



# **Brocade® SANnav™ Global View Installation and Upgrade Guide, 2.3.x**

**Installation Guide**  
**April 28, 2023**

# Table of Contents

<b>Introduction.....</b>	<b>3</b>
Supported Hardware and Software.....	3
Contacting Technical Support for Your Brocade® Product.....	4
Document Feedback.....	5
<b>SANnav Global View Installation Overview.....</b>	<b>6</b>
Installing SANnav Global View for the First Time.....	6
Upgrading from Earlier Release of SANnav Global View.....	7
Managing SANnav Global View.....	7
<b>Upgrading from an Earlier Release of SANnav.....</b>	<b>8</b>
Upgrade Paths for SANnav.....	8
<b>Pre-Installation Checks for SANnav Global View.....</b>	<b>9</b>
Installation Prerequisites for SANnav Global View.....	9
Upgrade Prerequisites for SANnav Global View.....	11
System and Server Requirements for SANnav Global View.....	11
Port and Firewall Requirements for SANnav Global View.....	12
Configuring the FirewallD Backend for RHEL 8.4 or 8.6.....	14
<b>Installing SANnav Global View.....</b>	<b>15</b>
SANnav Installation Prompts and Customizations.....	15
<b>Post-Installation for SANnav Global View.....</b>	<b>18</b>
Upgrading the OS with SANnav Installed.....	18
Upgrading from CentOS or RHEL 7.9 with SANnav Global View Installed.....	19
Uninstalling SANnav.....	19
<b>Installation Log File.....</b>	<b>20</b>
<b>Scripts for Managing the SANnav Server.....</b>	<b>21</b>
SANnav Management Console.....	22
Checking the Server Health.....	22
Checking the Availability of Linux User ID and Group ID.....	23
Changing the SSL Self-Signed Certificates.....	23
Migrating the SANnav Management Portal from one Server to the Other.....	23
<b>Required Linux Commands.....</b>	<b>25</b>
<b>Enabling FIPS Mode after SANnav Installation.....</b>	<b>27</b>
<b>Changing the SANnav Server IP Address.....</b>	<b>28</b>
<b>Revision History.....</b>	<b>29</b>
<b>Documentation Legal Notice.....</b>	<b>30</b>

# Introduction

---

This guide contains detailed steps for installing SANnav™ Global View and for upgrading from an earlier version of SANnav.

Within this document, SANnav Global View might also be referred to simply as *SANnav*.

Refer to the following guides for additional information:

- *Brocade SANnav Global View User Guide* describes how to use SANnav Global View to monitor and manage multiple Management Portal instances.
- *Brocade SANnav Management Portal User Guide* describes how to monitor and manage your storage area network (SAN) using Brocade SANnav Management Portal.
- *Brocade SANnav Management Portal Installation and Upgrade Guide* contains detailed steps for installing SANnav Management Portal and for upgrading from an earlier version. The guide also includes information about installing SANnav Management Portal as an Open Virtual Appliance (OVA).
- *Brocade SANnav Global View Release Notes* includes a summary of the new and unsupported features for this release.

## Supported Hardware and Software

SANnav supports Gen 5, Gen 6, and Gen 7 switches and directors.

SANnav Global View 2.3.x supports SANnav Management Portal 2.3.x instances that manage fabrics containing the following Fabric OS software versions and hardware platforms.

### **Fabric OS Software Support**

The following Fabric OS software versions are supported by this release of SANnav:

- Fabric OS 9.0 or later
- Fabric OS 8.2.3d or later

#### **NOTE**

Gen 4 and Gen 5 hardware platforms with Fabric OS (FOS) version 7.4.x or 8.x (other than 8.2.3d) are managed by SANnav, however, customer support is limited.

### **Brocade Gen 7 (64G) Fixed-Port Switches**

- Brocade G720 Switch
- Brocade G730 Switch
- Brocade 7850 Extension Switch

### **Brocade Gen 7 (64G) Directors**

- Brocade X7-4 Director
- Brocade X7-8 Director

**Brocade Gen 6 (32G) Fixed-Port Switches**

- Brocade G610 Switch
- Brocade G620 Switch
- Brocade G630 Switch
- Brocade 7810 Extension Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module

**Brocade Gen 6 (32G) Directors**

- Brocade X6-4 Director
- Brocade X6-8 Director

**Brocade Gen 5 (16G) Fixed-Port Switches**

- Brocade 6505 Switch
- Brocade 6510 Switch
- Brocade 6520 Switch
- Brocade M6505 Blade Server SAN I/O Module
- Brocade 6542 Blade Server SAN I/O Module
- Brocade 6543 Blade Server SAN I/O Module
- Brocade 6545 Blade Server SAN I/O Module
- Brocade 6546 Blade Server SAN I/O Module
- Brocade 6547 Blade Server SAN I/O Module
- Brocade 6548 Blade Server SAN I/O Module
- Brocade 6558 Blade Server SAN I/O Module
- Brocade 7840 Extension Switch

**Brocade Gen 5 (16G) Directors**

- Brocade DCX 8510-4 Director
- Brocade DCX 8510-8 Director

## **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](http://www.broadcom.com/support/fibre-channel-networking/contact-brocade-support).

Online	Telephone
<p>For nonurgent issues, the preferred method is to log on to the Support portal at <a href="http://support.broadcom.com">support.broadcom.com</a>. (You must initially register to gain access to the Support portal.) Once registered, log on and then select <b>Brocade Products</b>. You can now navigate to the following sites:</p> <ul style="list-style-type: none"><li>• <b>Case Management</b></li><li>• <b>Software Downloads</b></li><li>• <b>Licensing</b></li><li>• <b>SAN Reports</b></li><li>• <b>Brocade Support Link</b></li><li>• <b>Training &amp; Education</b></li></ul>	<p>For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at <a href="http://www.broadcom.com/support/fibre-channel-networking/contact-brocade-support">www.broadcom.com/support/fibre-channel-networking/contact-brocade-support</a>.</p>

## 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](mailto: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 Global View Installation Overview

SANnav Global View supports deployment on RHEL servers. If FIPS mode is required, it may be possible to enable FIPS mode on RHEL either before or after SANnav is installed.

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

### NOTE

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

SANnav Global View deployment involves the following processes:

- [Pre-Installation Checks for SANnav Global View](#)

### NOTE

Make sure that you review this section carefully, because the information can change for every release.

- [Installing SANnav Global View](#)
- [Post-Installation for SANnav Global View](#)

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

## Installing SANnav Global View for the First Time

The following table provides the detailed steps for installing SANnav Global View for the first time on a VM or Bare Metal.

1.	Ensure that your server meets the requirements for SANnav installation. Upgrade the OS if you are running an unsupported version.	See <a href="#">SANnav Global View System and Server Requirements</a> .
2.	Review and comply with the installation prerequisites.	See <a href="#">Installation Prerequisites for SANnav Global View</a> .
3.	Ensure that the required ports are open in the firewall.	See <a href="#">Port and Firewall Requirements for SANnav Global View</a> .
4.	If your OS has firewalld running, ensure it meets the SANnav recommended configuration.	See <a href="#">Configuring the Firewalld Backend for RHEL 8.4 or Later</a> .
5.	Install SANnav Global View.	See <a href="#">Installing SANnav Global View</a> .

After the SANnav Global View installation completes, you may need to perform some post-installation tasks (see [Post-Installation for SANnav Global View](#)).

## Upgrading from Earlier Release of SANnav Global View

The following table provides the detailed steps for upgrading from an earlier version of SANnav Global View.

### NOTE

- CentOS and RHEL 7.9 are no longer supported when installing or upgrading SANnav. If your current SANnav Global View is running on CentOS or RHEL 7.9, see [Upgrading from CentOS or RHEL 7.9 with SANnav Global View Installed](#).
- Upgrade to SANnav v2.3.0 requires a valid SANnav license. If the license is expired, you cannot access SANnav after migration until you apply an unexpired license.
- Upgrade from a Trial license is not supported.
- If the current SANnav license is expired, but within the 30 day grace period, you can upgrade to SANnav v2.3.0. However, you must apply a new license to login after the upgrade.
- It is strongly recommended that you back up the current SANnav installation before you start the upgrade process. Refer to the *Brocade SANnav Global View User Guide*.
- It is strongly recommended that you perform support data collection on the current SANnav installation before you start the upgrade process. Refer to the *Brocade SANnav Global View User Guide*.

1.	Ensure that your server meets the requirements for SANnav installation. Upgrade the OS if you are running an unsupported version.	See <a href="#">SANnav Global View v2.3.0 System and Server Requirements</a> .
2.	Review and comply with the installation prerequisites.	See <a href="#">Installation Prerequisites for SANnav Global View</a> .
3.	Ensure that the required ports are open in the firewall.	See <a href="#">Port and Firewall Requirements for SANnav Global View</a> .
4.	Upgrade SANnav Global View.	See <a href="#">Upgrading from an Earlier Release of SANnav</a> .

After the SANnav installation completes, you may need to perform some post-installation tasks (see [Post-Installation for SANnav Global View](#)).

## Managing SANnav Global View

You can use the SANnav Management Console for most day-to-day SANnav Global View operations.

The SANnav installation provides executable scripts that allow you to customize and manage SANnav (see [Scripts for Managing the SANnav Server](#)).

The following lists some of the common tasks you can perform after installing SANnav Global View:

- [Enabling FIPS Mode after SANnav Installation](#)
- [Changing the SANnav Server IP Address](#)

## 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 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.
- User-configured data, customized data, and historical data (such as events) are upgraded. Only the most recent one million events are upgraded.
- The previously discovered portals are rediscovered.

### NOTE

SANnav Global View is compatible only with SANnav Management Portal instances that are running the same version as Global View. Older versions of SANnav Management Portal are not supported. Refer to the SANnav release notes for additional information.

When you upgrade SANnav Global View to a newer version, SANnav Management Portal instances that are running an older version are available in the upgraded Global View; however, the portals are in a disconnected state. Before you can reconnect these portals, you must upgrade them to the same version as SANnav Global View.

### OS Upgrade Options

See [System and Server Requirements for SANnav Global View](#) 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.

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

**Table 1: Supported Upgrade Paths for SANnav Global View**

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



## Pre-Installation Checks for SANnav Global View

This section outlines the steps that you must take before you start SANnav Global View 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 SANnav installation prerequisites.
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 Global View tarball to the installation folder.

The file name is in the format `Global_<version>-distribution.tar.gz`.

4. Untar the .gz file to extract the file to the current location.

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

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

5. (Optional) Check system requirements.

The SANnav installation script checks the system requirements, including port availability. See the following sections for additional information:

- [Port and Firewall Requirements for SANnav Global View](#)
- [System and Server Requirements for SANnav Global View](#)
- [Required Linux Commands](#)

The next step is to install or upgrade SANnav.

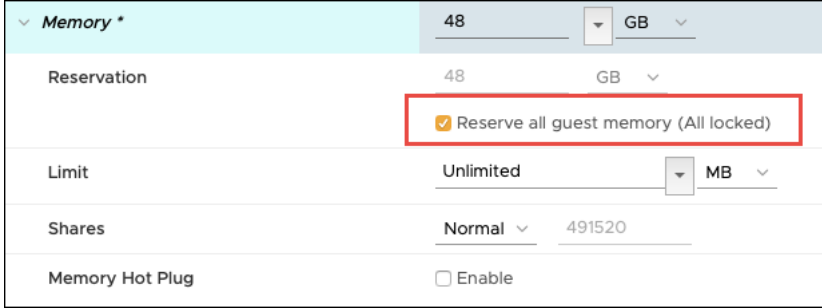
## Installation Prerequisites for SANnav Global View

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

**Table 2: Installation Prerequisites**

Task	Task Details or Additional Information
Gather the necessary information.	Make sure that you have the following information: <ul style="list-style-type: none"> <li>• Root user credentials. You must log in to the SANnav server as the root user or a user with root privilege (sudo).</li> <li>• The SANnav Global View server IP address.</li> </ul>
Uninstall other applications.	SANnav is expected to be installed and run on a dedicated host. If any other application is installed on the host, uninstall it before starting SANnav installation. If you are upgrading SANnav, do not uninstall the current SANnav instance.
Uninstall Docker, if already installed.	The SANnav installation installs Docker. If you have a Docker installed other than the Docker that SANnav installs, you must remove it before starting the installation. During the boot-up of the Linux, an administrator must ensure that the Docker-mounted file system (for example, <code>var/lib/docker</code> ) is mounted successfully before the Docker service is started by the <code>systemd</code> . If this is not performed, it may cause issues for SANnav to recover from unexpected hard or cold server reboots.

