# SANnav™ Management Portal v2.3.1

## SANnav Management Portal v2.3.1 Release Notes (Digest Edition)

## Version 5 (Digest Edition)

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.

# 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 | 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:<br>▪ Case Management<br>▪ Software Downloads<br>▪ Licensing<br>▪ SAN Reports<br>▪ Brocade Support Link<br>▪ 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.

For questions regarding service levels and response times, contact your OEM/solution provider.

To expedite your call, have the following information immediately available:

- General Information
  - Technical support contract number, if applicable
  - Switch model
  - Switch operating system version and SANnav version
  - Error numbers and messages received
  - SANnav Support Data Capture (SSDC) and Switch supportSave command output and associated files

  For dual-CP platforms, the `supportSave` command gathers information from both CPs and any AP blades installed in the chassis:

  - Detailed description of the problem, including the SANnav and switch or fabric behavior immediately following the problem and any specific questions
  - Description of any troubleshooting steps already performed and the results
  - Serial console and telnet session logs
  - Syslog message logs

- Switch Serial Number

The switch serial number is provided on the serial number label, examples of which follow:

FT00X0054E9

The serial number label is located as follows:

- Brocade G630, G620, G610, G720, and G730 – On the switch ID pull-out tab located on the bottom of the port side of the switch
- Brocade 7810 – On the pull-out tab on the front left side of the chassis underneath the serial console and Ethernet connection and on the bottom of the switch in a well on the left side underneath (looking from the front)
- Brocade X6-8, X6-4, X7-8, and X7-4 – Lower portion of the chassis on the non-port side beneath the fan assemblies

- World Wide Name (WWN)
  - When the Virtual Fabric feature is enabled on a switch, each logical switch has a unique switch WWN. Use the `wwn` command to display the switch WWN.
  - If you cannot use the `wwn` command because the switch is inoperable, you can get the primary WWN from the same place as the serial number.
- License Identifier (License ID)
  - There is only one license ID associated with a physical switch or director/backbone chassis. This license ID is required as part of the ordering process for new FOS licenses.
  - Use the `license --show -lid` command to display the license ID.

## 1.2 Related Documentation

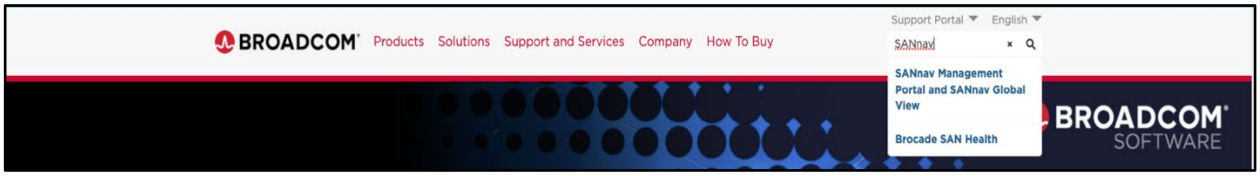
White papers, data sheets are available at www.broadcom.com. Product documentation for all supported releases is available on the support portal to registered users. Registered users can also find release notes on the support portal.

# Chapter 2: Locate Product Manuals and Release Notes

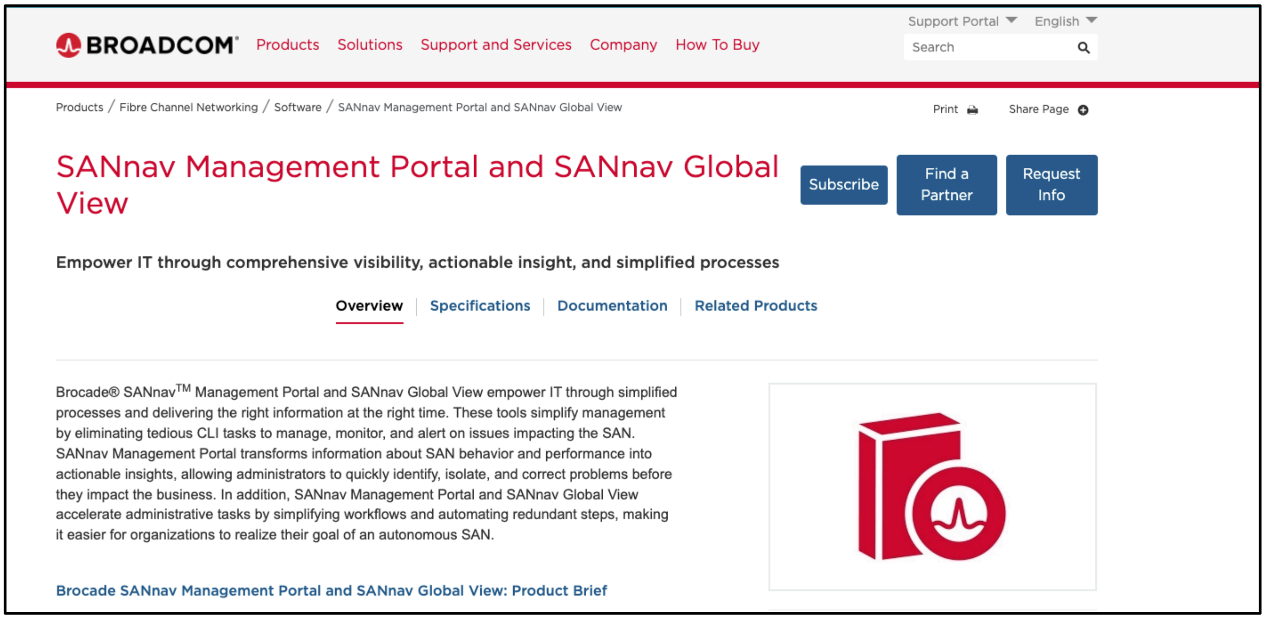
## 2.1 Locate Product Manuals on Broadcom.com

