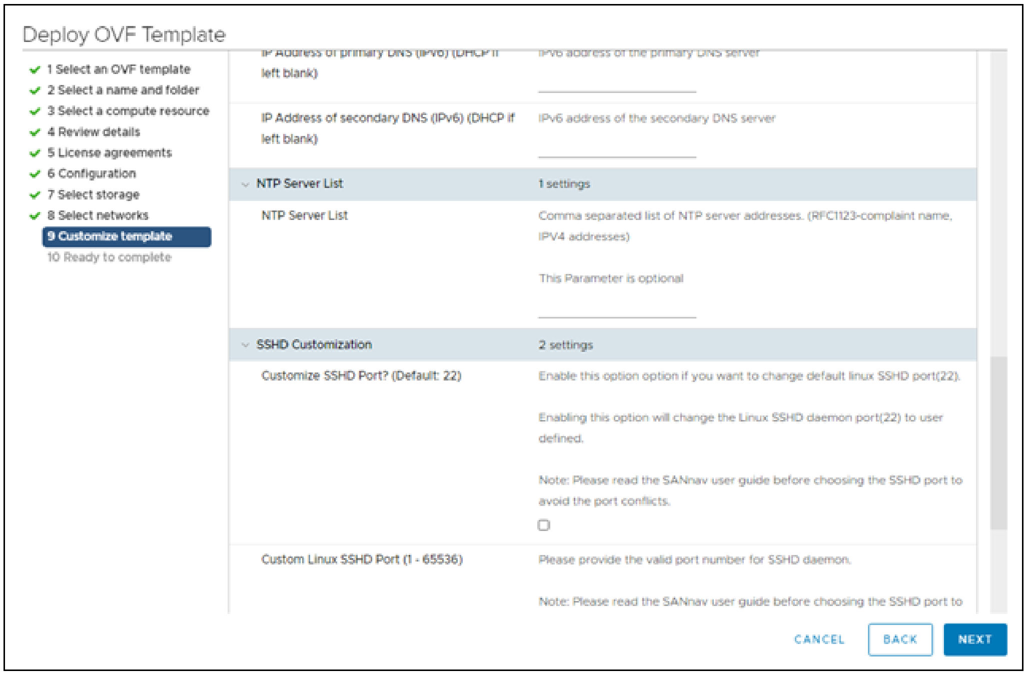
Customize template

IPv6 Network Configuration	6 settings
Enable IPv6?	Select this option if you want to enable IPv6 on the SANnav. □
IP Address (IPv6)	IPv6 Address for the appliance.
IPv6 Netmask prefix (1 - 128)	Net mask prefix for the IPv6 address. Valid Range: 1 - 128 128
Default Gateway Address (IPv6)	Default IPv6 gateway address
IP Address of primary DNS (IPv6)	IPv6 address of the primary DNS server
IP Address of secondary DNS (IPv6)	IPv6 address of the secondary DNS server
NTP Server List	1 settings
NTP Server List	Comma separated list of NTP server addresses. (RFC1123-compliant

Host Name: The default host name is set to **sannav-portal-<*version*>**. If you want to change this name, you can enter a new name or FQDN. If you plan to use secure syslog in SANnav, it is recommended to configure FQDN for the SANnav Management Portal appliance VM.

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

SSHD Customization: By default, port 22 is used for the Linux/VM server management. If you want to change this port, select the checkbox and enter the new port number. See Installation Prerequisites for VM and Bare Metal Deployment for additional information about changing port 22.



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
✓ 5 License agreements
✓ 6 Configuration
✓ 7 Select storage
✓ 8 Select networks
9 Customize template
10 Ready to complete

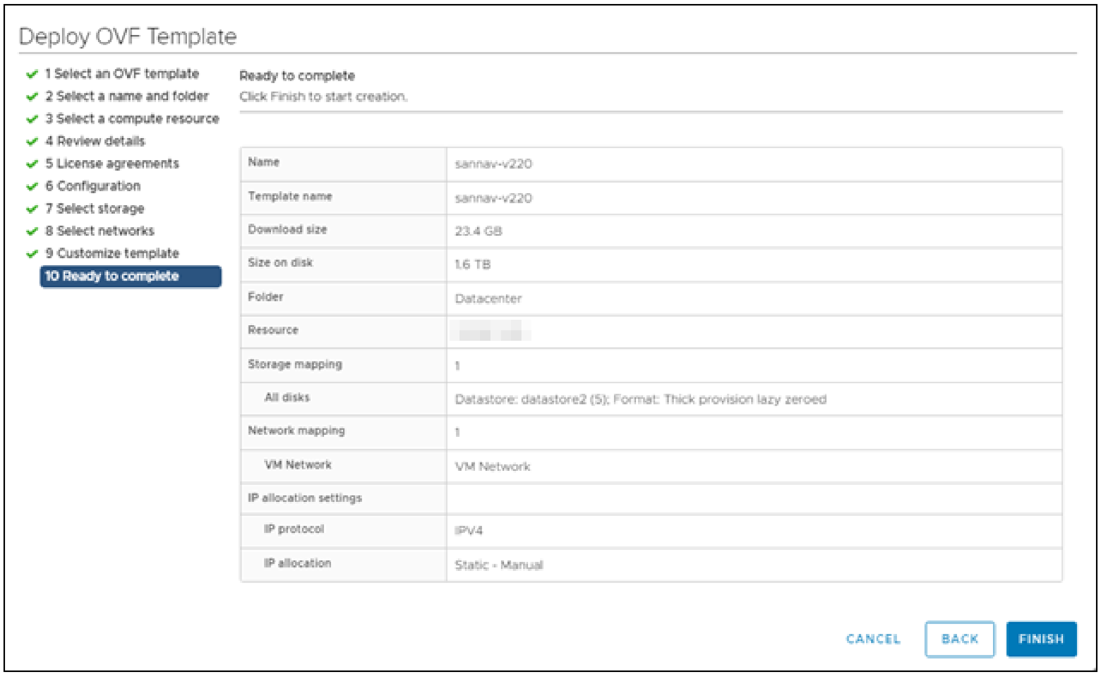
IP Address of primary DNS (IPv6) (DHCP if left blank)	IPv6 address of the primary DNS server
IP Address of secondary DNS (IPv6) (DHCP if left blank)	IPv6 address of the secondary DNS server
NTP Server List	1 settings
NTP Server List	Comma separated list of NTP server addresses. (RFC1123-compliant name, IPV4 addresses) This Parameter is optional
SSHD Customization	2 settings
Customize SSHD Port? (Default: 22)	Enable this option option if you want to change default linux SSHD port(22). Enabling this option will change the Linux SSHD daemon port(22) to user defined. Note: Please read the SANnav user guide before choosing the SSHD port to avoid the port conflicts. □
Custom Linux SSHD Port (1 - 65536)	Please provide the valid port number for SSHD daemon. Note: Please read the SANnav user guide before choosing the SSHD port to

Application services subnet: This network is used internally. Enter a new IP address range if there are any conflicts with 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**.



Ready to complete

Click Finish to start creation.

Name	sannav-v220
Template name	sannav-v220
Download size	23.4 GB
Size on disk	1.6 TB
Folder	Datacenter
Resource	[redacted]
Storage mapping	1
All disks	Datastore: datastore2 (5); Format: Thick provision lazy zeroed
Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

3. After successful network configuration, log on as the root user through the VM console or SSH terminal.
4. Start the SANnav Management Portal installation on OVA. For detailed information, see Installing SANnav Management Portal on OVA Deployments.

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

Installing SANnav Management Portal on OVA Deployments

After successful OVA extraction and configuration of all the VM parameters including Network Configuration parameters, perform the following steps to install SANnav.

> **NOTE**
> If the `/install-sannav.sh` script fails during the installation or startup, you must uninstall SANnav in OVA, reboot the server, and then redeploy the OVA.

1. Go to the `/sannav-home/<install_home>/bin` directory.

   ```
   cd /sannav-home/Portal_<version>_bldxx/bin
   ```

2. Execute the following script to install the SANnav Management Portal.

   ```
   ./install-sannav.sh
   ```

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

3. If you are prompted about migrating the SANnav server, 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 either back up the current SANnav instance; and restart the installation script or you can uninstall the current SANnav instance and can restart the installation script without migrating.
4. Read and respond to each prompt carefully.

   NOTE

   Some installation parameters cannot be updated after installation. If you must update these parameters after installation, you must uninstall and then reinstall SANnav.

   On the successful installation of the software, the SANnav Management Portal server starts up. The startup may take up to 15 minutes.
5. Check the SANnav status by running the following script:

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

NOTE

- After installation, do not modify the name of the installation directory or the permissions of the files and folders in the SANnav installation directory.
- If you upgrade from a previous version of SANnav, after the upgrade, you must clear the browser cache before launching the new version of SANnav.

Upgrading the SANnav Appliance from 2.2.1

Upgrading from SANnav Appliance 2.2.1 to 2.3.x is not supported directly. You must first perform an inline upgrade to SANnav 2.2.2 Appliance before you upgrade to 2.3.x Appliance.

NOTE

- Before you start the upgrade, take a backup of the current SANnav installation.
- After the upgrade, it is your responsibility to update Rocky Linux with new security patches on the SANnav server (if required).

To upgrade SANnav Appliance 2.2.1 to SANnav Appliance 2.2.2, perform the following steps:

1. Back up the current SANnav installation and save it in a location outside of the VM.
2. Log on to the current SANnav Appliance VM as the root user.
3. Download the SANnav 2.2.2 tar file to the `<sannav_home>` directory.

   The `<sannav_home>` directory is not the `<install_home>` directory, but is the directory above the `<install_home>` directory ((*/sannav-home*).

   The file name is `Portal_2.2.2_<build>-distribution.tar.gz` .
4. Verify the authenticity of the downloaded tarball by validating the MD5 checksum. Run the command `md5sum Portal_2.2.2_build-distribution.tar.gz` . Match the printed checksum with the MD5 checksum file present in Broadcom Portal.
5. Untar the .gz file to extract the file to the current location.

```
tar -xvf Portal_<version>_<build>-distribution.tar.gz
```

6. Go to the untarred directory (`Portal_<version>_<build>/bin`) and execute the `install-sannav.sh` script to start the migration.

At the end of the upgrade, if the host name of SANnav OVA is left as the default (for example, sannav-portal-v221), the host name will be changed to reflect the upgraded version (for example, sannav-portal-v222). The login banner will also be updated to reflect the upgraded SANnav version. You must log out and must log on to the VM to see the updated host name and banner.

Upgrading the SANnav Appliance from 2.2.2x

Upgrading the SANnav Appliance from 2.2.2x to 2.3.0x involves the following tasks:

1. Preparing for the SANnav Management Portal Appliance Upgrade.
2. Deploying the SANnav OVA Package.
3. Upgrading the SANnav Management Portal Appliance.

Preparing for the SANnav Management Portal Appliance Upgrade

If you are upgrading the SANnav Management Portal Appliance from 2.2.2x, you must perform some additional steps before you start the deployment.

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

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

- The ESXi version where the SANnav Management Portal appliance is running and where the new SANnav appliance will be deployed should be the same. If the versions cannot be the same, then the VMDK file of the current SANnav Management Portal appliance must be accessible from the vCenter datastores.
- At least 640 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 the SANnav Management Portal appliance after you complete the upgrade and uninstall the earlier version of SANnav.

Perform the following steps to prepare the SANnav Management Portal appliance for upgrade:

1. Back up the current SANnav installation and save it in a location outside of the current virtual machine (VM).
2. (*Optional*) Release the license from the current SANnav installation, and copy the rehost key for later use when generating the SANnav license on the new installation.

   Refer to the section "Rehosting a License on a Different Server: Planned Migration" in the *Brocade SANnav Management Portal User Guide* for details.

   If you do not release the license now, it is automatically released during migration.
3. Stop the current SANnav server.

   ```
   <install_home>/bin/stop-sannav.sh
   ```
4. Copy the MAC address of the current SANnav VM.

   You can use Ctrl-C in vCenter to copy the MAC address.

   NOTE
   The MAC address to copy is the address of the Network Interface Card (NIC) that is used by SANnav to communicate with the switches. This MAC address is used during the upgrade process and is mandatory for license migration. If you do not manually update the MAC address on the new SANnav VM, the license is not migrated.
5. Power off the VM.

   Next, proceed with Deploying the SANnav OVA Package.

Deploying the SANnav OVA Package

During the deployment, you can select a Small or Large configuration. The hardware specifications are configured depending on the selected configuration.

Perform the following steps to deploy the SANnav OVA package using vCenter:

1. Download the SANnav OVA package.

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

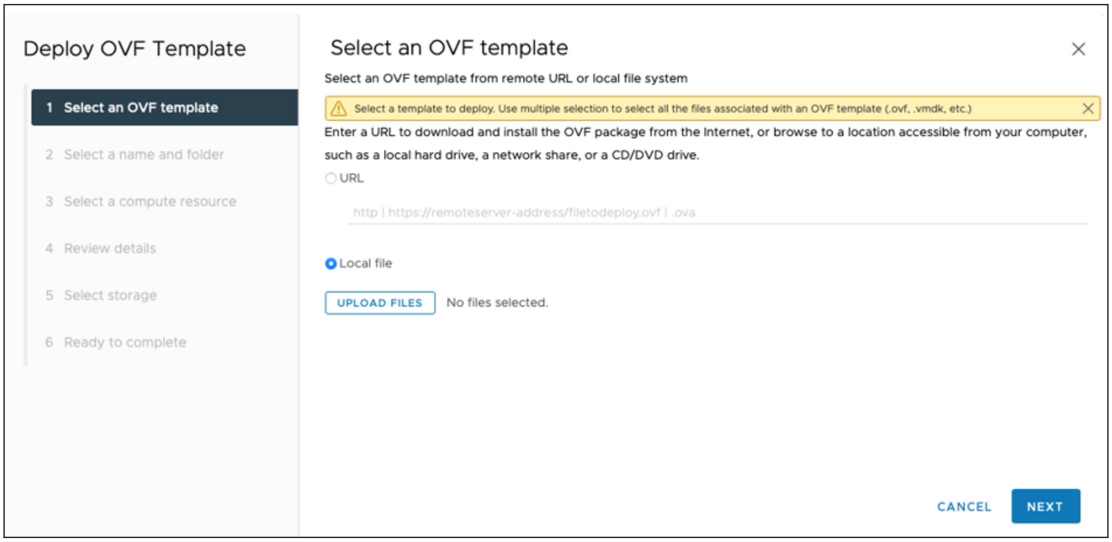
2. Log on to vCenter, right-click the host on which you want to deploy SANnav, and select **Deploy OVF Template**.

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

   NOTE
   The following steps correspond to the steps in the vCenter interface. The screenshots are for 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**.



Select an OVF template

Select an OVF template from remote URL or local file system

Select a template to deploy. Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

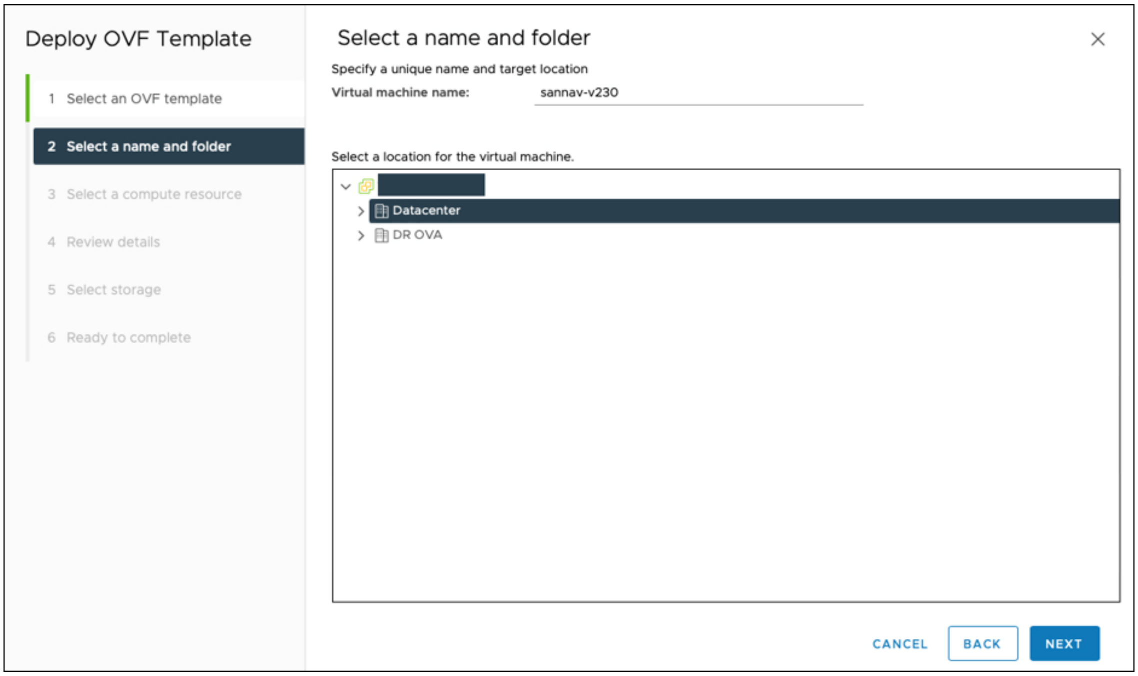
http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

No files selected.

   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**.



Deploy OVF Template

Select a name and folder

Specify a unique name and target location

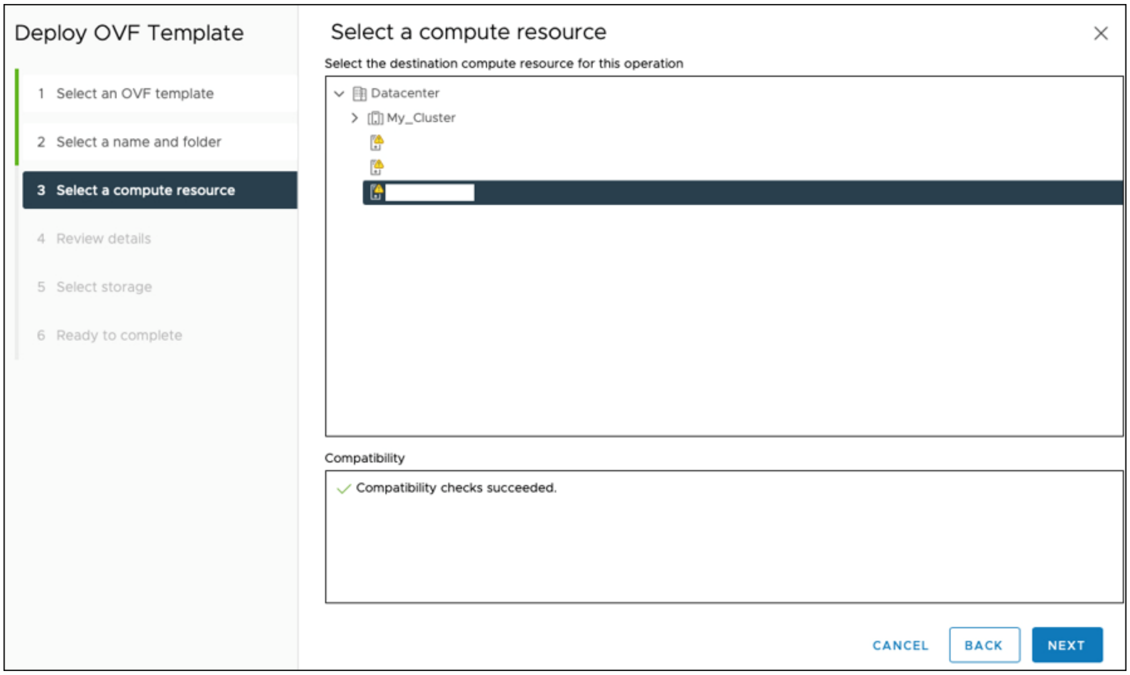
Virtual machine name: sannav-v230

Select a location for the virtual machine.

[redacted]

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**.



Deploy OVF Template

Select a compute resource

Select the destination compute resource for this operation

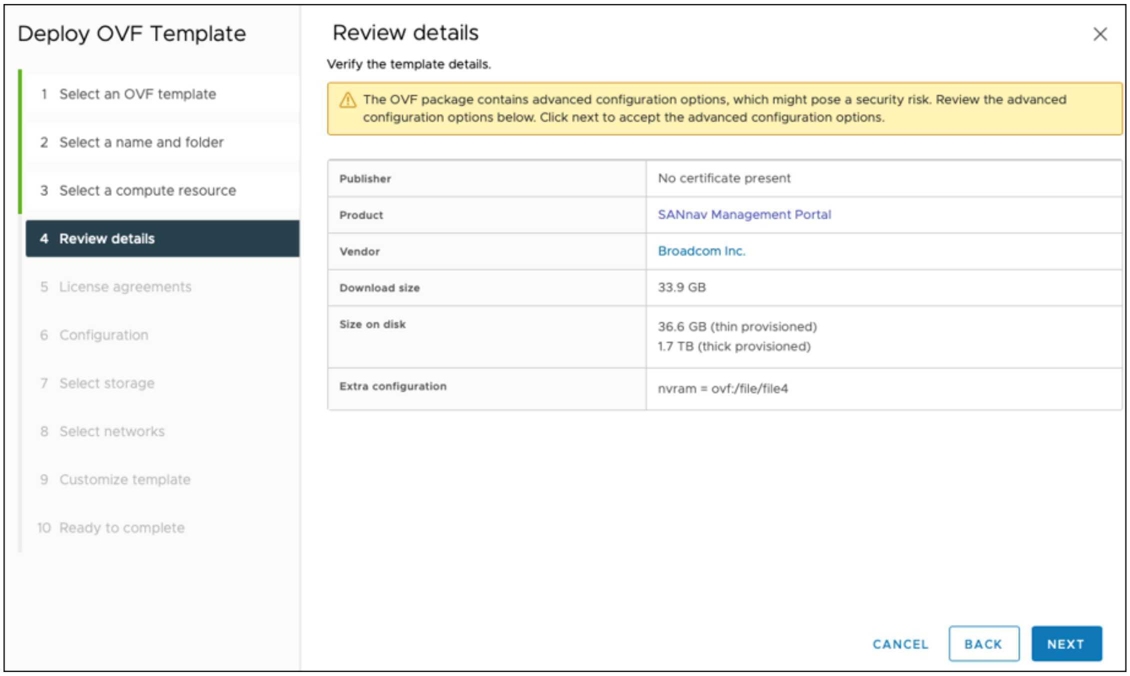
[redacted]

Compatibility

✓ Compatibility checks succeeded.

d) **Review details**.

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



Review details

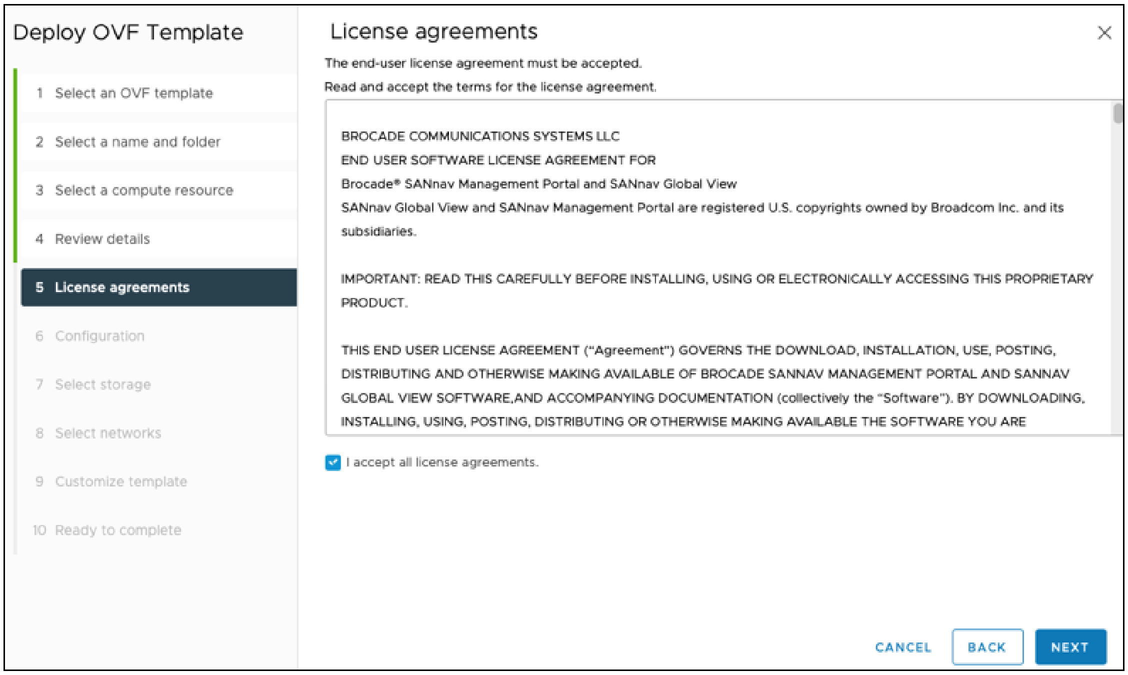
Verify the template details.

The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	No certificate present
Product	SANnav Management Portal
Vendor	Broadcom Inc.
Download size	33.9 GB
Size on disk	36.6 GB (thin provisioned) 1.7 TB (thick provisioned)
Extra configuration	nvram = ovf:/file/file4

e) **License agreements**.

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



License agreements

The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

BROCADE COMMUNICATIONS SYSTEMS LLC
END USER SOFTWARE LICENSE AGREEMENT FOR
Brocade® SANnav Management Portal and SANnav Global View
SANnav Global View and SANnav Management Portal are registered U.S. copyrights owned by Broadcom Inc. and its subsidiaries.

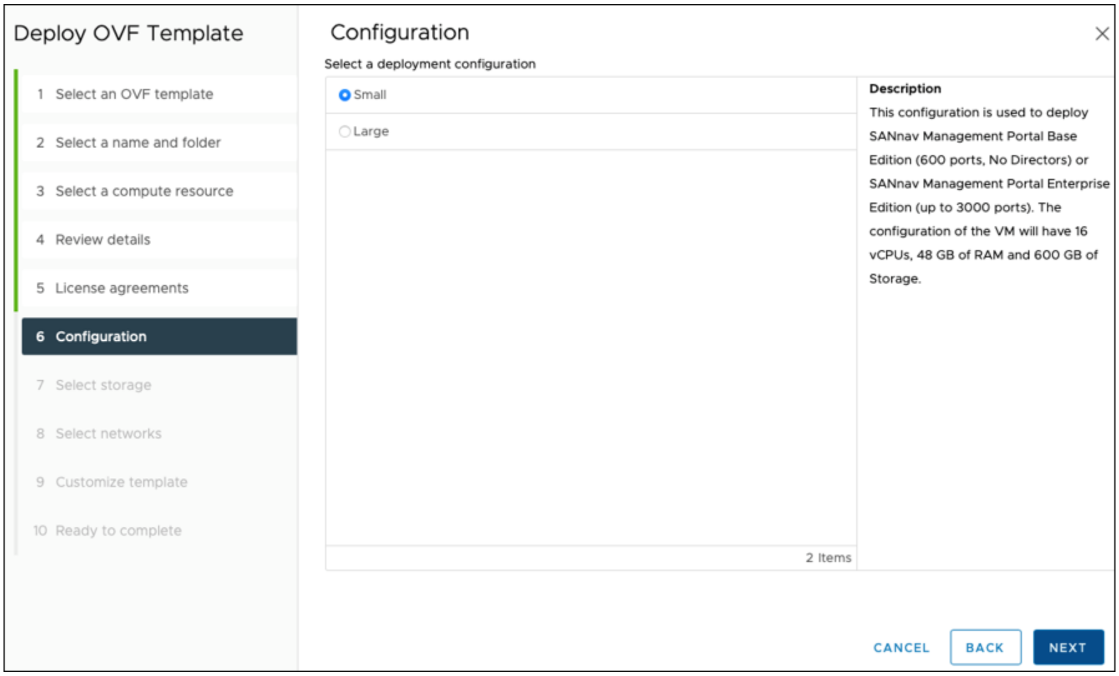
IMPORTANT: READ THIS CAREFULLY BEFORE INSTALLING, USING OR ELECTRONICALLY ACCESSING THIS PROPRIETARY PRODUCT.

THIS END USER LICENSE AGREEMENT ("Agreement") GOVERNS THE DOWNLOAD, INSTALLATION, USE, POSTING, DISTRIBUTING AND OTHERWISE MAKING AVAILABLE OF BROCADE SANNAV MANAGEMENT PORTAL AND SANNAV GLOBAL VIEW SOFTWARE,AND ACCOMPANYING DOCUMENTATION (collectively the "Software"). BY DOWNLOADING, INSTALLING, USING, POSTING, DISTRIBUTING OR OTHERWISE MAKING AVAILABLE THE SOFTWARE YOU ARE

☑ I accept all license agreements.

f) **Configuration**.

The **Small** configuration includes 48-GB memory, which supports the Base License (600 ports) or 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.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Configuration

Select a deployment configuration

● Small
○ Large

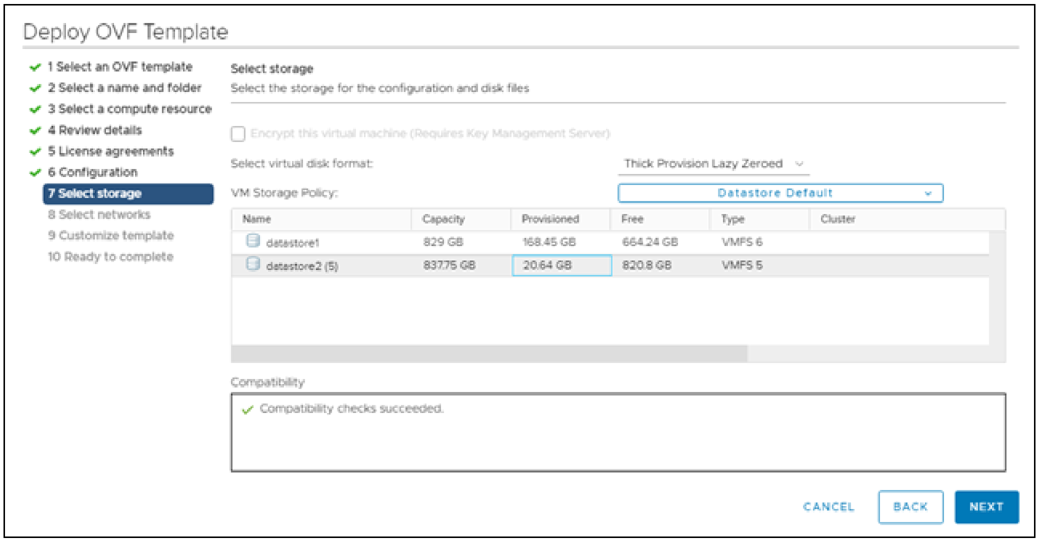
2 Items

Description

This configuration is used to deploy SANnav Management Portal Base Edition (600 ports, No Directors) or SANnav Management Portal Enterprise Edition (up to 3000 ports). The configuration of the VM will have 16 vCPUs, 48 GB of RAM and 600 GB of Storage.

g) **Select storage**.

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



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
✓ 5 License agreements
✓ 6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type	Cluster
datastore1	829 GB	168.45 GB	664.24 GB	VMFS 6	
datastore2 (5)	837.75 GB	20.64 GB	820.8 GB	VMFS 5	

Compatibility

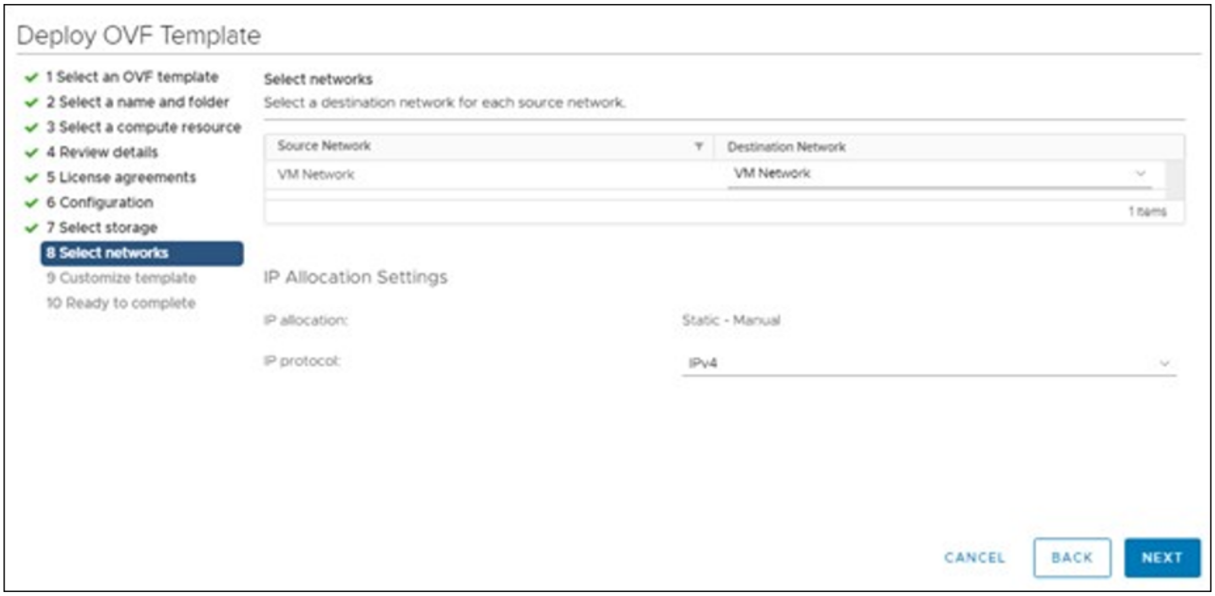
✓ Compatibility checks succeeded.

h) **Select networks**.

Choose the IP allocation strategy and IP protocol:

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

Click **Next**.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

1 items

IP Allocation Settings

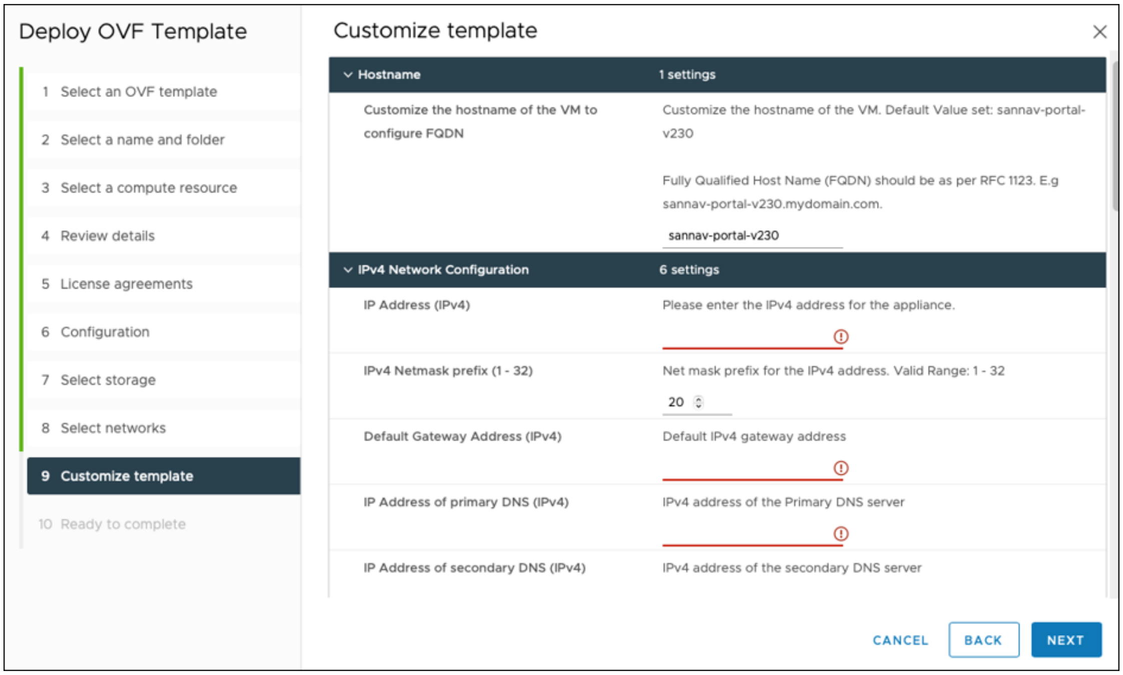
IP allocation: Static - Manual

IP protocol: IPv4

i) **Customize template**.

Provide all values for SANnav customization.

IPv4 Network Configuration. SANnav Management Portal appliance does not support DHCP. Only IP **Static - Manual** allocation policy is supported. The **IP Address of secondary DNS** and **DNS search string** properties are optional.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Customize template

Hostname — 1 settings

Customize the hostname of the VM to configure FQDN: Customize the hostname of the VM. Default Value set: sannav-portal-v230

Fully Qualified Host Name (FQDN) should be as per RFC 1123. E.g sannav-portal-v230.mydomain.com.

sannav-portal-v230

IPv4 Network Configuration — 6 settings

IP Address (IPv4): Please enter the IPv4 address for the appliance.

IPv4 Netmask prefix (1 - 32): Net mask prefix for the IPv4 address. Valid Range: 1 - 32

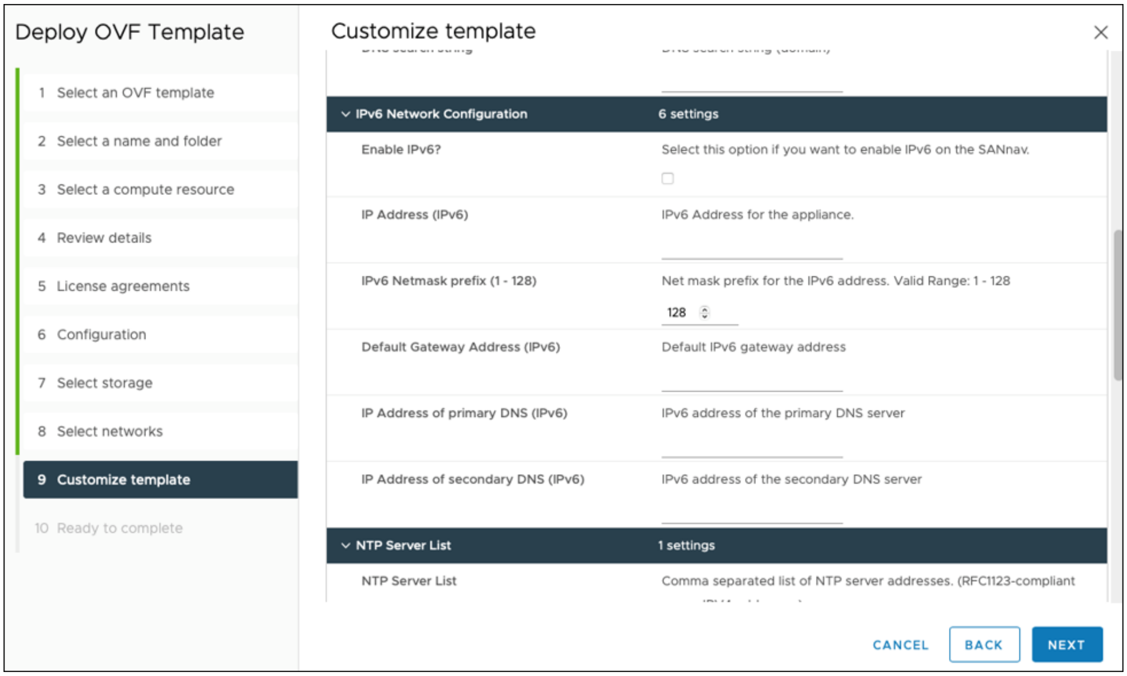
20

Default Gateway Address (IPv4): Default IPv4 gateway address

IP Address of primary DNS (IPv4): IPv4 address of the Primary DNS server

IP Address of secondary DNS (IPv4): IPv4 address of the secondary DNS server

IPv6 Network Configuration: If you choose to enable IPv6 on the SANnav Management Portal appliance, you must enter the values for the IPv6 address, Netmask, Gateway, and primary DNS. The **IP Address of secondary DNS** property is optional. DHCP for IPv6 configuration is not supported.



Customize template

IPv6 Network Configuration — 6 settings

Enable IPv6? — Select this option if you want to enable IPv6 on the SANnav. □

IP Address (IPv6) — IPv6 Address for the appliance.

IPv6 Netmask prefix (1 - 128) — Net mask prefix for the IPv6 address. Valid Range: 1 - 128 — 128

Default Gateway Address (IPv6) — Default IPv6 gateway address

IP Address of primary DNS (IPv6) — IPv6 address of the primary DNS server

IP Address of secondary DNS (IPv6) — IPv6 address of the secondary DNS server

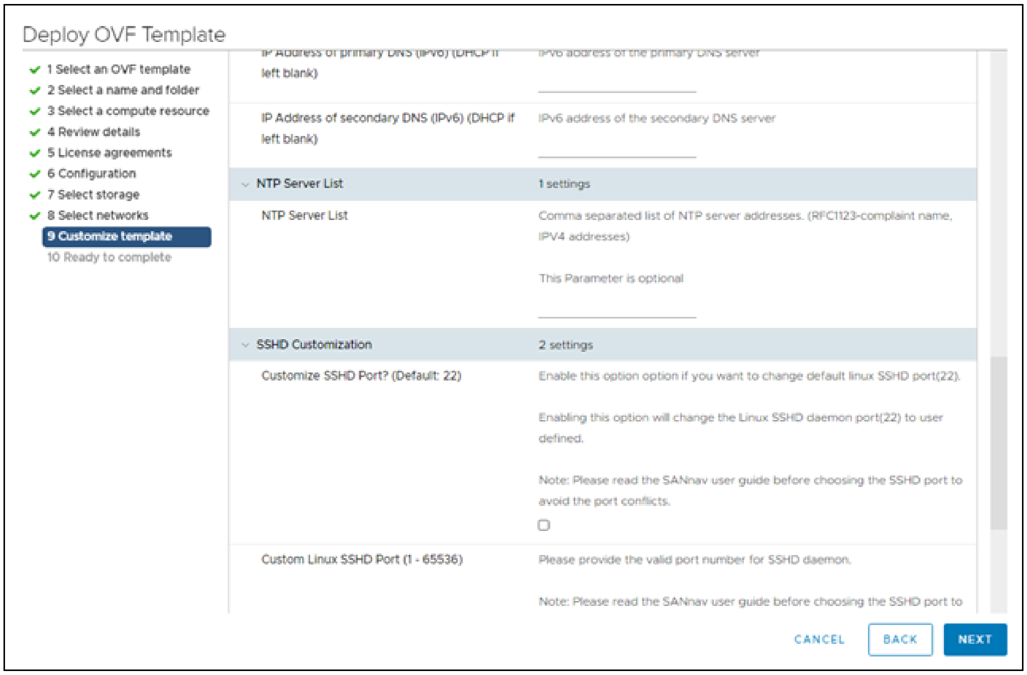
NTP Server List — 1 settings

NTP Server List — Comma separated list of NTP server addresses. (RFC1123-compliant

Host Name: The default host name is set to **sannav-portal-<*version*>**. If you want to change this name, you can enter a new name or FQDN. If you plan to use a secure syslog in SANnav, it is recommended to configure FQDN for the SANnav Management Portal appliance VM.

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

SSHD Customization: By default, port 22 is used for the Linux/VM server management. If you want to change this port, select the checkbox and enter the new port number. See Installation Prerequisites for VM and Bare Metal Deployment for additional information about changing port 22.



IP Address of primary DNS (IPv6) (DHCP if left blank) — IPv6 address of the primary DNS server

IP Address of secondary DNS (IPv6) (DHCP if left blank) — IPv6 address of the secondary DNS server

NTP Server List — 1 settings

NTP Server List — Comma separated list of NTP server addresses. (RFC1123-complaint name, IPV4 addresses)

This Parameter is optional

SSHD Customization — 2 settings

Customize SSHD Port? (Default: 22) — Enable this option option if you want to change default linux SSHD port(22).

Enabling this option will change the Linux SSHD daemon port(22) to user defined.

Note: Please read the SANnav user guide before choosing the SSHD port to avoid the port conflicts.

□

Custom Linux SSHD Port (1 - 65536) — Please provide the valid port number for SSHD daemon.

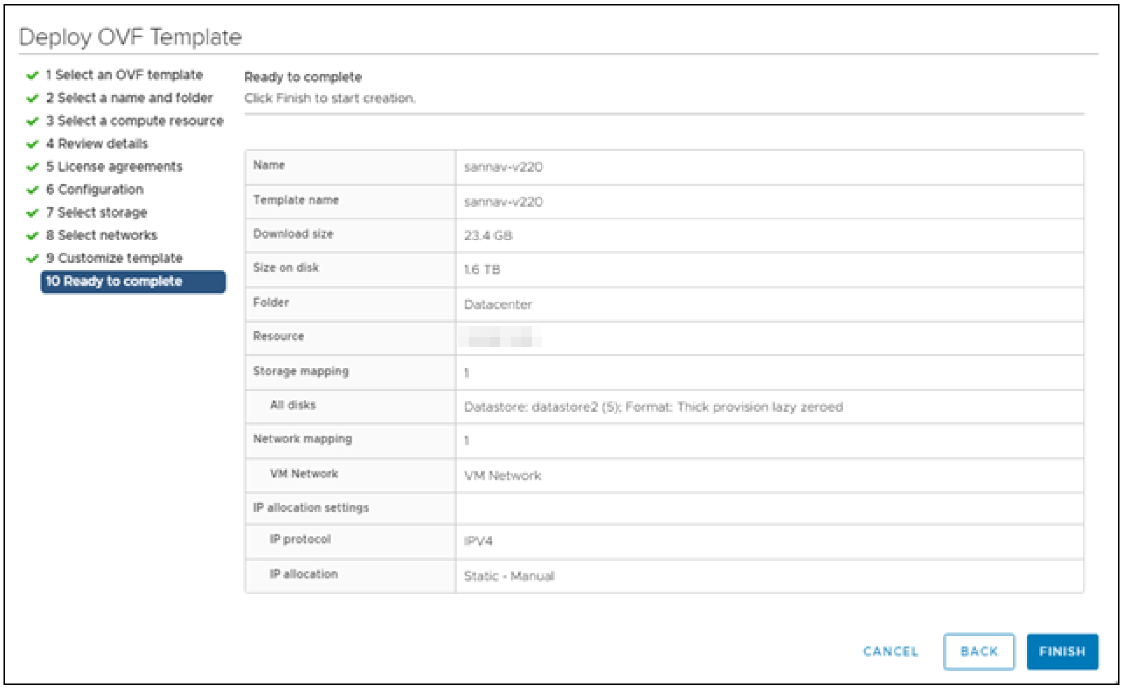
Note: Please read the SANnav user guide before choosing the SSHD port to

Application services subnet: This network is used internally. Enter a new IP address range if there are any conflicts with 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**.



Ready to complete

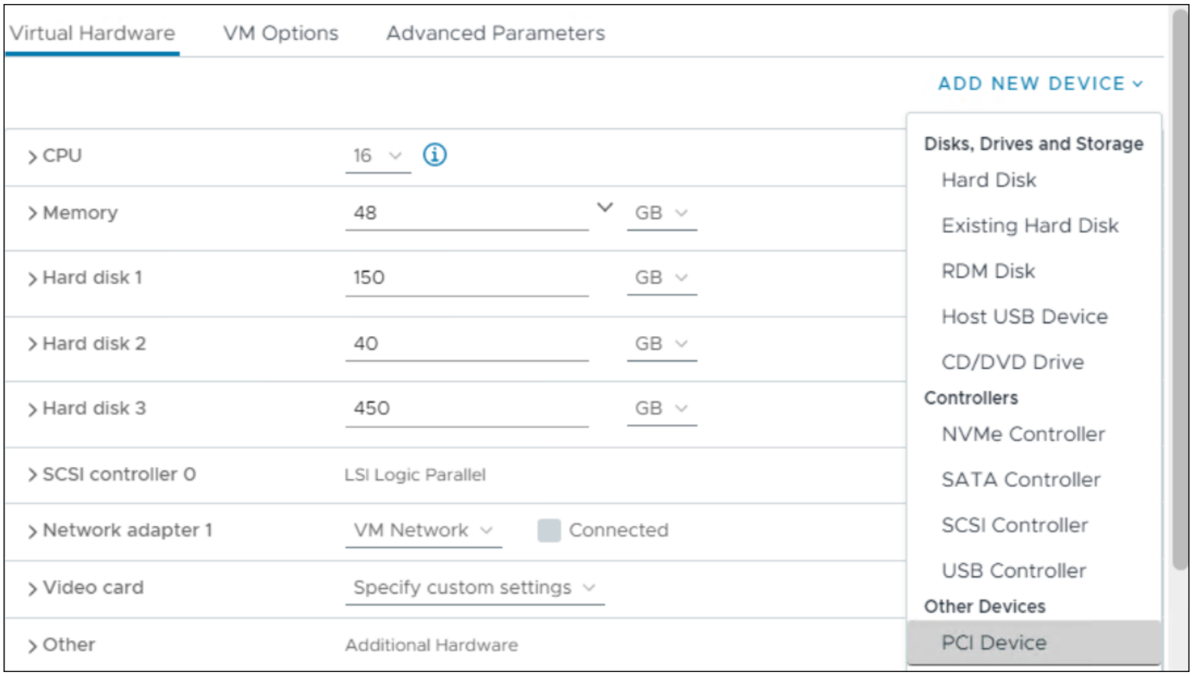
Click Finish to start creation.

Name	sannav-v220
Template name	sannav-v220
Download size	23.4 GB
Size on disk	1.6 TB
Folder	Datacenter
Resource	[redacted]
Storage mapping	1
All disks	Datastore: datastore2 (5); Format: Thick provision lazy zeroed
Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

NOTE

Do not power on the VM now.

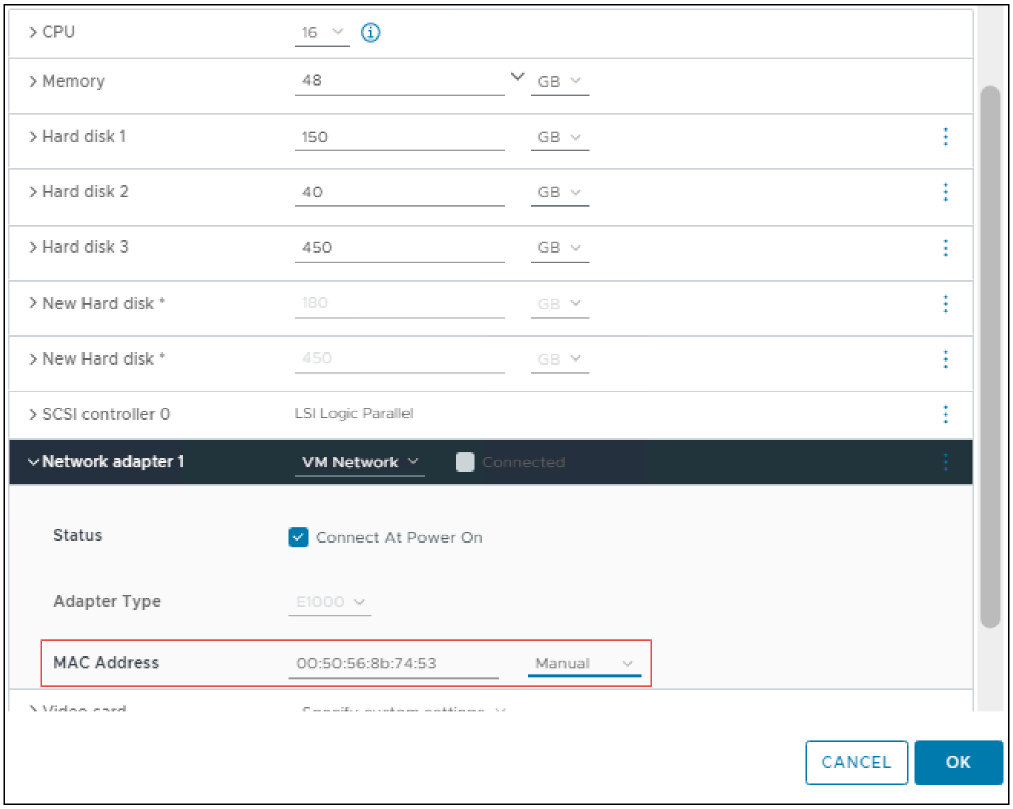
3. Attach the VMDK file from the earlier version of SANnav as a new disk. Ensure to attach both the VMDK files from the source for migration:
   a) Right-click the newly deployed VM.
   b) Select **Edit Settings > Add New Device > Existing Hard Disk**.



> CPU 16
> Memory 48 GB
> Hard disk 1 150 GB
> Hard disk 2 40 GB
> Hard disk 3 450 GB
> SCSI controller 0 LSI Logic Parallel
> Network adapter 1 VM Network □ Connected
> Video card Specify custom settings
> Other Additional Hardware

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

4. 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**.



> CPU 16
> Memory 48 GB
> Hard disk 1 150 GB
> Hard disk 2 40 GB
> Hard disk 3 450 GB
> New Hard disk * 180 GB
> New Hard disk * 450 GB
> SCSI controller 0 LSI Logic Parallel
⌄ Network adapter 1 VM Network ☐ Connected

Status ☑ Connect At Power On

Adapter Type E1000

MAC Address 00:50:56:8b:74:53 Manual

> Video card Specify custom settings

5. Power on the VM.

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

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

6. After you power on the VM, the disk is automatically mounted. You can check that the disk is successfully attached using the `fdisk -l /dev/sdc` command. Check that the disk is successfully mounted and the mount point folder is created using the `lsblk` command. If the disk is attached, but the mount point folder is not created, you can manually mount the disk using the `mount-sannav-disk.sh` command.

Next, proceed to Upgrading the SANnav Management Portal Appliance.

Upgrading the SANnav Management Portal Appliance

Perform the following steps to upgrade the SANnav Management Portal appliance from an earlier version:

1. Log on to the SANnav terminal as the root user and start the installation (`/sannav-home/Portal_<version>_<build>/bin/install-sannav.sh`).

   The new disk is automatically detected and the upgrade script starts.

   SANnav detects if a new disk is attached to the VM and issues a prompt:

```
Found an additional disk attached to this VM. If it is a SANnav disk for migrating data, Press Enter
 (Yes / Y) or (No / N) to install SANnav: [Yes]
```

2. Press **Enter** to continue with migration.

   The steps in this script are the same as for the initial installation. Read each prompt carefully before responding.

After the upgrade completes, the disk is unmounted. At this point, you can power off the VM, remove the disk, and delete the VM for the previous SANnav version.

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

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

Post-Installation for OVA Deployment

After the SANnav installation completes, you may need to perform some post-installation tasks.

- Recover from upgrade failure.

  If the SANnav upgrade fails, you can return to the previous version. See Recovering from Upgrade Failure of the SANnav Management Portal Appliance.
- Uninstall SANnav and bring the system back to its original state.

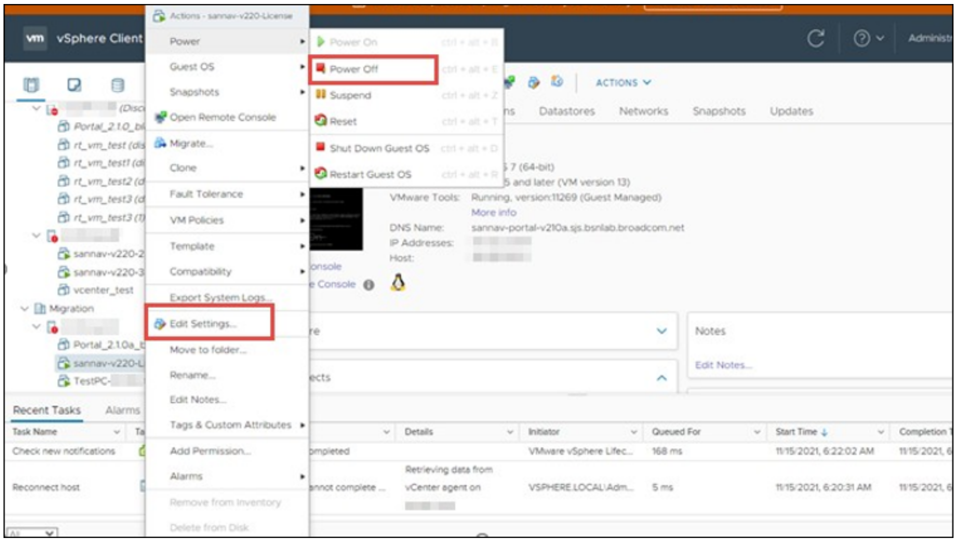
  See Uninstalling the SANnav Management Portal Appliance.

  NOTE
  It is your responsibility to update CentOS with security patches on the SANnav server after SANnav has been installed and deployed.

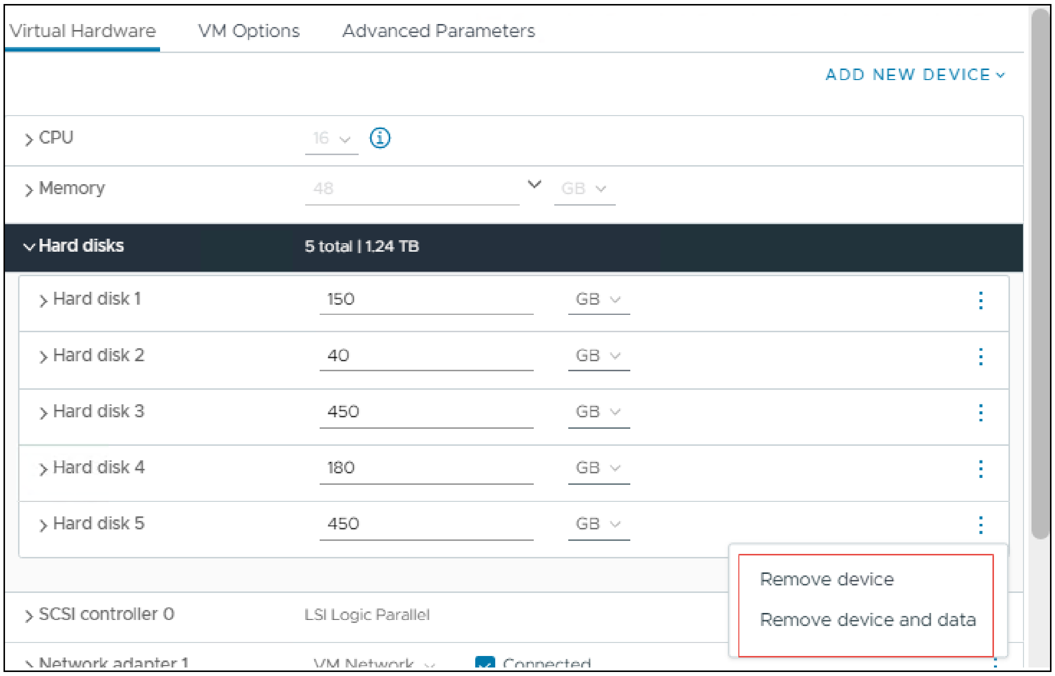
Recovering from Upgrade Failure of the SANnav Management Portal Appliance

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

1. Power off the VM (Failed OVA), and select the **Edit Settings** option.

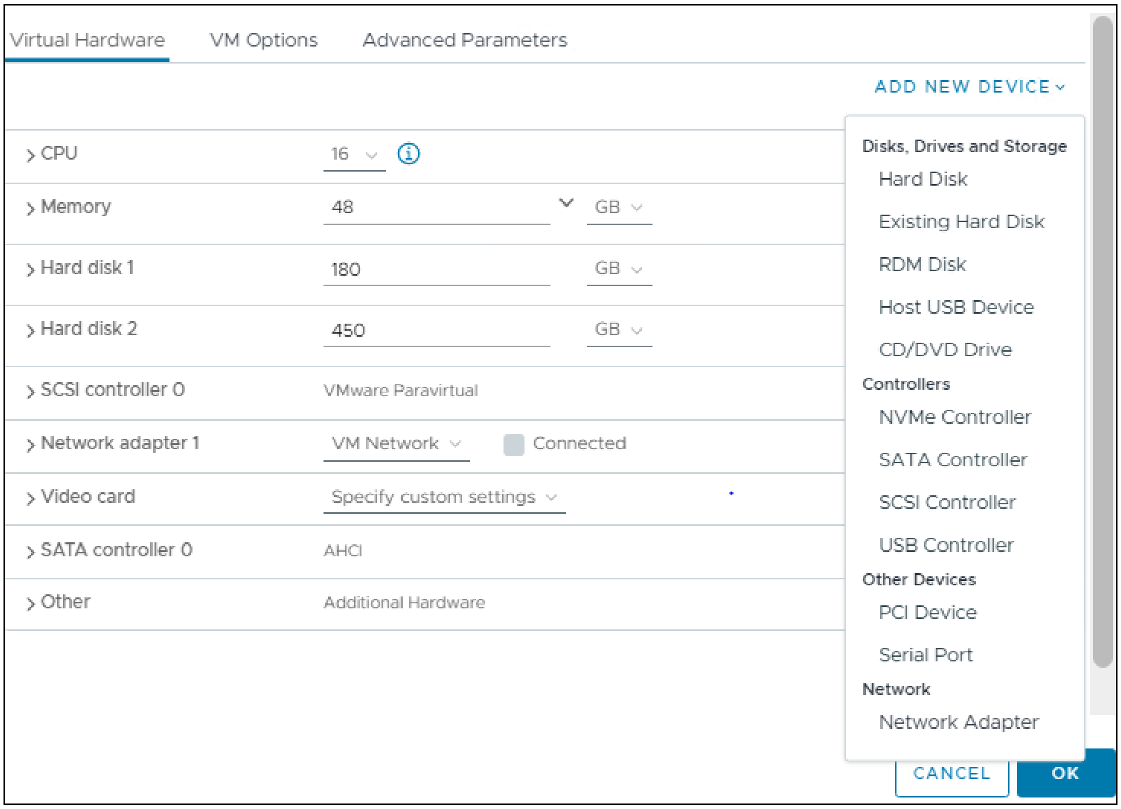


2. Detach the source hard disk drive (HDD).



CPU	16	
Memory	48	GB
Hard disks	5 total | 1.24 TB	
Hard disk 1	150	GB
Hard disk 2	40	GB
Hard disk 3	450	GB
Hard disk 4	180	GB
Hard disk 5	450	GB
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	VM Network	☑ Connected

3. Attach the HDD to the source server again.



> CPU 16

> Memory 48 GB

> Hard disk 1 180 GB

> Hard disk 2 450 GB

> SCSI controller 0 VMware Paravirtual

> Network adapter 1 VM Network □ Connected

> Video card Specify custom settings

> SATA controller 0 AHCI

> Other Additional Hardware

4. Power on the source server.
5. Log on to the source server, go to `<install_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 VM.
2. Delete the VM.

Installation Log File

A log file is created during the SANnav installation process. You can use the log file to troubleshoot installation errors, if any.

During the SANnav installation process, the log file is saved to the following directory:

```
<install_home>/logs
```

You can list installation logs by using the following command:

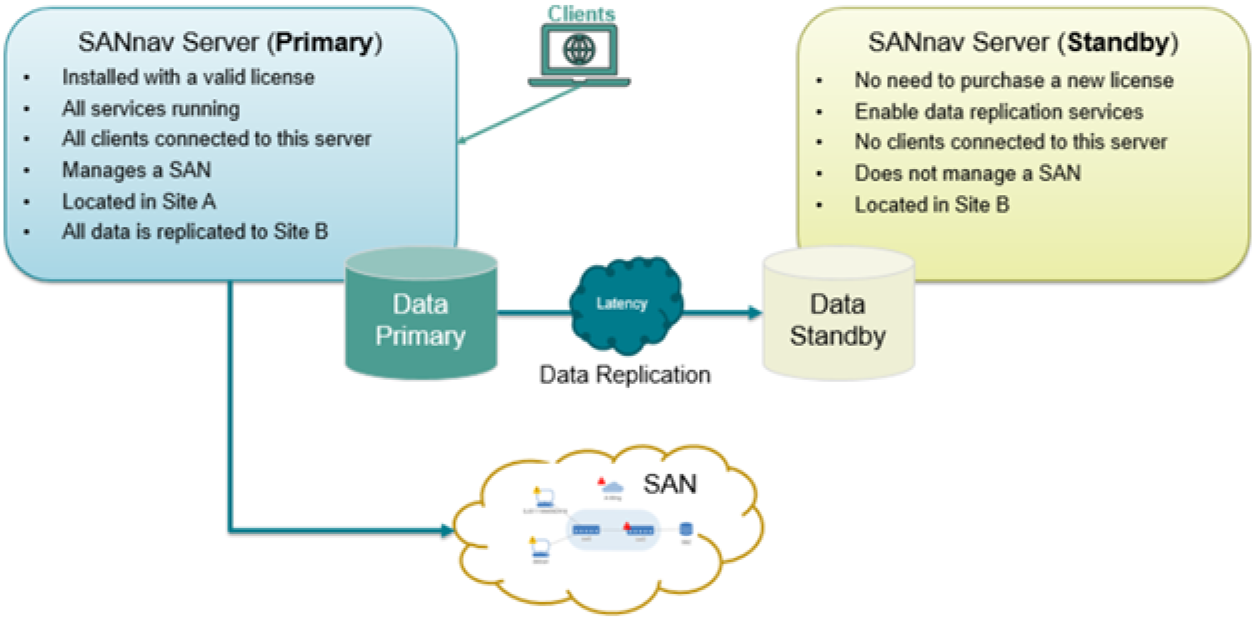
```
ls -ltr install*.log
```

Disaster Recovery

The 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 in an hour or less.

Without 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.

Figure 1: Disaster Recovery Components


SANnav Server (Primary)
Installed with a valid license
All services running
All clients connected to this server
Manages a SAN
Located in Site A
All data is replicated to Site B
Clients
SANnav Server (Standby)
No need to purchase a new license
Enable data replication services
No clients connected to this server
Does not manage a SAN
Located in Site B
Data Primary
Latency
Data Replication
Data Standby
SAN

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 in less than an hour.

After the failover completes, the standby server is now the only SANnav server, and you must 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

Before configuring Disaster Recovery (DR) in SANnav Management Portal, ensure that your system meets the requirements that are listed here.

Disaster Recovery is supported *only* for Enterprise licenses. Disaster Recovery is not available for Base licenses.

Disaster Recovery is supported in VM deployments and in OVA deployments with SANnav v2.3.0. 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:

- **Primary Node** – The primary node is the active node where SANnav is fully installed and all services are running. When Disaster Recovery is enabled, users can access and stream data to this server.
- **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.

The following are additional requirements for Disaster Recovery:

- 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 SANnav installation must be an IPv4 installation. Dual-stack IPv4/IPv6 installation is not supported.
- 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 following table lists the system requirements for Disaster Recovery.

Table 13: System Requirements for Disaster Recovery

Component	Requirement
Operating system	RHEL 8.4 and 8.6 and higher 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 or SANnav OVA appliance Bare metal and Hyper-V are not supported. If you have an existing version of SANnav installed on bare metal or Hyper-V and you migrate to SANnav 2.3.0x, you cannot enable Disaster Recovery. If you are planning to enable DR on OVA, ensure both primary and standby nodes are OVA. Mix and Match are not allowed.
CPUs	24
License	The SANnav primary node requires an Enterprise license. The SANnav standby node does not require a license.
Bandwidth latency between primary and standby servers	Maximum latency between the primary and standby servers: 100 ms. Minimum dedicated bandwidth between the primary and standby servers: 100 Mb/s.

Ports That Must Be Open in the Firewall for Disaster Recovery

For SANnav Management Portal, 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 14: Ports That Must Be Open in the Firewall

Port Number	Transport	Inbound/Outbound	Communication Path	Description
5432	TCP	Both	Primary server --> Standby server	Used for data replication.
SANnav DR SSH Port	TCP	Both	Primary server --> Standby server	Used for the SSH connection between the primary and standby nodes.
SANnav DR REST Port	TCP	Both	Primary server --> Standby server	Used for REST communication between the primary and standby nodes.
SANnav DR IPERF Port	TCP	Both	Primary server --> Standby server	Used to calculate the bandwidth between the primary and standby nodes.

NOTE
SANnav disaster recovery SSH, REST, and Iperf ports are not fixed port numbers. These port numbers are allocated based on the port range user has allocated for SANnav during installation. Execute `<install_home>/bin/manage-sannav-configurations.sh` and press option **5** to see the port numbers that are allocated for these services.

Upgrading and Disaster Recovery

After upgrading SANnav Management Portal, disaster recovery is disabled, and you must set up disaster recovery again.

If disaster recovery is enabled, you must initiate the upgrade from the primary node. The upgrade script notifies you if it detects that disaster recovery is configured on the server.

Perform the following steps to upgrade the primary server and reconfigure disaster recovery:

1. On the primary server, perform the SANnav upgrade.

   See Upgrading from an Earlier Release of SANnav.

   Disaster recovery is disabled after a successful upgrade.

2. After the upgrade, log on to the standby server and run the following script:

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

3. After uninstallation completes, reboot the standby server.

4. Log on to the upgraded SANnav server and configure disaster recovery as a primary node using the following script:

   ```
   <install_home>/bin/dr/setup-dr-primary.sh
   ```

5. On the standby server, set up disaster recovery.

   See Setting Up Disaster Recovery on the Standby Node.

6. On both the primary node and the standby node, run the following command to check the status of the disaster recovery setup.

   ```
   <install_home>/bin/dir/show-dr-status.sh
   ```

Tasks for Setting Up Disaster Recovery

You must perform the following tasks to set up disaster recovery in SANnav Management Portal:

- Install SANnav on the primary node.
- Set up disaster recovery on the primary node.
- Set up disaster recovery on the standby node.
- (Optional) Set up a web proxy for license rehosting.

In addition, SANnav provides a script (`show-dr-status.sh`) that shows you the status of disaster recovery.

> **NOTE**
>
> - Make sure to follow the disaster recovery procedures correctly; otherwise, you may have to restart the entire process from the beginning.
> - After disaster recovery is set up, do not uninstall SANnav services on the standby node. If you must replace the standby node, see Replacing the Standby Node.

Setting Up Disaster Recovery on the Primary Node

The first task for configuring disaster recovery is to set up the SANnav Management Portal server 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 an Enterprise license. You cannot use a Base license.

3. Go to `<install_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.

> **NOTE**
>
> If you are setting up disaster recovery as a `sudo` user, ensure that the same user is set up for both Primary and Standby nodes.

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

After you install SANnav Management Portal and set up disaster recovery on the primary node, you must set up disaster recovery on the standby node. You do not install SANnav on the standby node.

Perform the following steps on the server that is to be used as the standby node:

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

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

2. Verify the authenticity of the downloaded tarball by validating the MD5 checksum. Run the command `md5sum Portal_<version>-distribution.tar.gz` . Match the printed checksum with the MD5 checksum file present in Broadcom Portal.
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 `<install_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 address

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

NOTE
SANnav sends an email to the configured address if the primary node detects that the standby node is unreachable. If these addresses are incorrect, SANnav will fail to send the email.

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. See Requirements for Disaster Recovery for bandwidth latency requirements.

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

If the SANnav server does not have access to the internet, see Setting Up a Web Proxy for Internet Connectivity.

NOTE
If you reboot the standby node, you must manually load the iptables using the following steps:

1. Log on to the SANnav SSH terminal.
2. Go to `<install_home>/bin/tools` and run the following script:

```
sannav-iptable-block-ports.sh apply_dr_iptables_rules_standby
```

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 `<install_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 Management Portal:

- 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 of SANnav Management Portal 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.

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

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

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

   The script displays the last successful checkpoint to which the system will be restored. The time that is 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 *if the server has external internet connectivity*:
      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.

      If the server cannot connect to the internet or the Licensing Portal is not reachable, SANnav creates a new temporary license that is valid for 30 days.
   4. Starts all services on the standby node.

After failover completes, you can log on to the new SANnav server. 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 SANnav Management Portal 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 SANnav Management Portal standby node in certain circumstances.

The following are situations in which the standby node must be replaced:

- 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:

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

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

   During script execution, provide the following information:

   - The IPv4 address of the new 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 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.

Resetting or Uninstalling Disaster Recovery

After successfully setting the Disaster Recovery or if you want to remove Disaster Recovery at any time, perform the following steps: Executing this script restarts SANnav server.

1. Uninstall the Disaster Recovery on the standby server if configured. Run the following script on the standby server: `<install_home>/bin/uninstall-sannav.sh`.
2. Log in to the Disaster Recovery Primary server.
3. On the Disaster Recovery Primary server, run the following script: `<install_home>/bin/dr/reset-dr-primary.sh`.

On the successful execution of this script, Disaster Recovery is uninstalled. You can reset the Disaster Recovery later based on your requirement. Executing this script restarts the SANnav server.

Tasks to be Performed 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 15: 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: `<install_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, Syslog, and telemetry 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.
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 license certificate is not retrieved. In this case, SANnav creates a new, temporary 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 creation. After 30 days, SANnav prevents access until you provide a valid 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 primary SANnav Management Portal server in Global View.

Disaster Recovery Impact on Other Features

When disaster recovery is enabled in SANnav Management Portal, other features may be impacted.

Table 16: 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. A backup that is collected from the primary node is intended to be restored on a different SANnav instance. 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.
Support data collection	Support data collection 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 `<`*`install_home`*`>/bin/dr` and run the following script: `collect-supportsave-standby.sh`

Scripts for Managing the SANnav Server

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 VM, bare metal, and OVA installations.

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

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

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

Table 17: SANnav User-Executable Scripts

Script	Description
`add-user-to-sannavmgr-group.sh`	Allows a Linux root user or a user with `sudo` privileges to add another user with `sudo` privileges to the `sannavmgr` group.
`change-ipv4-installation-to-ipv6.sh`	Changes SANnav from an IPv4 installation to a dual-stack IPv4/IPv6 installation.
change-sannav-authentication-to-local.sh	Changes the SANnav authentication from SAML Identity Provider (IdP) to Local Database.
`check-sannav-firewall-status.sh`	Checks if firewalld is enabled and if the required ports are open.
`check-sannav-status.sh`	Checks the status of the SANnav server.
`check-sannav-system-requirements.sh`	Checks that the system requirements for SANnav installation are met, in a VM or bare metal deployment. Not supported in an OVA installation.
`delete-ssh-key.sh`	Deletes the ssh-keypair.ser. A new key is generated by the server when the first file transfer operation is performed.
`install-sannav.sh`	Installs the SANnav server. SANnav should not be running when you run this script.
`manage-sannav-configurations.sh`	Allows you to perform several actions on the SANnav server.
`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 96 GB, to support 15,000 ports. Before running this script, ensure that the memory capacity of the SANnav host is at least 96 GB.
`remove-sannav-audit-rules.sh`	Deletes Linux audit rules created by SANnav during the installation. Deleted audit rules cannot be added again.
`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.
`troubleshooting-sannav.sh`	Detects drifts in the SANnav system requirements.

Script	Description
`setup-webproxy.sh`	Configures a proxy to connect to the Internet.
`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 that is 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.
`trigger-trufos-check-and-renew.sh`	Triggers a call to the license portal to get TruFOS certificates without waiting for the regularly scheduled TruFOS check.
`uninstall-sannav.sh`	Uninstalls the SANnav server.
`update-auto-enclosure-features.sh`	Enables and disables automatic host and storage enclosure creation during fabric discovery. By default, this feature is enabled.
`update-reports-purge-settings.sh`	Changes the number of days after which reports are automatically deleted.
`usage-data-collection.sh`	Configures whether collected SANnav usage data is sent to Broadcom.

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

Table 18: 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.
`pause-dr.sh`	Primary node	Temporarily pause disaster recovery service.
`replace-standby.sh`	Primary node	Replaces the standby node with a different standby node.
`reset-dr-primary.sh`	Primary node	Reset the Disaster Recovery primary configurations from the primary Disaster Recovery server.
`restart-dr.sh`	Primary and standby nodes	Restart disaster recovery service.
`resume-dr.sh`	Primary node	Resume disaster recovery service after it was paused.
`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 `manage-sannav-configurations.sh` script allows you to perform several actions on the SANnav server without having to run individual scripts.

> **NOTE**
> When you change a switch protocol from HTTP to HTTPS or HTTPS to HTTP, you may have to wait for 30 minutes to perform other operations.

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

```
./manage-sannav-configurations.sh
```

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

1. Check SANnav status.
2. Restart SANnav.
3. Stop SANnav.
4. Start SANnav.
5. Show SANnav configuration.
6. 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 sample output is 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 sample output is 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.

Checking the Availability of Linux User ID and Group ID

The following User IDs and Group IDs must be available on the Linux Operating System for a successful installation. During installation, SANnav creates these users on the Linux Operating System without a login privilege.

Table 19: SANnav Required Linux UIDs and GIDs

UIDs	User Names	Notes
56900/56900	sannavmgr	The UID 56900 is not configurable in SANnav and must be available in the operating system.
1000/1000	sannavstreaming	If UID 1000 is bound to another user (not `sannavstreaming`), whatever the user name UID 1000 is bound to, is used by SANnav.

You must not delete or modify these users. Without these users, the installation prerequisite fails.

Changing the SSL Self-Signed Certificates

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

> **NOTE**
> If the chained CA root certificates file size is more than 13.65 KB telemetry streaming does not work.

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 receive Syslog events from Fabric OS (FOS), ensure that these additional requirements are met:
  - Configure FQDN for the server where SANnav is installed and generate the SSL with CN matching to that FQDN.
  - 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 the 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, and SANnav functions may not work properly.

Setting Up a Web Proxy for Internet Connectivity

SANnav requires an internet connection to perform several licensing operations. If you do not have an Internet connection, you can set up a web proxy by using the `setup-webproxy.sh` script.

For example, SANnav requires an Internet connection in the following cases:

- When the SANnav license expires, SANnav is by default configured to automatically retrieve and activate a renewal license. This automatic renewal process requires an Internet connection.
- In a disaster recovery configuration, 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.

In a disaster recovery configuration, you may need to run the `setup-webproxy.sh` script on both the primary node (for license auto-renewal) and on the standby node (for automatic license rehosting in case of failover). Wait until you complete the standby setup before running this script.

> **NOTE**
> SANnav uses the following external URL:
>
> `https://enterprise.broadcom.com/broadcom/v1/slkserviceweb/`

To set up a web proxy for Internet connectivity, perform the following steps:

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

   ```
   setup-webproxy.sh
   ```

2. 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

Migrating the SANnav Management Portal from one Server to the Other

If you want to migrate the SANnav Management Portal that is installed on Server A to Server B, perform the following steps:

> **NOTE**
> This procedure is applicable only if the MAC address of Server B is different from Server A. If you are modifying the IP address of the server, see Changing the SANnav Server IP Address.

1. Take a backup of the SANnav Management Portal that is installed on Server A and move it to Server B.
2. Rehost a License on a different Server. Planned Migration section for releasing the current SANnav License installed on Server A. This enables you to rehost the SANnav license to Server B later. For detailed information, refer to *SANnav Management Portal User Guide*.
3. Log in to Server B and install the new SANnav Management Portal.

   See Installing SANnav on a Bare Metal or VM for the First Time.
4. After successful installation, change the password on the first login. Log in to the SANnav Management Portal and rehost the license to the new UUID.
5. After successfully rehosting the SANnav license to Server B, restore the backup that is taken in step 1 by running the following command:

   ```
   <install_home>/bin/ backuprestore/restore.sh
   ```

Required Linux Commands

The SANnav installation script uses many commonly available Linux commands. If any of the commands that are used in the script are not available on the SANnav server, the SANnav installation fails.

> **NOTE**
> The `check-sannav-system-requirements.sh` script checks for the availability of these modules.

The Red Hat minimal installation may not have all the required packages, and the missing packages must be added manually. If you want to avoid installing individual packages and modules, build Red Hat as "Server".

The following table lists the required Linux utilities, commands, services, and kernel modules. The table includes the remediation command that you can use if an item is missing and an error is reported.

Table 20: Required Linux Utilities, Commands, Services, or Kernel Modules

Name	Remediation
`auditctl`	`yum install audit audit-libs`
`ip6tables`	`yum install iptables`
`ipcalc`	`yum install ipcalc`
`lsof`	`yum install lsof`
`mkswap`	—
`netstat`	`yum install net-tools`
`openssl`	—
`rngd`	`yum install rng-tools`
`rngd.service`	—
`setfacl`	—
`ssh-keygen`	—
`tar`	`yum install tar`
`nslookup`	`Yum install bind-utils`

ipcalc

The `ipcalc` command is used to validate the IP address of the SANnav server.

Make sure that `ipcalc` is available and is working properly. If the command is working properly, the output looks similar to that shown here:

```
[root@rhel_7 xxxxx]# ipcalc
        ipcalc: ip address expected
        Usage: ipcalc [OPTION...]
        -c, --check Validate IP address for specified address family
        -4, --ipv4 IPv4 address family (default)
        -6, --ipv6 IPv6 address family
        -b, --broadcast Display calculated broadcast address
        -h, --hostname Show hostname determined via DNS
        -m, --netmask Display default netmask for IP (class A, B, or C)
```

```
-n, --network Display network address
-p, --prefix Display network prefix
-s, --silent Don't ever display error messages

Help options:
-?, --help Show this help message
--usage Display brief usage message
[root@rhel_7 xxxxx]#
```

If the command does not work, the output displays "Command not found." To install the command, run `yum install ipcalc`.

iptables

Docker needs `iptables` to create NAT rules for the Docker network. Without `iptables` , Docker cannot start, and SANnav installation fails.

The `iptables-services` is not the same as `iptables` . The behavior of `iptables-services` is different from `iptables` . When `iptables-services` is enabled, it works like a firewall in which the default access is to block all ports.

If `iptables-services` is installed and running, you must manually open the required ports for client and switches on the server.

SANnav does not need `iptables-services` . It is recommended that you stop and disable `iptables-services` to avoid any issues with misconfigured rules. Use the following commands to stop and disable `iptables-services` :

```
systemctl stop iptables.service
systemctl disable iptables.service
```

NOTE
Removing `iptables` is **not recommended** because vulnerabilities are prevented by blocking ports using `iptables` .

Enabling FIPS Mode after SANnav Installation

SANnav supports deployment on RHEL servers with FIPS mode enabled.

The SANnav deployment does not enable FIPS mode as part of the 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:

   ```
   <install_home>/bin/manage-sannav-configurations.sh
   ```

2. Enable FIPS.
3. Restart the host or VM.
4. Restart SANnav, if any service fails to start up after the server restart.
   Again, you can use the SANnav Management Console script.

Changing the SANnav Server IP Address

Changing the IP address of the SANnav server is a **disruptive** operation and requires a full uninstall and reinstall of SANnav.

If you need to change the IP address of the SANnav server, perform the following steps:

1. Take a backup of the SANnav server.

   The backup must be taken from the SANnav user interface. Refer to the section "Backing Up On Demand" in the *Brocade SANnav Management Portal User Guide*.

2. Uninstall SANnav.

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

3. Change the IP address.
4. Install SANnav.

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

5. Restore the backup.

   The backup file must be a .tar.gz file and must have been previously generated from the SANnav user interface.

   ```
   <install_home>/bin/backuprestore/restore.sh <path_to_file>/file.tar.gz
   ```

Upgrading and SSL Certificates

When you upgrade to SANnav 2.3.0x, certificates are migrated from previous releases 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 are migrated and are valid for the remainder of their original validity period. SANnav uses a single set of certificates for both SANnav client-to-server communication and telemetry data streaming.

Revision History

The revision history provides a list of the significant changes in each version of the document.

SANnav-23x-MP-Install-IG100; April 28, 2023

Initial document version.

Documentation Legal Notice

This notice provides copyright and trademark information as well as legal disclaimers.

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

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

BROADCOM®