Task	Task Details or Additional Information
Ensure that IP network addresses do not conflict with Docker addresses.	<p>SANnav comes with Docker preinstalled. By default, Docker uses an IP address range of 192.168.255.240/28.</p> <p>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 is unreachable.</p> <p>The installation script allows you to change the default Docker address range to a different address range.</p>
Disable SELinux, if it is enabled.	<p>SELinux is not supported. If SELinux is enabled, you must disable it before installing SANnav. To disable SELinux, perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Log in to your server.</li> <li>2. Check the current SELinux status by executing the <code>sestatus</code> command.</li> <li>3. To disable SELinux on RHEL 8.x, open the <code>/etc/selinux/config</code> file in a text editor of your choice and set <code>SELinux</code> to disabled.</li> <li>4. Reboot the Linux server.</li> <li>5. Verify the SELinux status by executing the <code>sestatus</code> and <code>getenforce</code> commands.</li> </ol>
Check operating system requirements.	<ul style="list-style-type: none"> <li>• Ensure that the operating system can be loaded through a bootable disk or through a PXE server.</li> <li>• Ensure that the <code>lsuf</code> and <code>nslookup</code> packages are installed on the operating system machine. If they are not installed, run the following commands to install them:</li> </ul> <pre>yum install lsuf yum install bind-utils</pre>
Ensure these Linux user IDs, group IDs, user names, and group names are available in the OS.	<ul style="list-style-type: none"> <li>• UID:UNAME – 56900:sannavmgr</li> <li>• GID:GNAME – 56900:sannavmgr</li> <li>• UID:UNAME – 1000:sannavstreaming</li> <li>• GID:GNAME – 1000:sannavstreaming</li> </ul> <p>If the ID 56900 is already in use by another user (not sannavmgr), installation fails. See <a href="#">Checking the Availability of Linux User ID and Group ID</a> for more information.</p>
Format the XFS file system.	<p>If you are using XFS as the file system, make sure that you set <code>d_type=true</code> while creating the disk.</p> <p>You can verify the XFS file system format by running the command <code>xfs_info &lt;docker-installation-directory&gt;</code> and verifying that <code>fotype=1</code>. The default Docker installation directory is <code>/var/lib</code>.</p>
Set umask.	<p>The umask for the root user must be set to 0022. Enter the following command to set the umask:</p> <pre>umask 0022</pre> <p>You must set the umask <i>before</i> you unzip the installation files. If you extract the installation files before setting the umask, you must delete the installation folder, run <code>umask 0022</code>, and unzip files again.</p>
Check port 80 availability.	<p>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.</p>
Check additional port requirements.	<p>If your network utilizes a firewall, there may be other ports that must be open. See <a href="#">Port and Firewall Requirements for SANnav Global View</a> for details.</p>

Task	Task Details or Additional Information
Allocate memory in the VM.	<p>(Optional) If you are installing SANnav on a VMware-based virtual machine, select <b>Reserve all guest memory</b> 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.</p> 
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 <b>n/a</b> , SANnav database installation fails.
Start the <code>rngd</code> service.	<p>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.</p> <pre> yum install rng-tools systemctl start rngd.service systemctl enable rngd.service </pre>
Run additional commands.	<ul style="list-style-type: none"> <li>Ensure that the <code>hostname -i</code> command resolves to a single valid IPv4 address.</li> <li>The <code>nslookup</code> command must be successful for the host name of the physical host and VM.</li> <li>Enter the <code>ifconfig</code> command to verify that the MTU size is at least 1500. For example:</li> </ul> <pre> ifconfig eth0: flags=4163&lt;UP,BROADCAST,RUNNING,MULTICAST&gt; 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>

## Upgrade Prerequisites for SANnav Global View

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

- Back up SANnav Global View. After the backup completes, generate a full support data collection (logs and database, with the **Full** option).  
Refer to the *Brocade SANnav Global View User Guide* for instructions.
- Make sure that you have a valid license before starting the upgrade.
- Upgrade from a Trial license is not supported.