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

1. Go to www.broadcom.com, click **Login**, and enter your username and password.
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:



SANnav Management Portal and SANnav Global View

Empower IT through comprehensive visibility, actionable insight, and simplified processes

Brocade® SANnav$^{TM}$ Management Portal and SANnav Global View empower IT through simplified processes and delivering the right information at the right time. These tools simplify management by eliminating tedious CLI tasks to manage, monitor, and alert on issues impacting the SAN. SANnav Management Portal transforms information about SAN behavior and performance into actionable insights, allowing administrators to quickly identify, isolate, and correct problems before they impact the business. In addition, SANnav Management Portal and SANnav Global View accelerate administrative tasks by simplifying workflows and automating redundant steps, making it easier for organizations to realize their goal of an autonomous SAN.

Brocade SANnav Management Portal and SANnav Global View: Product Brief

## 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.

## 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 v2.3.1 Release Overview

Brocade SANnav Management Portal v2.3.1 is a maintenance software release introduced to support Fabric OS® (FOS) v9.2.1 and to provide support for Brocade Unified Storage Fabric. Brocade Unified Storage Fabric (USF) is a new capability introduced in FOS v9.2.1, enabling IP Storage (IPS) in parallel with Fibre Channel on the same unified fabric.

With Brocade USF the fabric is a dedicated network with integrated storage services for all types of storage, including Fibre Channel, FICON, iSCSI, NVMe/TCP, and NAS. SANnav v2.3.1 pairs with FOS v9.2.1 which is required to deploy IPS functionality.

This chapter highlights the new features, support, capabilities, and changes in the SANnav Management Portal v2.3.1 release. Specifically, features to manage USF for IPS devices end to end as well as other features and enhancements not related to USF are highlighted.

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** v2.3.1 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 v2.3.1

SANnav v2.3.1 is introduced to provide all required functions and features to manage USF and IPS capabilities in a SAN Fabric as well as to introduce incremental enhancements in specific SANnav functional areas.

The USF-related and IPS-related highlights are as follows:

- Hardware support and USF IPS Fabric Discovery
- IPS Inventory
- IPS Provisioning and Configuration
- IPS Fabric creation and management
- IPS end-to-end IP device connectivity
- IPS Monitoring
- IPS Troubleshooting
- IPS Topology
- IPS Reports

The non-USF-related highlights are as follows:

- Deployment, OS Support, Disaster Recovery (DR) enhancements such as RHEL 9.2 support and DR on bare metal platforms
- Security enhancements
- Zoning enhancements
- Inventory enhancements
- Configuration Policy Management enhancements
- Call Home enhancements

- User Management enhancements
- Fault Management enhancements
- Miscellaneous enhancements
- Flow Management changes

### 3.2.1 What’s New in SANnav Management Portal v2.3.0

SANnav v2.3.0 provides new features and feature enhancements that aim at simplifying and automating common and frequent operations.

The following new features or feature enhancements are provided in various functional areas of SANnav:

- Server Platform deployment, Installation, Upgrade, and Migration (including Disaster Recovery)
- Security and Infrastructure: provide security features and enhancements in all areas (SANnav server and managing Switch and FOS security)
- SANnav Licensing
- FOS Certificates Management
- FOS Firmware Platform Specific Download (PSD) Management
- