BROCADE
A Broadcom Company

SANnav™ Management Portal v3.0.1

SANnav Management Portal v3.0.1 Release Notes (Digest Edition)

Version 3 (Digest Edition)

Table of Contents

Chapter 1: Preface

1.1 Contact Technical Support for your Brocade® Product

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	Web/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

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

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

1.2 Related Documentation

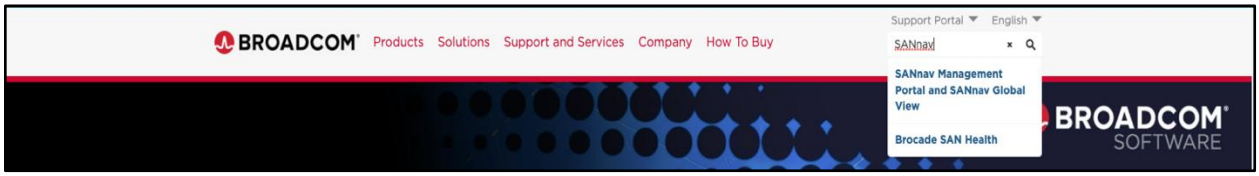
White papers and data sheets are available at www.broadcom.com. Product documentation for all supported releases is available on the support portal to registered users. Registered users can also find release notes on the support portal.

Chapter 2: Locate Product Manuals and Release Notes

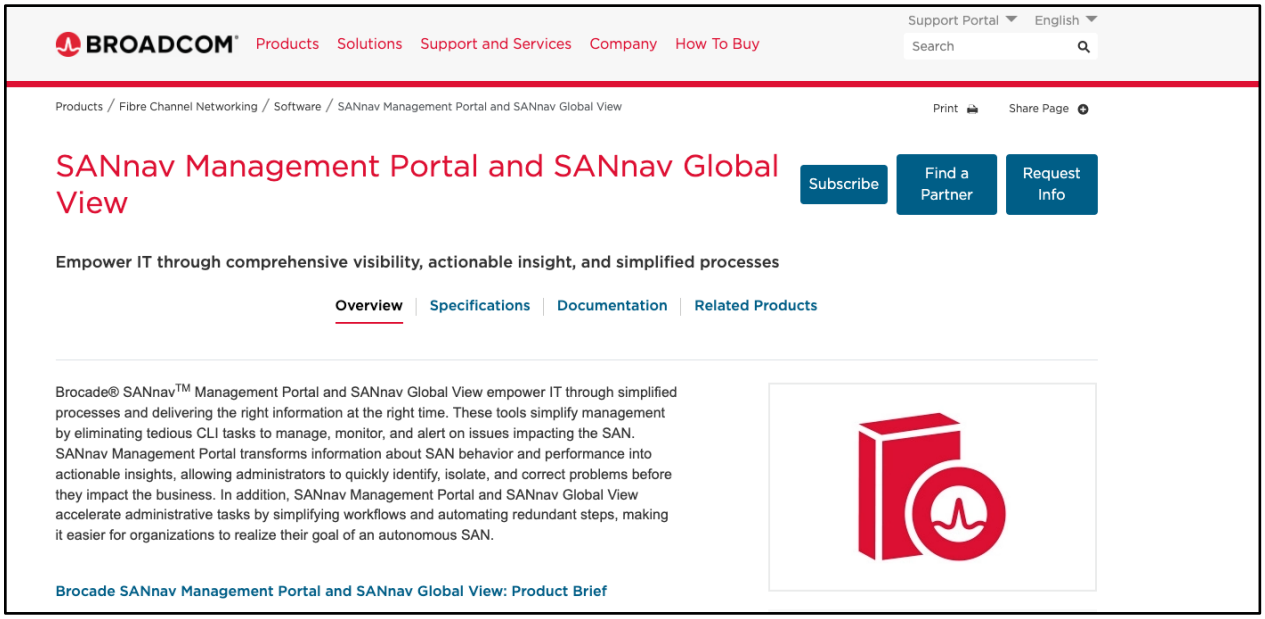
2.1 Locate Product Manuals on Broadcom.com

Complete the following steps to locate product manuals on the Broadcom website:

1. Go to www.broadcom.com, click **Support Portal**, and **Go to Portal** (enter your username and password) or click **Register** if you don't have an account with Broadcom.
2. Enter the product name or the software version number in the **Search** box. For example, the following search is for software and documentation files for *SANnav*.



3. The list of documents will be listed under **Documentation** tab in the search result screen as shown below:



2.2 Locate Product Manuals and Release Notes on the Support Portal

Complete the following steps to locate product manuals on the support portal:

1. Go to support.broadcom.com, click **Login**, and enter your username and password.
2. If you do not have an account, click **Register** to set up your account.
3. Select **Brocade Storage Networking** in the support portal.

ATTENTION Be sure to periodically check for newer versions updates of SANnav Release Notes and User Guide documents.

NOTE In case of conflictual information between the Release Notes and the SANnav User Guide and/or the SANnav Installation Guide, the Release Notes supersedes the SANnav User Guide and/or the SANnav Installation Guide.

2.3 Document Feedback

Quality is our first concern and we have made every effort to ensure the accuracy and completeness of this document. If you find an error, omission, or think that a topic needs further development, we want to hear from you. You can provide feedback by sending an email to documentation.PDL@broadcom.com. Provide the publication title, publication number, and as much detail as possible, including the topic heading and page number, as well as your suggestions for improvement.

Chapter 3: Release Contents

3.1 Brocade SANnav Management Portal v3.0.1 Release Overview

Brocade SANnav Management Portal v3.0.1 is a software maintenance release that supports corresponding Fabric OS (FOS) v10.0.1x firmware. This version includes feature enhancements and defect fixes.

This document highlights the feature enhancements and defects fixes implemented in the SANnav Management Portal v3.0.1 release. Note that this document applies only to the Brocade SANnav Management Portal product. There is a separate Release Notes document for the Brocade SANnav Global View v3.0.1 release.

ATTENTION This document pertains exclusively to the SANnav Management Portal v3.0.1 release. Consequently, customers performing a fresh installation of SANnav v3.0.1 (rather than upgrading from SANnav Management Portal v3.0.0) are strongly advised to consult the latest revision of the SANnav v3.0.0 Management Portal Release Notes document which provides a comprehensive description of the major, fundamental software architecture changes and new features that were initially implemented with the SANnav Management Portal v3.0.0 release.

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

3.2 What's New in SANnav Management Portal v3.0.1

SANnav v3.0.1 provides several software enhancements to existing features and address several defects. The following feature enhancements and notable defects are addressed in various functional areas of SANnav:

- Support new 128G LWL optics hardware
- Support for FOS v10.0.1x enhancements
- SANnav Server deployment and OS support
  - Installation, upgrade, and migration including `sannavcc` enhancements
  - Custom Location for `Authorized_Keys` SSHD file
- Security enhancements
- User Management enhancements (Open LDAP)
- Configuration Policy Management enhancements
- Zoning enhancements
- Inventory enhancements
- Topology enhancements
- Logical Fabric management enhancements
- New REST Interfaces added
- Fault Management enhancements
- Switch Status and Diagnostics feature
- Dashboards enhancements
- Call Home enhancements
- vCenter integration enhancements
- Licensing enhancements (TruFOS, POD and Feature Licenses)
- IANA Time Zone Support
- Usability and UI/UX enhancements

There are features that have been deprecated in SANnav v3.0.1, as well as features that have been obsoleted and removed from the SANnav software. These are also listed in this document.

Supported SAN switches and supported FOS versions, as well as recommendations and guidelines for SANnav and FOS upgrades, are also explained in this document.

NOTE FOS v10.0.1 adds a few enhancements to the SAN Fabric Intelligence (SAN FI) feature. SANnav v3.0.0x or SANnav v3.0.1 do not support this feature or enhancements. There are no external interfaces other than FOS CLI in FOS v10.0.x for external clients to consume this feature.

3.3 What's New in SANnav Management Portal v3.0.0

SANnav v3.0.0 introduces a fundamental software architecture change affecting the entire SANnav software stack. This is one of the main reasons for the increase of the principal version number from SANnav version 2.x to SANnav version 3.x.

The fundamental software architecture change is to replace `docker` with `podman`. This change, along with its implications, will be explained later in the document.

In addition to the architecture change, there are new features as well as multiple feature enhancements and significant user interface (UI) and user experience (UX) changes.

NOTE SANnav v3.0.0 builds on previously released features. It is recommended to consult and refer to the release notes for SANnav v2.4.x and SANnav v2.3.x for what's new in those releases.

The following new features and feature enhancements are provided in various functional areas of SANnav v3.0.0:

- Support Gen 8 hardware platforms, and blades
  - Includes support for FOS v10.0.0x new features and enhancements
- New software architecture where `docker` has been removed and replaced with `podman`
- Server deployment and OS support
- Installation, upgrade, and migration, including disaster recovery
- SANnav Command Center (`sannavcc`)
- SANnav security features
  - Support for SELinux enabled in enforced or permissive mode
  - Support and management of FOS v10.0.0x new security features including quantum-safe cryptography
- Configuration Policy Management (CPM) new features and enhancements
- Switch Configuration Backups enhancements
- Zoning new features and enhancements
- Health Summary Dashboard - Entity Profiles (new)
- Host or Storage Troubleshooting context (new)
- Fault management enhancements
- Webhooks – Service Now Integration (new)
- Troubleshooting Context (new)
- Discovery enhancements
- User Management enhancements
- External REST Interfaces (new)
- Flow Management enhancements
- Inventory enhancements
- Logical Fabrics enhancements
- Extension Tunnels and Circuits enhancements
- Topology enhancements
- Usability and UI/UX enhancements

There are features that have been deprecated in SANnav v3.0.0, as well as features that have been obsoleted and removed from the SANnav software. These are also listed in this document.

Supported SAN switches and supported FOS versions, as well as recommendations and guidelines for SANnav and FOS upgrades, are also explained in this document.

NOTE FOS v10.0.0 introduces a new feature named SAN Fabric Intelligence (SAN FI). SANnav v3.0.0 does not support this feature. There are no external interfaces other than FOS CLI in FOS v10.0.0 for external clients to consume this feature.

3.4 New Hardware Platforms Supported in SANnav Management Portal v3.0.x

SANnav Management Portal v3.0.1 adds support for the following hardware:

- 128G LWL Optics: Long Wavelength 128G Gen8 Optics (FC)
- SR-4 100G Optics (for USF and IP Storage)

SANnav Management Portal v3.0.0 added support for the following **new Gen 8 hardware platforms**:

- X8-8: new Gen 8 8-slot chassis
- X8-4: new Gen 8 4-slot chassis
- G820: new Gen 8 mid-range switch
- G748: 64G FC embedded switch

3.5 New Blades Supported in SANnav Management Portal v3.0.x

There are no new blades added with SANnav Management Portal v3.0.1.

The following **new Gen 8 blade platforms** have been added in SANnav Management Portal v3.0.0:

- FC128-48: 48-port blade
- CR128-8: 8-slot core routing blade
- CR128-4: 4-slot core routing blade
- ICL8-8: 8-slot ICL port blade
- ICL8-4: 4-slot ICL port blade

3.6 SANnav Management Portal Server Deployment and OS Support

3.6.1 SANnav Management Portal v3.0.1 OVA Support

SANnav v3.0.1 continues to support deploying SANnav Management Portal as an Open Virtual Appliance (OVA).

SANnav v3.0.1 OVA now packages the following:

- Rocky Linux 9.7

NOTE Deployment of the OVA file is officially supported on vCenter 9.x (and associated ESXi 9.x versions). Extraction of the SANnav OVA image using vCenter 8.x (and associated ESXi 8.x versions) *should* work but has **not** been tested or qualified with SANnav v3.0.x. vCenter 7.x and ESXi 7.x has not been tested and is not supported.

- OVA is currently available only for SANnav Management Portal and **not** for SANnav Global View.
- Upgrade from SANnav v3.0.0 to SANnav v3.0.1 on OVA deployments can be performed *inline*.

NOTE Make sure to strictly follow the *SANnav MP Installation and Upgrade Guide* before attempting the upgrade and migration from SANnav MP v3.0.0x OVA to SANnav MP v3.0.1 OVA.

3.6.1.1 First Time Installation of SANnav v3.0.1 OVA

The procedure to perform a first time installation of SANnav v3.0.1 in OVA deployment at a high level consists of first downloading the SANnav v3.0.1 OVA tar file `Portal_3.0.1_installer-distribution.ova` from the Broadcom BSN Customer Support Portal or the OEM Assist Site, extracting it and following the prompts for installing SANnav v3.0.1 code image.

ATTENTION With SANnav v3.0.1, SELinux is automatically enabled and set to Enforced mode by default on first time installation of SANnav v3.0.1 OVA. This is because the Rocky 9.7 OS included in the OVA tar file already is set to enabled and enforce SE Linux. Note that this was not the case with SANnav v3.0.0 in where SE Linux was not enabled or set to enforced.

3.6.1.2 OVA Inline Upgrade from SANnav v3.0.0/v3.0.0.1 to SANnav v3.0.1

SANnav v3.0.1 tar file `Portal_3.0.1_installer-distribution.tar.gz` must be downloaded from the Broadcom BSN Customer Support Portal or the OEM Assist Site in case of upgrade.

ATTENTION For inline upgrade from SANnav v3.0.0/v3.0.0.1 to SANnav v3.0.1 the OS (Rocky) must be upgraded first. To do so, the file `sannav_ova_9x_os_03_2026.tar.gz` and associated Release Notes file `sannav_ova_9x_os_03_2026-RN-v2.pdf` must be downloaded from the Broadcom Customer Support Portal or OEM Assist site and installed **before** proceding to the SANnav upgrade.

ATTENTION The file `Portal_3.0.1_installer-distribution.ova` is **not** needed to upgrade to SANnav v3.0.1 (no need to downbload it for upgrade to SANnav v3.0.1).

ATTENTION Ensure to first run the pre-requesites as **`root`** user before you attempt to upgrade to SANnav v3.0.1. To do so, login as **`root`** user then extract the tar file `Portal_3.0.1_installer-distribution.tar.gz` and then follow the procedure in the Install and Upgrade Guide to install the pre-requesites. Note that this step is not required for the first time installation of SANnav v3.0.1 OVA.

NOTE The OS packaged in the OS tar file (see next section) does not enable or enforce SELinux.

After successful upgrade, SELinux should be enabled and set to Enforced by a user with `root` or `sudo` privileges. It is strongly recommended to not disable SELinux or to set it to Permissive mode after installation or upgrade.

NOTE After fully completing the upgrade process to SANnav v3.0.1, and in order to get the latest Rocky OS CVE updates and fixes, it is recommended to upgrade the Rocky OS to the latest Rocky version (Rocky 9.8) by downloading the OS file located under the **SANnav v3.0.0a** repository in CSP/eCX or OEM Assist Site named `sannav_ova_9x_os_06_2026.tar.gz` and associated Release Notes file `sannav_ova_9x_os_06_2026-RN-v1.pdf`.

3.6.1.3 OVA and Rocky Linux CVEs New Process

While Brocade ensures that Rocky Linux CVEs on the OS are addressed at the release of the SANnav v3.0.x software, it is possible that some specific Rocky Linux 9.x CVEs are found and disclosed after SANnav v3.0.1 has been released and before a patch on SANnav v3.0.1 is issued.

A process is in place to allow customers that deploy SANnav in OVA to upgrade the OS to the latest patch containing the latest security vulnerabilities.

3.6.1.3.1 Example Use Case

To illustrate the process with an example, consider the following:

- SANnav v3.0.1 was GA by Brocade on March 26, 2026. It packages the latest Rocky Linux version 9.7 available.
- Assume a new Rocky Linux patch release with critical CVE fixes is available in the future, say sometime in December 2026 on Rocky 9.9.
- The Broadcom Customer Support Portal (eCX) as well as all the OEM Assist Sites will now publish a new entry in the software download list page containing these two entries:
  - `sannav_ova_9x_os_12_2026.tar.gz` - This is the actual OS image containing the December OS security vulnerabilities fixes.
  - `sannav_ova_9x_os_12_2026-RN-v1.pdf` - A document with information on how to install this OS patch on the SANnav server.
- A customer that has previously installed SANnav v3.0.1 may now access the website to download the `sannav_ova_9x_os_12_2026.tar.gz` file and install it on the current SANnav v3.0.1 server by following the instructions in the `sannav_ova_9x_os_12_2026-RN-v1.pdf` file.

3.6.2 SANnav Management Portal v3.0.1 VM/BM Support

SANnav Management Portal v3.0.1 is fully qualified and tested with the following versions of RHEL:

- RHEL release 9.7

NOTE When installing SANnav v3.0.1 on a non-qualified OS version (for example RHEL 9.6 or RHEL 9.8), the installation script displays a warning message indicating that the SANnav Management Portal installation will proceed on an untested and non-qualified OS version. Explicit end user acceptance is required for SANnav Management Portal installation to proceed.