## System and Server Requirements for SANnav Global View

Before you start the SANnav Global View installation, you must meet all the system and server requirements.

**NOTE**

- Make sure that you review this section carefully, because the information can change for every release.
- The disk space requirement that is listed in the table is for SANnav Global View only. You must account for the additional space required by the operating system, for saving files, and for the 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 v2.3.0x installation only. Starting in SANnav 2.3.0x, the installation script does not enforce the CPU sockets and CPU speed requirement. If the CPU sockets and CPU speed do not meet the SANnav recommendation, the information is logged and installation continues.  
Failure to meet the recommended number of CPU sockets and CPU speed may lead to performance degradation of the SANnav server.
- Use the latest generation processors for better SANnav performance.

The following table lists the system and server requirements for SANnav Global View.

**Table 3: System and Server Requirements for SANnav Global View Installation**

Requirement	Value
Operating system	Red Hat Enterprise Linux (RHEL): 8.4 and 8.6. Language = English, Locale = US <b>Note:</b> RHEL 9.0 is not supported. Check the SANnav release notes for information about support for other OS versions.
Processor architecture	x86
Host type	<ul style="list-style-type: none"> <li>• Bare metal server</li> <li>• VMware ESXi v7.0</li> <li>• HyperV on Windows Server 2022</li> </ul> SANnav Global View does not support Open Virtual Appliance (OVA) deployment.
CPU	16 cores
Memory (RAM)	32 GB
Hard disk	390 GB, distributed as follows: <ul style="list-style-type: none"> <li>• 300 GB – Installation directory</li> <li>• 90 GB – Docker installation directory</li> </ul> The disk space can be from a direct-attached disk or through a network-mounted disk. However, Docker must be installed on a direct-attached disk.
Minimum number of CPU sockets	2
Minimum CPU speed	2000 MHz

## Port and Firewall Requirements for SANnav Global View

SANnav Global View requires certain ports to be open to ensure proper communication and operation.

### Ports Required for SANnav Global View Installation

SANnav Global View v2.3.0x allows you to input a range of 100 ports (default is 12000 – 12099) for SANnav containers to use. All 100 ports in that range must be free for SANnav to use. The port range cannot be modified after installation.

In addition, SANnav Global View uses the following ports. Ensure that these ports are available before starting SANnav installation or migration.

**Table 4: Ports Required for SANnav Installation**

Port Number	How the Port Is Used in SANnav	What Happens if the Port Is Not Open	Customizable During Installation?
80	Needed for the SANnav proxy to serve the clients.	The SANnav user interface cannot be accessed using HTTP.	No
443	Needed for the SANnav proxy to serve the clients.	The SANnav user interface cannot be accessed.	Yes
2377, 7946	Internal use for Docker.	Installation fails.	No
5432	Internal use for the database.	Installation fails.	No
8080, 11211	Internal use for Ignite.	Installation fails.	No
10800 – 10819	Internal use for Ignite.	Installation fails.	No
47100 – 47119, 47500	Internal use for Ignite.	Installation fails.	No

**Ports That Must Be Open in the Firewall**

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

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

The script lists the required ports that are not open.

The following table lists the ports that must be open in the firewall. In the **Communication Path** column, communication coming in to the SANnav server is inbound. Communication going out from the server to SANnav Management Portals is outbound.

**Table 5: Ports That Must Be Open in the Firewall**

Port Number	Transport	Inbound/ Outbound	Communication Path	Description
80	TCP	Inbound	Client --> Server	HTTP port for access from the browser to the server; for HTTP to HTTPS redirection.
443 If port 443 is not utilized, open its replacement port.	TCP	Both	Inbound: Client --> Server Outbound: Server --> SANnav Management Portal	Inbound: HTTPS port for secure access from the browser to the server. Outbound: HTTPS port for secure access from the server to SANnav Management Portal.