NOTE Non-qualified OS versions will be treated as supported OS versions unless it is identified by Brocade Support that the support issue is due to incompatibility between the SANnav version and the installed OS version.

For both Rocky and RHEL OS, the following must be set in the OS on which SANnav Management Portal server is installed:

- Language = English
- Locale = US

Other languages and locales are not supported.

3.6.3 Other Installation and Deployment Features

3.6.3.1 UID/GID 56900 (`sannavmgr`) customization

With SANnav v3.0.x, the UID/GID for user `sannavmgr` (default UID/GID 56900) can be customized to any valid Linux UID/GID in the range defined in `/etc/login.def` during first time installation for all SANnav MP and GV deployments. The UID or the GID can be customized by changing the values `(UID_MIN, UID_MAX, GID_MIN, GID_MAX)`, however, the username `sannavmgr` cannot be customized.

NOTE Since UID/GID for `sannavmgr` cannot be customized post SANnav installation or during upgrade and migration, customers upgrading from previous releases of SANnav and who must configure the default UID/GID to another value must follow the procedure described in the *SANnav Management Portal Installation and Upgrade Guide*.

3.6.3.2 Disk Usage Warnings

SANnav v3.0.x notifies users when 70% or above of the allocated disk space is full. These alerts can be seen in the SANnav Events view and the Notification Panel.

With SANnav v3.0.x, the disk usage may be checked by the SAN administrator using `sannavcc`. This allows the user to find the largest size files or folders (sorted by size) in the installation folder. The user can then free up space by removing unwanted files. See the *SANnav Command Center* section of this document.

3.6.3.3 `umask` Setting

SANnav versions prior to SANnav v3.0.x required Linux parameter `umask` set to 022. With SANnav v3.0.x, there is no longer a check for the `umask` setting.

The best practice for `umask` setting is 027. Any value of `umask` more restrictive than 027 (e.g. 077) is not supported for SANnav v3.0.1 installation or upgrade in any deployment (VM/BM/OVA).

ATTENTION The below only applies to first time installation and not upgrade. If umask is set to 027, and the ssh key folder location is customized, a `root/sudo` user must make an exception for `sannavmgr` user to use the Linux standard default ssh key path by following the procedure below:

1. **Edit the SSH Daemon configuration file**

   - Open the SSH configuration file using a standard Linux editor like `nano` or `vi`
     - For example: `sudo nano /etc/ssh/sshd_config`

2. Set the Override for `sannavmgr` user

- Scroll to the very bottom of the file and add the `Match` block as shown below. For example, it should look like this:

```
# Override strictly for sannavmgr (must be at the bottom of the file)

Match User sannavmgr
AuthorizedKeysFile %h/.ssh/authorized_keys
```

3.7 First-Time Installation, Upgrade, and Disaster Recovery Changes

3.7.1 SANnav v3.0.1 Installation/Upgrade

The first-time installation of SANnav v3.0.1 is still a two-step process as was the case in SANnav v3.0.0. An initial step requiring a privileged user (`root/sudo`) to set prerequisite configurations (via Linux commands) and to create an unprivileged user called `sannavmgr`, followed by the actual installation performed by the unprivileged user `sannavmgr`.

A handoff between these two steps may be necessary. The first step may be carried out by the customer's IT department, who procure and configure the SANnav server to meet the hardware specifications and execute commands requiring privileged access. Subsequently, the server is transitioned to the SAN administrator for the second step. Note that for SANnav v3.0.0 and later, the installation or upgrade procedures do not require `root/sudo` access. It is highly recommended that the installation upgrade be performed by `sannavmgr` user.

In some instances, the SAN administrator may also be the `root/sudo` user in which case there is no handoff. In this case, it is important to make sure that the SAN Administrator performs the first step with `root/sudo` privileges and the second step as the `sannavmgr` user. Failure to do so will result in errors or issues later.

SANnav v3.0.0 required two files to be downloaded separately. The first file was named `Portal_3.0.0_rootuser-distribution.tar.gz` was required for installing the prerequisites configurations. The second file was named `Portal_3.0.0_installer-distribution.tar.gz`. and contained the actual SANnav code image.

With SANnav v3.0.1, only one tar file called `Portal_3.0.1_installer-distribution.tar.gz` is required to be downloaded from the Broadcom BSN customer support portal or the OEM Assist Site. This file contains both the prerequisites' configurations as well as the SANnav code image.

NOTE Make sure to strictly follow the *SANnav MP Installation and Upgrade Guide* before attempting the installation of, or the upgrade and migration to, SANnav MP v3.0.1.

3.7.2 Installation/Upgrade and Disaster Recovery Changes

Setting up disaster recovery (DR) involves the same two-step process described earlier in this section: a privileged user must first set up the standby server and install all prerequisite packages, followed by the SANnav v3.0.1 software installation or upgrade by the unprivileged `sannavmgr` user.

NOTE DR configurations are not migrated from the previous release when upgrading SANnav to SANnav v3.0.1. DR must be reconfigured again after successful upgrade to SANnav v3.0.1.

Refer to the *SANnav Management Portal Installation Guide* for detailed steps to set up DR with SANnav v3.0.1.

3.8 SANnav Command Center (`sannavcc`)

To install, upgrade, configure, manage, and troubleshoot the SANnav server, a new paradigm called SANnav Command Center (SCC) was introduced with SANnav v3.0.0. There are no longer any Linux shell script invocations with SANnav v3.0.x.

All previous release functionality provided via bash shell script execution has now been folded into the SCC which, when executed, launches a console ASCII menu with various options allowing users to invoke functions to install, upgrade, configure, manage, and troubleshoot the SANnav server. All previous script functions are now replaced with the new `sannavcc` command with special arguments as detailed below.

In SANnav v3.0.0, the command `sannavcc` was to be executed with arguments `"--system-admin", "--sannav-admin"` or `"--sannav-user".`

With SANnav v3.0.1, this has been simplified and no additional arguments are required to the `sannavcc` command, they are automatically determined based on the user who executes the command.

Refer to the *SANnav Management Portal v3.0.x Installation and Upgrade Guide* for additional details on the enhancements implemented in SANnav v3.0.1 (on top of existing SANnav v3.0.0 functionality) for the `sannavcc` command.

3.9 SANnav Security

3.9.1 SANnav Code Signing with Quantum-Safe Cryptography

SANnav v3.0.1 code images include an LMS quantum-safe code signing hash code. A special executable is provided along with the code software artifacts (code image) to verify the authenticity of the code image. In the OEM Assist website as well as in the Broadcom Customer Support Portal, a new zipped tar file will be available as explained below:

- `SANnav-<version>-code-verification.tar.gz` contains the following files after extraction:
  - `verify-sananv-code.sh`: the script to be used to verify SANnav images
  - `readme`: the usage
  - `bin/lms-util`: the binary that verifies code
  - `lms_key.pub`: the public key
  - `sig`: directory that contains the code signatures of the SANnav products

To verify the authenticity of the SANnav code image, run the following:

- `./verify-sannav-code.sh -f|--file <sannav-code-to-verify>`

If the SANnav code image is authentic, the script output will be `Signature verified.` If not, `Signature NOT verified` will be output.

NOTE The package name to verify the SANnav v3.0.0 code was named `SANnav-code-verification.tar.gz.` Make sure to use the new package `SANnav-<version>-code-verification.tar.gz` to verify SANnav v3.0.1 code.

NOTE In the case of OVA, make sure to download the file `SANnav-<version>-code-verification.tar.gz` either on Linux as the extracted script `verify-sannav-code.sh` will not run on Windows OS or MacOS.

3.9.2 IP Tables Replaced with NF Tables

In RHEL versions 9.x, the use of IP tables has been deprecated and NF tables are recommended as an alternative. With SANnav v3.0.0, all IP tables have been replaced with NF tables. The NF tables are persistent (unlike IP tables) in SANnav, meaning they will survive a server reboot.

3.9.3 Stronger Password Security Rules

Starting with SANnav v3.0.0, for the following four passwords that are entered during SANnav installation, new password rules are now enforced to comply with security requirements. The four passwords are:

1. SANnav Security password
2. SANnav Database password
3. SNMP password (Auth and Priv)
4. SFTP/SCP password

NOTE This section does not apply to the SANnav user login passwords.

The four passwords must follow these rules:

- Contain at least 12 characters
- Contain at least 3 of the following categories:
  - Lower-case letters
  - Upper-case letters
  - Digits
  - Only the following special characters (spaces not allowed) !#.$*()

3.9.4 SSH Related Changes (OVA)

Prior to SANnav v3.0.x the SANnav OVA image had the SSH TCP port forwarding enabled. `AllowTcpForwarding`, `AllowAgentForwarding`, and `X11Forwarding` were enabled by default.

The following two changes have been implemented for SANnav v3.0.x OVA image deployments:

1. SSH TCP port forwarding has been disabled; `AllowTcpForwarding`, `AllowAgentForwarding`, and `X11Forwarding` are disabled by default.
2. SSH configuration files and SSH private keys files will have permissions set to 600.

3.9.5 Support for SELinux Enabled in Enforced or Permissive Mode

SANnav MP v3.0.x supports running SANnav software on a Linux platform with SELinux enabled in either Permissive or Enforced modes.

- Managing SELinux on a Linux VM/BM server must be performed by a privileged user.
- For the first-time installation, SELinux may be enabled (permissive or enforced modes) before or after the installation.
- For upgrade to SANnav v3.0.x, SELinux may be enabled (permissive or enforced modes) only after a successful upgrade.
- With SANnav v3.0.1, SELinux is enabled and set to Enforced in OVA deployments. It is recommended to not change this setting.
- Only the targeted SELinux policy is supported by SANnav v3.0.x.

- There are required packages for enabling SELinux on the SANnav server. These are:
  - selinux-policy-targeted
  - libselinux-utils
  - policycoreutils
  - policycoreutils-python-utils
  - container-selinux
  - Optional recommended package for troubleshooting: setools-console
- Run `rpm -q <package-name>` to check for existence of any of the above packages, and run `yum install <package-name>` to install any missing package. These commands must be run by a Linux privileged user (`root/sudo`).

NOTE Installing SANnav on an external storage device other than the one originally provisioned during the VM creation (by the IT department administrator) is not supported when SELinux is enabled (for example adding an external storage to `/mnt` is not supported).

3.9.5.1 Custom Location for `Authorized_Keys` SSHD file

With SANnav v3.0.0, the installation process assumed that the SSH keys location for a given user lived in the default and standard Linux file located by default under `(~/.ssh/authorized_keys)` irrespective of the property `AuthorizedKeysFile` configured in the `sshd` configuration standard file `/etc/ssh/sshd_config`. In other words, SANnav v3.0.0 did not consider this configuration file.

With SANnav v3.0.1, the installation process determines the location of the ssh keys from the property `AuthorizedKeysFile` value which is set in the `sshd` configuration file `/etc/ssh/sshd_config`. If the location of the ssh keys is set to a custom location (for example and most commonly `/etc/ssh_keys/%u` , where `%u` is replaced by the username at runtime) then this custom location is used when creating the `sannavmgr` user and for the rest of the SANnav installation process.

3.10 Feature Enhancements

3.10.1 User Management enhancements (Open LDAP)

SANnav users can now be authenticated via a server supporting Open LDAP protocol with SANnav v3.0.1. This is in addition to the already supported user authentication via AD LDAP and CA LDAP.

3.10.2 FOS Firmware Image Import Enhancements

FOS versions v10.0.x support firmware image files verified against a new SHA-512 checksum. MD5 continues to be supported for FOS versions lower than FOS 10.0.x.

SANnav v3.0.1 allows to import a new SHA-512 checksum file when importing FOS v10.0.1 firmware images in the SANnav Firmware Repository and continues to support importing MD5 checksums for FOS versions lower than 10.0.x.

Configuration Policy Management

The enhancements below have been added to the SANnav v3.0.1 Configuration Policy Management feature.

- Provide for bulk Export of SANnav Configuration and MAPS blocks. This is to address the use case where a user needs to Export Blocks from one SANnav instance and Import them in another SANnav instance.
- Progress indication when drifts are being checked on demand. A progress indication showing <*4/20 switches*> in the **Drift Status** column of CPM list view has been added to indicate that the drift check has been executed 4 switches out of a total of 20 switches associated with the policy.
- The existing progress indication when performing Bulk Switch Backup(s) or Restore has been enhanced to show similar information as for drift computation, that is 4/20 will indicate that the operation has been completed for 4 switches out of a total of 20 selected.
- Support FOS v10.0.1 MAPS RoR increase to 100
- Usability enhancement – when **Pushing** or **Syncing** a policy with multiple Config blocks and/or MAPS blocks modified a detailed confirmation window will be shown with additional enhancements compared to previous releases as follows:
  - Configuration blocks that were skipped due to blocks being marked as **Monitor Only** or not supported on FOS version running on the switch or the switch model
  - MAPS Rules which were skipped due to the fact that they are not supported on FOS version running on the switch or the switch model
  - MAPS rules which were Pushed or Synced with modification of the Action list due to the fact that the specified actions are not supported on FOS version running on the switch or the switch model
- When a Policy is cloned using the "Save As" workflow, the list of associated switches is now retained upon user confirmation (the list of associated switches was empty, that is not cloned, prior to SANnav v3.0.1)

3.10.3 Zoning Enhancements

The enhancements below have been added to the SANnav v3.0.1 Zoning feature.

- Option to automatically export snapshots to a **network mounted storage** when scheduling them (snapshot exported as a .zip file)
- Added 5 new columns to Zone Inventory:
  - Connected Switch,
  - Connected Switch IP Address,
  - Connected Switch FID
  - Offline Date Time (date and time at which the device port went offline)
  - Online Date Time (date and time at which the device port went online)

3.11 Inventory Enhancements

The enhancements below have been added to the SANnav v3.0.1 Inventory feature.

- A new column **Licensed Port Count** has been added in the Switch Inventory List View to indicate the total number of licensed ports (POD) on a switch (Logical Switch). Note the following:
  - This new Licensed Port Count column has also been added to the Switch report template as a non-default column.
  - The Port Count column in the Logical Switches table on the Chassis Details page was previously displaying an incorrect value (Managed Port Count). This issue has been corrected in this release, and now displays the correct port count.

- A new **Supported Speeds** (Gb/s) column has been added to the Inventory of switch ports. For example, a value of 8, 16, 32, 64 ,128 (always listed in ascending speeds) indicates that the port is capable of supporting any of the speeds (in Gb/s) in the list.
  - This new attribute has also been added to Switch Inventory detailed views, Switch Port properties popup, Switch Port Reports, and associated REST interface responses.
  - After upgrade and migration, this new column will appear after the column Speed
- A new column **Speed (Gb/s)** has been added in the ISL Trunks List view to show the aggregate value of all links speeds. For example, for a Trunk containing 4 individual links each running at 64 Gb/s, this new Trunk Speed column will display 256 Gb/s.
  - When invoking Show Link on a Trunk, the detailed table shown now contains for each link (row) the Switch (1) Speed and Switch (1) Supported Speed and Switch (2) Speed and Switch (2) Supported Speed
  - When viewing the Properties of the Trunk, the Speed and Supported Speeds of each Master Port of each end Trunk are also displayed as Switch (1) Speed and Switch (1) Supported Speeds and Switch (2) Speed and Switch (2) Supported Speeds.
- A new column **State** has been added to the Inventory Chassis views to indicate the state of a chassis (Enabled/Disabled).
  - The chassis state transitions to Disabled, when all the Logical Switches (LS) in the chassis have been disabled. The state transitions back to Enabled, when any one of the LS in the chassis transitions to Enabled.
- The column named **Backbone to Edge Routing** has been renamed to **FCR** in the Chassis Inventory views. The values for this column (Enabled or Disabled) remain unchanged.
- The column **Port Type** (Values Physical/Virtual-NPIV) in the Host Port and the Storage Port Inventory views is now searchable and filterable.
- Two new columns, **Online Date Time** and **Offline Date Time** have been added to the SANnav inventory views of Host Ports and Storage Ports (list and detailed views) to indicate when the device port has gone online and offline respectively. The date and time shown is that of the SANnav server since FOS does not record the device login/logout time.

3.11.1.1 Important Note for FICON Inventory (RNID Sequence Number)

When SANnav discovers multiple virtual switches on a chassis, the *FICON RNID sequence number* displayed is from the *last* discovered virtual switch, which may be incorrect in the **SANnav > Logical Fabrics > FICON Fabrics** table and the **Inventory Switch** detailed view. (Note: **RNID Sequence Number** and **Sequence #** are the same attribute).

To get the correct sequence number, use **Inventory > Switches > Run Cli Commands** to issue `ficonshow switchrnid` or use Webtools.

NOTE The **Sequence #** shown on the Chassis Inventory pages is incorrect and should be ignored, as the *FICON RNID sequence number* is a logical switch attribute. This will be removed in a future SANnav release.

3.11.2 Topology Enhancements

The enhancements below have been added to the SANnav v3.0.1 Topology feature.

With SANnav v3.0.1, the newly added attribute in the Inventory **Supported Speed (Gb/s)** has been added in all Topology associated views and Properties wherever applicable.

When viewing a Zoning context, a limit of 20 Zones maximum has been implemented to avoid unnecessary cluttering of the Topology and to avoid and prevent performance and scale issues.

3.11.3 Logical Fabrics Management Enhancements

With SANnav v3.0.1 a usability enhancement has been implemented for logical fabrics creation or modification, specifically in the port movement phase where FC ports need to be moved from any switch to the target logical switch.

When creating a Logical Fabric an important step in the workflow is to perform the port assignment to the target Logical Switches.

For QSFP/OSFP ports specifically (4/8 SFP ports respectively), when deciding which QSFP/OSFP ports to move from the base switch (or another Logical Switch) to the target logical switches, all 4/8 ports must be moved as a unit simultaneously (even if the ports are on blades in different slots).

To help the user properly select the (4/8) required ports, two new columns have added:

- **Form Factor** with values *SFP, OSFP, QSFP28, etc. or Not Present*
- **Unit #** with value *2, 4, 8,* etc*. or – (when unknown)*

Selecting a partial port subset will cause SANnav to throw an error if the SFPs are plugged in; that is, if **Form Factor** value is not (*Not Present)* and **Unit #** value is not (-).

3.11.4 New REST Interfaces

The following new REST interfaces have been introduced with SANnav v3.0.1:

- Retrieve current Active SANnav Serial Number `(GET /external-api/v1/license/active/)`
- Change passwords for one or more local SANnav users. (`PUT /external-api/v1/usermgmt/users/credentials`)
  - Input parameters - List of (username, new password)
  - This API targets users authenticated against the SANnav Local Database (not SAML or LDAP or any external authentication method). This API includes modification of the SANnav Administrator user password. Note that the password is encrypted over the wire due to TLS encryption used in the REST call. The supplied password must follow the SANnav user password policy defined in SANnav.
  - **NOTE:** For customers using CyberArk to rotate the SANnav Administrator user (or any other locally authenticated by SANnav user) password periodically, a script (`change-user-password.sh`) existed in previous SANnav releases (up to SANnav v3.0.0) to achieve this with CyberArk invoking this script via SSH. With SANnav v3.0.1, these customers should plan to use this new REST interface instead of the script (`change-user-password.sh`).
- Change passwords for one or more local chassis (`PUT /external-api/v1/inventory/chassis/credentials/`)
  - Input parameters - List of (chassis IP address, username, new password)
  - This REST interface operates in a similar way as the User Interface under SANnav > Security > Chassis Password Management to achieve the same functions
  - **NOTE:** This interface is only applicable for chassis running FOS versions v9.1.1x or higher (user will get an error)
  - **NOTE:** Only **non-default** `maintenance` and `admin` passwords may be changed through this REST API. For a factory default switch, CLI must be used to first change the password for these two FOS user accounts before using this REST API to change their passwords
- Retrieve the Zone DB snapshot for a given Fabric `(GET /external-api/v1/zoning/snapshots/)`
  - Input parameters - Fabric Name

3.11.4.1 Modified REST Interfaces

The following REST Interfaces have been modified or refactored:

- GET: /external-api/v1/inventory/chassis/
- GET: /external-api/v1/inventory/switches/
- GET: /external-api/v1/inventory/deviceports/
- GET: /external-api/v1/inventory/switchports/
- GET: /external-api/v1/inventory/fabrics/
- GET: /external-api/v1/inventory/enclosures

For these interfaces, the following has been implemented in SANnav v3.0.1:

- New fields have been added or removed to/from the JSON response
- Some fields have been updated with appropriate data
- Some fields have been updated in the YAML description and user documentation

3.11.5 Fault Management Enhancements

The enhancements below have been added to the SANnav v3.0.1 Fault Management feature.

3.11.5.1 SNMP Forwarding Credentials

- Added **Auth Protocol** value HMAC_SHA_512
- Deprecated **Auth Protocol** values HMAC_MD5 and HMAC_SHA
- Deprecated **Priv Protocol** values CBC_DES & CFB_AES_128
- Removed **Auth Protocol** value NONE
- Removed **Priv Protocol** value NONE

NOTE If the value **NONE** has been used for Auth Protocol or Priv Protocol for SNMP Forwarding credentials in the previous SANnav version (i.e., SANnav v3.0.0.x), then during the upgrade process to SANnav v3.0.1 the user will be prompted to either accept to clear the current SNMP forwarding credentials and re-enter them later or to cancel the upgrade process.

3.11.5.2 Violations List View and Detailed View

- Added column **Fabric** in Violations View
- Added new operation **Show in Topology** for violations that pertain to Switch or Switch Port

- Alarms List View and Detailed View
  - Changed column **Switch** to **Source Name**
  - Changed column **Switch IP** to **Source Address**
  - Added new operation **Show in Topology** for alarms that pertain to Switch or Switch Port
- Event Action Filters new UI design
  - To enhance the usability of the Event Action Policy, the UI for each of these now includes a separate **Exclude from results** check box in the filter section which includes **Message ID** and **Description** fields with an option to **Match Any (OR)** or **Match ALL (AND)**. Both **MessageID** and **Description** fields support comma separated strings to specify multiple values.
  - This allows users to construct filtering criteria such:
    - Include all events with **Severity** of either *Critical* or *Major* but exclude them if **Message ID** is either *EM-1004* ***OR*** *MS-1009"*

3.11.5.3 Violations Action Filters New UI design

- To enhance the usability of the Violations Action Policy the UI for each of these now includes a separate **Exclude from results** check box in the filter section which includes **Measure**, **Rule Name** and **Entity Name** fields with an option to **Match Any (OR)** or **Match ALL (AND)**. All criteria **Measure, Rule Name** and **Entity Name** fields support comma separated strings to specify multiple values.
- This allows users to construct filtering criteria such:
  - Include all violations except those with **Measure** of *TX ,RX* and **Rule Name** contains the string *FPI_3*

3.11.6 SANnav Event Action Filters New UI design

- To enhance the usability of the SANnav Event Action Policy the UI for each of these now includes a separate **Exclude from results** check box in the filter section which includes **MessageID** , **Description, Entity Name, and Entity Address** fields with an option to **Match Any (OR)** or **Match ALL (AND)**. All criteria **MessageID, Description** and **Entity Name** fields support comma separated strings to specify multiple values.

During the upgrade and migration to SANnav v3.0.1, any existing Switch Event, Violations Action, or SANnav Event Action policies that used the "Use to exclude from results" filter condition (checkbox checked) will be removed. After the upgrade to SANnav v3.0.1, these exclusion policies must be manually reconfigured and redefined using the new filter definition method.

NOTE With SANnav v3.0.x, the Event Action Policies, Violation Action Policies and SANnav Application Event Policies have a condition for the filter which was modified to be an “exact” match as opposed to a ‘contains’ match. For example, in SANnav releases prior to SANnav v3.0.x, an action would be triggered if any part of the rule name matched the criteria, however, with SANnav v3.0.x, the action would be triggered only if the full rule name exactly matched. Therefore, it is critical to use the full rule name when creating filters for Event Action Policies, Violation Action Policies and SANnav Application Event Policies.

3.11.7 Switch Status and Diagnostics

The Switch Status and Diagnostics is a minor feature that has been added to SANnav v3.0.1. It is closely related to the CLI Troubleshooting feature provide in the `sannavcc` commands to troubleshoot SANnav for various communication issues.

A new menu under **SANnav > Monitoring > Switch Status and Diagnostics** has been introduced with SANnav v3.0.1.

This new menu takes the user to a table list page which is typically empty when there are no communication issues or errors between the SANnav and the switches.

There are two important columns:

- **Primary State** with the following possible values:
  - Monitoring Impaired
  - Authentication Failed
  - Not Reachable
- **Secondary State** with many possible values, such as (refer to the *SANnav Management Portal User Guide* for a list of all possible values for the secondary state)
  - SNMP Error
  - Syslog Error
  - Telemetry Error
  - Authentication Error

- Switch not ready
- Discovery Error
- Etc.

SANnav periodically (hourly) runs tests and diagnostics tests and if no errors are found, the table list view is empty.

If there are errors found during the diagnostics test, then the table will list one row for each issue found. That is, each table row represents an error for a given switch. If there are 3 errors that are affecting 2 switches then there will be 6 rows.

Users can then view the details of each test which will list the Test Name, Details, Recommendation and Result. Users can also run a suite of test on demand for one or more switches by selecting them and invoking the **Run Diagnostics** action or row action menu for one switch. The Test suite that can be executed is one of **SNMP, Syslog or Telemetry**.

Refer to the *SANnav Management Portal v3.0.1 User Guide* for details on this feature.