**Ports Required for External Authentication**

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

**Table 6: Ports That the Server Must Be Able to Access**

Port Number	Transport	Inbound/ Outbound	Communication Path	Description
25	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications without SSL or TLS.
49	TCP	Outbound	Server --> TACACS+ Server	TACACS+ server port for authentication if you use TACACS+ for external authentication.
389	TCP	Outbound	Server --> LDAP Server	LDAP server port for authentication if you use LDAP for external authentication and SSL is not enabled.
465	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications with SSL.
587	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications with TLS.
636	TCP	Outbound	Server --> LDAP Server	LDAP server port for authentication if you use LDAP for external authentication and SSL is enabled.
1812	UDP	Outbound	Server --> RADIUS Server	RADIUS server port for authentication if you use RADIUS for external authentication.
3269	TCP	Outbound	Server --> LDAP Global Catalog	LDAP Global Catalog port for authentication if you use LDAP Global Catalog for external authentication. This is the default SSL port.

## 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`.

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 Global View

---

After you have finished the pre-installation checks, complete these steps to install SANnav Global View on the server.

Ensure that your system meets the requirements that are listed in [System and Server Requirements for SANnav Global View](#).

Download and copy the SANnav Global View software package to the server. The package contains the SANnav Global View tarball.

1. Go to the `<install_home>/bin` directory.
2. Run the `install-sannav.sh` script to install SANnav Global View.  
`./install-sannav.sh`

The installation script checks whether an earlier instance of SANnav Global View is installed, and if so, it prompts if you want to exit the installation and take a backup or continue the installation without backing up the server.

3. If you are prompted about migrating SANnav, enter one of the following options.
  - To proceed with migration, press **Enter**. You are prompted to select the auto-detected path or to enter the location of the existing SANnav installation.
  - To exit the installation, press **Ctrl-C**. The script ends. Now you can back up the current SANnav instance and restart the installation script. Or you can uninstall the current SANnav instance and restart the installation script without migrating.
4. Read and respond to each prompt carefully.

## NOTE

Some 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 preinstall requirements test. If any test fails, the installation exits with error messages. You must fix the reported issues and re-run the install script. After the diagnostics pass, installation of SANnav Global View software continues.

On successful installation of the software, the SANnav Global View server starts up. The startup may take up to 10 minutes.

5. Check the SANnav status by running the following script:

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

## NOTE

- After installation, do not modify the file and folder permissions in the SANnav installation directory.
- If you upgraded from a previous version of SANnav, then after the upgrade, 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 7: SANnav Installation Customizations**

Item	Description	Change After Installation?
Start port for the SANnav installation port range	By default, SANnav uses the ports 12000 – 12099 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
Docker installation directory	The default home directory for installing Docker is <code>/var/lib/</code> , but you can change to another directory during installation. Make sure the directory has enough space for SANnav installation.	No
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. <b>NOTE:</b> 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
Port customization	You can customize the client-to-server HTTPS port when installing SANnav. The default HTTPS port is 443. The port must be unused and available. <b>Note:</b> See <a href="#">Port and Firewall Requirements for SANnav Global View</a> for a list of ports that are reserved for internal communication. Do not use any of these ports for customization.	No
Database password	You must provide a password for the SANnav database (Postgres database). There is no default password. <b>Note:</b> Making any changes to the SANnav database manually results in loss of support.	Yes
SANnav security password	This password is used for the enhanced security of SANnav infrastructure service components.	Yes



Item	Description	Change After Installation?
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.	Yes

## Post-Installation for SANnav Global View

---

After the SANnav Global View 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.
- Upgrade the OS with SANnav installed.  
If you upgraded SANnav to an unsupported OS, you may need to change the OS after installation. See [Upgrading the OS with SANnav Installed](#).
- During the boot-up of 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.
- Add the license to the SANnav server.  
If this is a first time installation, you must obtain your Server UID, generate a license, and then add the license to the SANnav server. Refer to the *Licensing* section of the *Brocade SANnav Global View User Guide*.
- Uninstall SANnav and bring the system back to its original state.  
See [Uninstalling SANnav](#).

## Upgrading the OS with SANnav Installed

You can upgrade the OS after SANnav is installed using Yellowdog Updater, Modified (YUM) on the same host where SANnav is running. First, stop the SANnav services, perform the 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 Global View is running on CentOS or RHEL 7.9, see [Upgrading from CentOS or RHEL 7.9 with SANnav Global View Installed](#).
- 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 from CentOS or RHEL 7.9 with SANnav Global View Installed

If your current SANnav Global View instance is running on CentOS or RHEL 7.9, you must upgrade the OS to RHEL 8.4 or 8.6.

Perform the following steps if your current SANnav instance is running on CentOS or RHEL 7.9.

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

Refer to the *Brocade SANnav Global View User Guide* for instructions.

2. Install your current SANnav version on an OS that supports both the current and target SANnav versions.

For example, SANnav v2.2.1, v2.2.2, and v2.3.0 are supported on RHEL 8.4 and 8.6.

See [Installing SANnav Global View](#) for instructions.

### NOTE

If you prefer to retain the IP Address of the SANnav currently installed on CentOS or RHEL 7.9, move the backup files off the current server and shutdown the OS.

3. Restore the backup files to the newly installed SANnav instance.

Refer to the *Brocade SANnav Global View User Guide* for instructions.

4. Rehost the SANnav license from the older server to the new SANnav server.

Refer to the *Brocade SANnav Global View User Guide* for instructions.

5. Upgrade from your current SANnav version to the target SANnav version.

See [Installing SANnav Global View](#) for instructions.

## 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.

## 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
```

## 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.

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 8: SANnav User-Executable Scripts**

Script	Description
<code>add-user-to-sannavmgr-group.sh</code>	Allows a Linux root user or a user with <code>sudo</code> privileges to add another user with <code>sudo</code> privileges to the <code>sannavmgr</code> group.
<code>change-sannav-authentication-to-local.sh</code>	Changes the SANnav authentication from SAML Identity Provider (IdP) to Local Database.
<code>check-sannav-firewall-status.sh</code>	Checks if <code>firewalld</code> is enabled and if the required ports are open.
<code>check-sannav-status.sh</code>	Checks the status of the SANnav server.
<code>install-sannav.sh</code>	Installs the SANnav server. SANnav should not be running when you run this script.
<code>manage-sannav-configurations.sh</code>	Allows you to perform several actions on the SANnav server.
<code>manage-sannav-whitelisting.sh</code>	Creates and manages a list of IP addresses that are allowed SANnav access. Refer to the <i>Brocade SANnav Global View User Guide</i> for details.
<code>merge-files.sh</code>	Merges files previously split by the <code>split-file.sh</code> script.
<code>remove-sannav-audit-rules.sh</code>	Deletes Linux audit rules created by SANnav during the installation. Deleted audit rules cannot be added again.
<code>replace-sannav-certificates.sh</code>	Replaces SSL self-signed certificates with third-party signed certificates.
<code>restart-sannav.sh</code>	Stops the currently running SANnav server and then starts it.
<code>show-sannav-configurations.sh</code>	Displays SANnav port and server configurations.
<code>show-sannav-license-information.sh</code>	Displays the SANnav license serial number and server unique ID (UID).
<code>show-sannav-open-source-software.sh</code>	Displays information about open source software that is used by SANnav.
<code>split-file.sh</code>	Splits a large SANnav support data collection file into smaller files for faster transmission over the network.
<code>start-sannav.sh</code>	Starts the SANnav server after it has been stopped. SANnav should not be running when you run this script.
<code>stop-sannav.sh</code>	Stops the currently running SANnav server.
<code>uninstall-sannav.sh</code>	Uninstalls the SANnav server.

Script	Description
update-reports-purge-settings.sh	Changes the number of days after which reports are automatically deleted.

## 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.

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 13 services are currently down
~~~~~
g-connector
authentication-rbac-middleware
backuprestore-mw
be-consolidated
ignite-grid-object-manager-node
asyncjobscheduler-manager
supportsave-mw
fe-consolidated
kafka
dashboard-middleware
license-mw
asyncjobscheduler-worker
dashboard-summaryprovider
```

**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 9: 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 <code>sannavstreaming</code> ), 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 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.

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.

## 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.  
Refer to the *SANnav Management Portal Installation and Upgrade Guide*.
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.

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 10: Required Linux Utilities, Commands, Services, or Kernel Modules**

Name	Remediation
auditctl	yum install audit audit-libs
firewalld	yum install firewalld
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

### 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 SANnav management server and external authentication servers 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 Global View 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 true
```

## Revision History

---

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

### **SANnav-23x-GV-Install-IG100; April 28, 2023**

Initial document version.

## Documentation Legal Notice

---

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

Copyright © 2023. Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to [www.broadcom.com](http://www.broadcom.com). All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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.