3.11.8 Health Summary Dashboard Enhancements

Two new factors have been introduced for monitoring Switch health score in SANnav v3.0.1. These are:

- **Authentication Failure** (default score value 20): related to authentication-related errors when attempting to communicate with a switch.
- **Monitoring Impaired** (default score value 10): related to issues that prevent the effective monitoring of a switch

These health attributes or factors are detected by the Switch Status and Diagnostic feature explained earlier in this document and rolled up to the health score of the affected switches.

Note that the factors Unknown status (Switch Status) and Port Data Collection (Switch Important Incidents) have been removed as they are effectively covered and rolled up in the two newly added factors above.

NOTE While the Switch Status is computed and determined on an hourly basis by the Switch Status and Diagnostics feature, the health computation operates at a fifteen minute basis. This may lead to inconsistencies in the switch status shown. When such issues arise, it is recommended to manually trigger the computation of both the health score as well as re-run the diagnostics tests for the impacted switches.

With SANnav v3.0.1, a new event is generated with Message ID **SSMP-HLTH-1005** (severity **Major**) when a switch health status changes from state Healthy to Degraded or Poor, or Degraded to Poor. This new event will appear in the SANnav notification panel.

NOTE The existing application event with Message ID **SSMP-HLTH-1001** (severity **Info**) has been refactored to only be raised when a switch health status changes from Poor to Degraded or Healthy, or Degraded to Healthy. This event will not appear in the SANnav notification panel.

3.11.9 Call Home Enhancements

With SANnav v3.0.1, a usability enhancement has been added in the Call Home feature for the Event Filter selection as explained below.

When multiple chassis are selected for a Call Home center, and if all selected chassis have the exact same filtered events configured, then the existing events in the filter will be shown as pre-selected. Any changes to this dialog (checked or unchecked events) will apply to all selected switches.

When multiple chassis are selected for a Call Home center, and if the selected chassis do not have the same exact filtered events configured, then the existing events in the event filter will not be shown as pre-selected (no events checked). Any changes to this dialog (checked or unchecked events) will apply to all selected switches (and will override the previous filter selection).

3.11.10 vCenter Enhancements

With SANnav v3.0.1, the following enhancements have been added to the vCenter Integration feature in SANnav.

- A new quick filter has been added at the top right of the **VM Inventory** retrieved from the vCenter servers defined in SANnav. This filter allows users to select which physical host to view the VM inventory for. By default, all Hosts are shown. Users can pick and choose which Host(s) to view VMs for by clicking on the quick filter.
- In the **Hosts Inventory** list page, for each host row there a new operation to invoke **Show Virtual Machines** has been added. When this operation is clicked for one host (no multi selection allowed) the **VM Inventory** view filtered for the selected host is open in the same tab (click) or new tab (CTRL-click).
- In the VM Inventory view, a new **Export** has been added to allow users to export the entire inventory of the VM discovered form the vCenter servers defined in SANnav.

3.11.11 Licensing Enhancements (TruFOS, POD and Feature Licenses)

With SANnav v3.0.1, launching the FOS Certificate and License Management page, will open the TruFOS/FOS Licenses Chassis list page by default and not the HTTPS Certificates page as was the case in previous SANnav versions.

The previously dropdown labelled **TruFOS Certificates** has been renamed as **TruFOS/FOS Licenses** and is now the default and first option in the drop down.

The action previously named **Apply TruFOS** has been renamed to **Apply TruFOS/FOS Licenses**. This action retains its original behavior from the previous SANnav release, with the sole enhancement being its ability to accept any XML license file, not just TruFOS XML files.

With SANnav v3.0.1, a Notification Panel event will be raised if the Broadcom BSN Licensing Portal URL is not accessible during the TruFOS auto-renewal process.

3.12 Features Deprecated with SANnav Management Portal v3.0.1

A *deprecated* feature is a feature that is still available in the current SANnav version, however, it may be removed in a future release of SANnav.

- The **`sannavcc` CLI textual menu** (with numerical options) introduced in SANnav v3.0.0.x. is deprecated with SANnav v3.0.1. It will be replaced with a command line interface with arguments in a future release of SANnav. The command `sannavcc` will remain and will have multiple arguments to invoke it. This approach is consistent with FOS CLI and standard Linux standard shells.
- The functionality to configure a Web Proxy (`sannavcc` Option 6 then Option 7) is deprecated with SANnav v3.0.1. It will be replaced by a different approach in a future release.
- The SNMP/Syslog and Telemetry streaming troubleshooting functionality accessible through the `sannavcc` command (Option 8, then, Option 7 for SNMP/Syslog and Option 8 for Telemetry streaming) is now deprecated since the new Switch Status and Diagnostics available with SANnav v3.0.1 release provides the same functionality and more.
- The **Inventory > Flows** feature listing the IT flows for chassis that have the Flow Telemetry enabled is deprecated with SANnav v3.0.1 in anticipation of an upcoming SAN Fabric Intelligence (SAN FI) feature support in a future SANnav version.
- The **SANnav > Filter Management** feature allowing to manage various filters in the SANnav UI is deprecated in anticipation of a new paradigm to manage UI filters in a future SANnav version.

- The special character backslash \ in any SANnav username (for local users as well as external users) has been deprecated. Customers are encouraged to not use this special character in any SANnav username and if used, to remove it to avoid issues in the future.
- For the SNMP Forwarding Feature, the following protocol values are deprecated
    - Auth Protocol values **HMAC_MD5** and **HMAC_SHA**
    - Priv Protocol values **CBC_DES** and **CFB_AES_128**

3.13 Features Removed from SANnav Management Portal v3.0.1

- The LDAP Fetch Groups support has been removed with SANnav v3.0.1. It was deprecated with SANnav v2.4.x.
- For the SNMP Forwarding Feature, the following are protocol values have been removed. They were deprecated in SANnav v2.4.x).
    - Auth Protocol value **NONE**
    - Priv Protocol value **NONE**

3.14 SANnav Management Portal v3.0.1 Supported SAN Switches

3.14.1 SANnav v3.0.1 Supported FOS Versions

- SANnav v3.0.1 (or later) is required to manage FOS v10.0.1x.
- SANnav v3.0.1 (and future v3.0.1 patches) supports FOS versions from FOS v8.2.3e2 up to FOS v10.0.1x.
- SANnav v3.0.1 will not manage any FOS versions greater than FOS v10.0.1x. Attempting to discover a seed switch from SANnav v3.0.1 with FOS version greater than v10.0.1x will fail in SANnav. FOS v10.0.1x will reject the request.
- Attempting to import a FOS PSD version greater than v10.0.1x will not be allowed in SANnav v3.0.1x Firmware Repository import action.

NOTE If a switch managed by SANnav is upgraded via the switch CLI, Web Tools, or by using the SANnav External option for file transfer to FOS versions greater than 10.0.1x, then SANnav v3.0.1x will not be able to rediscover and manage the switch after the FOS upgrade. FOS will reject the SANnav v3.0.1x request to discover and manage a switch running a FOS version greater than FOS v10.0.1x.

3.14.2 Recommendation for SANnav and FOS Upgrades

In a Fibre Channel environment managed by Brocade SANnav, it is highly recommended to upgrade SANnav to a version that supports the required Fabric OS (FOS) version **before** upgrading the switches to that required FOS version.

Failure to follow this practice will result in the upgraded switches becoming Unmonitored and Unmanaged in SANnav.

For example, if SANnav is running version v2.4.x and the switches are running FOS versions 9.2.x, upgrading FOS to version v10.0.x on a given switch **before** upgrading to SANnav to 3.0.0x will cause SANnav to mark the switch as Unmonitored and Unmanaged due to unsupported firmware (FOS v10.0.x not supported in SANnav v2.4.0x).

In such a scenario, the user will have to *delete* and *rediscover* the fabric containing the Unmonitored and Unmanaged switch for SANnav to properly manage the newly upgraded switch.

3.14.3 Hardware Platforms and FOS Support Matrix

The officially supported matrix of supported hardware platforms and FOS versions is listed in the table below.

NOTE Switches running FOS versions that are non-target path releases may be managed by SANnav, however, issues specific to those FOS firmware versions will not be addressed by Broadcom. Refer to the latest *Brocade Software Release Support and Posting Matrices* for official support for FOS, SANnav, and Target Path versions: https://docs.broadcom.com/doc/Brocade-SW-Support-RM

Switch Type	Hardware Model	FOS Version(s) Supported
Gen 8 Switches	▪ Brocade G820 ▪ Brocade X8-4 ▪ Brocade X8-8	▪ FOS v10.0.x or later
Gen 7 Switches	▪ Brocade G710 ▪ Brocade G720 ▪ Brocade G730 ▪ Brocade X7-4 ▪ Brocade X7-8 ▪ Brocade 7850 ▪ Brocade G748	▪ FOS v10.0.x or later ▪ FOS v9.2.2a and later ▪ FOS v9.2.1b and later ▪ FOS 9.2.0c3 and later
Gen 6 Switches	▪ Brocade G610 ▪ Brocade G620 ▪ Brocade G620 (switchType 183) ▪ Brocade G630 ▪ Brocade G630 (switchType 184) ▪ Brocade 7810 Extension Switch ▪ Brocade X6-4 ▪ Brocade X6-8 ▪ Brocade MXG610s Blade Server SAN I/O Module ▪ Brocade G648	▪ FOS v9.2.2a and later ▪ FOS v9.2.1b and later
Gen 5 Switches	▪ Brocade 7840 Extension Switch ▪ Brocade 6520 ▪ Brocade 6543 Blade Server SAN I/O module ▪ Brocade 6558 Blade Server SAN I/O module	▪ FOS v8.2.3f and later

3.14.4 End of Support (EOS) Hardware Platforms

When a switch reaches its End-of-Support (EOS) date, SANnav will mark the switch as Unmonitored and Unmanaged.

It is recommended to check for switch events indicating that the switch is nearing or has reached the EOS date by searching the SANnav Events page with Message ID EM-1240 (90 days or less to EOS date) or EM-1241 (when the EOS date is reached).

Unmonitored and Unmanaged means that the switch cannot be managed by SANnav and that SANnav cannot receive events or violations from the switch. The switch is also removed from the Switch Inventory page and the Fabric Discovery detailed page will indicate that the switch is in Unmanaged and Unmonitored state due to EOS.

If a fabric that contains one or more EOS switches is discovered in SANnav (using a non-EOS seed switch), the discovery will succeed, but all the EOS switches will be marked as Unmonitored and Unmanaged.

NOTE A fabric cannot be discovered using an EOS switch as the seed switch.

If an Extended EOS (EEOS) license has been installed on the switch, SANnav may take up to **24 hours** to rediscover and transition the switch state to Managed. The user will need to go to the Fabric Discovery page and monitor the switch again. If the EOS applies to a virtualized chassis then each of the logical switches within the chassis needs to be monitored again.

Refer to the official Broadcom website for End-of-Life and End-of-Support hardware platforms details:
https://www.broadcom.com/support/fibre-channel-networking/eol

3.14.4.1 Gen 4 Hardware Platforms

Gen 4 platforms are no longer supported with SANnav v3.0.1x.

Chapter 4: Brocade SANnav Management Portal Deployment

4.1 Server Requirements

SANnav Management Portal v3.0.1 can be deployed either on a single bare-metal host, VM, or as an OVA. The following two tables provide details of server requirements in each case.

NOTE A static MAC address is required for the SANnav server. A MAC address change may cause the SANnav UID to change, thereby rendering the current license invalid for the server. In these cases, a SANnav license rehosting is required.

VM and Bare-Metal Deployments

Max Switch Ports Under Management (Base or Enterprise)	Operating System	Host Type	Minimum vCPU	Memory	Hard Disk
Small 600 Ports (Base) or 3000 (Enterprise)	RHEL 9.7	Bare metal or VMware ESX 9.x VM or Bare metal/HyperV Windows Server 2022 VM	16 vCPUs	48 GB	600 GB
Large 15,000 (Enterprise)	RHEL 9.7	Bare metal or VMware ESXi 9.x VM or Bare metal/HyperV Windows Server 2022 VM	24 vCPUs	96 GB	1.2 TB

- Installing and running SANnav on RHEL 9.6 or RHEL 9.8 versions are allowed upon user acceptance with conditional support.
- No other RHEL releases other than RHEL9.6, RHEL 9.7 and RHEL 9.8 are allowed with SANnav v3.0.1.
- ESXi 9.x is recommended. SANnav v3.0.0 has not been validated with ESXi 8.x but installation should work.
- The recommended CPU speed is 2000 MHz. Running SANnav with lower CPU speed may result in lower performance.
- The recommended number of physical CPU sockets is two.

OVA Deployments

Max Switch Ports Under Management (Base or Enterprise)	Supported Hypervisor	Host Type	Minimum vCPU	Memory	Hard Disk
Small 600 Ports (Base) or 3000 (Enterprise)	VMware ESXi 9.x	VMware ESXi VM	16 vCPUs	48 GB	600 GB
Large 15,000 (Enterprise)	VMware ESXi 9.x	VMware ESXi VM	24 vCPUs	96 GB	1.2 TB

- SANnav MP v3.0.1 OVA packages Rocky Linux 9.7 in the OVA file
- ESXi 9.x is required. SANnav v3.0.1 has not been validated with ESXi 8.x but installation should work.
- The OVA deployment allows users to select a small or large deployment configuration.
- The recommended CPU speed is 2000 MHz. Running SANnav with lower CPU speed may result in lower performance.
- The recommended number of physical CPU sockets is two.

4.2 Client Requirements

The latest versions of the following web browsers are supported for a SANnav Management Portal v3.0.1 client:

- Chrome (Windows, Linux, MacOS)
- Firefox (Windows, Linux)
- Edge (Windows)

NOTE Refer to the *Web Tools User Guide and Release Notes* for a list of supported browsers for Web Tools launch for all FOS versions (FOS v8.x– Java required, and FOS v9.x and above – no Java required).

NOTE If horizontal scroll bars are not shown in a MacOS-based browser, MacOS has a system setting to show scroll bars. To show the scroll bar option, select System Settings > Appearance > Show scroll bars, and then select the option Always.

4.3 Software Upgrade

The supported upgrade and migration paths to SANnav v3.0.1 as specified in the table below:

Current Version	New Version	Supported	Comments
SANnav v3.0.0/v3.0.0.1	SANnav v3.0.1	Yes	In line upgrade in OVA deployments
SANnav v2.4.0/v2.4.0a and earlier	SANnav v3.0.1	No	Upgrade to SANnav v3.0.0 first, then upgrade to SANnav v3.0.1
SANnav v2.4.0b	SANnav v3.0.1	No *	This upgrade is not supported to minimize SANnav supported upgrade paths
Any SANnav v2.4.0x patches released **after** the GA of v3.0.0	SANnav v3.0.0	No *	Cannot upgrade to SANnav v3.0.0 from such patches.
Any SANnav v2.4.0x or SANnav v3.0.0x patches released **after** the GA of SANnav v3.0.1	SANnav v3.0.1	No *	Cannot upgrade to SANnav v3.0.1 from such patches.

- (*) Future SANnav releases will provide guidance about how to upgrade from those versions to the latest SANnav version available at that time.
- Customers running SANnav v2.4.0b will be able to upgrade to future patches on SANnav v3.0.0 and SANnav v3.0.1.
- Refer to *SANnav Installation and Upgrade Guide* for details before attempting a SANnav MP upgrade in all deployments.

Chapter 5: Licensing

The Brocade SANnav Management Portal can be licensed in either a Base or Enterprise version.

- SANnav Management Portal Base enables management of up to 600 ports residing on fixed port switches or embedded blade switches, but it cannot be used to manage ports from any Director platform (4-slot or 8-slot).
- SANnav Management Portal Enterprise enables management of up to 15,000 ports from any embedded switch, fixed port switch, or Director-class products.

Product Offerings	Description
SANnav Management Portal Base	Manages up to 600 ports from fixed-port or embedded switches but does not manage directors.
SANnav Management Portal Enterprise	Manages up to 15,000 switch ports from any type of switch including directors (either 4-slot or 8-slot).

ATTENTION SANnav Management Portal uses a subscription-based licensing model, which allows the product to function for the duration for which it was purchased. The SANnav Management Portal license must be renewed and installed in a timely manner to keep the product functioning without disruption.

Chapter 6: Scalability

6.1 SANnav Management Portal v3.0.1 Scale

Feature	Scalability Limit – SANnav Management Portal Base	Scalability Limit – SANnav Management Portal Enterprise
Maximum Number of SAN Ports Managed	600	15,000
Maximum Number of End Device Ports Managed	2000	40,000
Maximum Number of End Device Ports per Fabric	10,000	
Maximum Number of Events Stored	2 million or 30 days	
Maximum Number of MAPS Violations Stored	2 million or 30 days	
Port Statistics Stored	5-minute samples are stored for up to 30 days. 1-hour data is stored for 30 days. 1-day aggregated data is stored for 30 days. 10-second samples are collected for up to 3 days for a maximum of 100 user-selected Gen 6, Gen 7, or Gen 8 ports. Once data collection is complete, the data is retained for 14 days.	
Extension Tunnel Statistics Stored	5-minute samples are stored for up to 30 days. 1-hour data is stored for 30 days. 1-day aggregated data is stored for 30 days. 10-second samples are collected for up to 3 days for a maximum of 100 circuits (only supported for the SX6 Blade and 7810/7850 switch). Once data collection is complete, the data is retained for 14 days.	
Maximum Number of Flows Supported	Enterprise Edition (15,000 ports) large platform only. No support on small platforms. Up to 215,000 IT Flows (only IT Flows) maximum allowed.	
Flow Statistics Stored	5-minute samples are stored for up to 7 days. 1-hour data is stored for 30 days.	
Number of Concurrent User Sessions per SANnav Management Portal Server (*Includes UI Sessions and REST Sessions*)	25	
Tested vCenter scale (vCenter instances, ESXi Hosts, VMs)	• One vCenter instance discovered in SANnav: Total of 500 ESXi Hosts and 40,000 VMs distributed across all 500 ESXi hosts. • Seven vCenter instances discovered in SANnav: Total of 500 ESXi Hosts distributed across all 7 vCenter instances and 40,000 VMs distributed across all 500 ESXi Hosts.	

Chapter 7: Important Notes

7.1 General

- The network latency between SANnav clients to the SANnav Management Portal server and between the SANnav Management Portal server to the switches must not exceed 100ms. If the latency is higher than 100 ms, then communication timeouts may occur and cause undesirable behavior.
- Cockpit web console for Linux cannot co-exist with SANnav Management Portal.
- SANnav is expected to be installed and run on a dedicated host. If any other application is installed on the host, it is mandatory to uninstall it before starting the SANnav installation.
- SANnav application performance may be affected during operations like SANnav backup and support data collection. It is recommended to schedule SANnav backup during times when the server is not heavily used (late at night, or during weekends for example).
- In the SANnav > SANnav Password and Lockout Policies menu tab, even if the checkbox *Keep dashboard active after session expires* is checked, the dashboard will disappear after 24 hours if there is no user activity due to SANnav forcing the session timeout.

7.2 Infrastructure, Installation, and Upgrade/Migration

- When installing SANnav Management Portal v3.0.x and the firewall needs to be enabled, ensure the firewalld is configured before SANnav Management Portal installation.
- When migrating from previous releases to SANnav v3.0.x, if a custom port is used for internal SFTP/SCP, make sure that this port is not part of the required ports list. If the custom port is in the required ports list, change this port to any other free port using `sannavcc` before starting the upgrade and migration.
- .der format certificates cannot be used for certificate replacements in SANnav.

7.3 Firmware Management and Switch Support Save

- SANnav only supports strong ciphers for SANnav-to-switch communications using HTTPS. If a switch which is running FOS 8.2.x is configured to support weak ciphers, the firmware download will fail with an appropriate error in SANnav. Use CLI to perform the firmware upgrade in this case.
- The updated FOS firmware might not show properly in the SANnav UI if one or more ports in the fabric are switching from online to offline (or vice versa). This issue must be resolved in the fabric so that SANnav updates the firmware version correctly in the UI.
- A switch supportsave or firmware download operation initiated using SANnav Management Portal SCP or SFTP server will fail in the following scenarios for switches discovered using Federated Authentication (**FA) only** mode in SANnav in the following cases:
    - strict Host Key is enabled and the switch does not hold the SANnav server Host Key or has a different Host Key
    - strict Host key is not enabled or not supported on the switch and the switch has a different Host Key

To avoid this situation, add the SANnav server as a known host to the switch on which the firmware download or supportsave is going to be performed using the command:

```
sshutil addknownhost {<IP Address> | <Hostname FQDN>} [:<Port>] -fp <fingerprint> [-f]
```

A fingerprint of the SANnav server can be found at: `<install_home>/conf/server.properties` with property name `dcm.ssh.server.host.key`

7.4 Discovery and Performance Management

- A Web Tools session depends on the session timeout set on the switch irrespective of direct or proxy launch. Web Tools running in proxy mode validates the SANnav session before sending a request to the switch to avoid any illegitimate connection. If Web Tools is open in proxy mode, the SANnav client session will be considered as active; inactive time will be computed from the time Web Tools is closed.
- In cases where a switch was discovered using HTTP initially and then changed to HTTPS later, the port 80 and/or 443 must not be blocked until the protocol change is reflected in the SANnav UI.
- If a switch running FOS v8.2.x is using a DSA algorithm for the HTTPS certificate, SANnav cannot discover the switch because all the supported ciphers for this algorithm are no longer supported. Update the switch certificate to RSA algorithm and rediscover the switch.
- If a password is incorrectly entered when discovering a seed switch, an error message is shown indicating an incorrect password. It is recommended to wait five minutes before retrying to enter the correct password. If the user tries to enter the correct password within the first five minutes of the failure the same error message will be displayed.

7.5 SANnav Backup/Restore, Disaster Recovery, and SANnav Support Data Collection

- When the SANnav Management Portal server is restored from a SANnav Management Portal backup or when performing a disaster recovery (DR) failover, high granularity performance data, FCIP performance data, and flow statistics and violations are no longer collected due to a new SANnav certificate which does not match the Kafka certificates on the switches.
    - To resolve this issue, unmonitor and monitor all data-streaming switches. This will update the Kafka certificates on the switches with the new certificate from the SANnav server.
- When generating SANnav Support Data Collection (SSDC) when SANnav services are down, use the CLI option to collect SANnav SSDC.

Chapter 8: Security Vulnerability Fixes

In addition to defect fixes, software releases may also contain updates to address Common Vulnerabilities and Exposures (CVEs). The latest security vulnerability disclosures and descriptions of each CVE can be found by visiting the Brocade Security Advisories web page:

www.broadcom.com/support/fibre-channel-networking/security-advisories

Specific CVEs addressed within any given software release will be publicly released a short period after the initial posting of the software. This is done to provide enough time for OEMs to qualify security updates prior to public disclosure.

The exact CVEs addressed within the SANnav software releases are provided in the following security announcement:

support.broadcom.com/external/content/SecurityAdvisories/0/24999

Chapter 9: Defects

9.1 Known Issues in SANnav Management Portal v3.0.1

Defect ID	Description
SANN-161894	Incorrect firmware version is displayed in SANnav inventory
SANN-162647	Switch discovery fails with "Generic SSL handshake error"
SANN-162654	Discovery fails with Incorrect Credential message
SANN-163120	SANnav services fail to start successfully
SANN-163168	Health summary dashboard incorrectly shows Authentication Failed status
SANN-163292	Investigate from MAPS violations does not select correct measures
SANN-164122	The chassis is disabled after config restore.

9.2 Defects Closed with Code Change in SANnav Management Portal v3.0.1

Defect ID	Description
SANN-157304	Unable to retrieve TruFOS and SANnav license from the licensing portal.
SANN-158839	Local search for speed value does not work.
SANN-159295	MAPS and Zoning data are not displayed in SANnav.
SANN-159546	Drift check fails occasionally with service not available error.
SANN-159613	Redundant message "No extensions in certificate" is displayed.
SANN-159728	One end of circuits not shown in Inventory and user not able to modify existing tunnels/circuits.
SANN-159754	User not able to import the CSV exported from Zone Inventory.
SANN-159843	SANnav services fail to start
SANN-159859	HAM-1001 and HAM-1007 syslog messages not forwarded to SNMP trap destination as traps.
SANN-160815	SANnav Backup and Support Data Collection fail.
SANN-160916	Events & violations are not seen.
SANN-160947	SANnav services do not start.
SANN-161244	SANnav services fail to start
SANN-161516	SANnav incorrectly reports storage (target) ports as initiators
SANN-161791	SANnav does not send email notifications
SANN-161912	REST API to retrieve Health Summary Details fails to return any data
SANN-161956	System logs are filled with SANnav messages
SANN-162107	Unable to generate CSR
SANN-162536	Unable to delete user accounts
SANN-162578	Connection to Webhooks server fails

9.3 Defects Closed without Code Change in SANnav Management Portal v3.0.1

Defect ID	Description
SANN-162317	Timezone acronyms not displayed correctly in fault management views

Revision History

Version	Summary of Changes	Publication Date
1.0	Initial version of Brocade SANnav Management Portal v3.0.1 Release Notes (Digest Edition).	03/26/2026
2.0	Updated Sections 3.11, 4.3, 9.1 and 9.2	04/27/2026
3.0	Updated Sections 3.6.1, 3.6.2, 3.6.3.3, 3.10.10, 4.1 and 9.1	07/13/2026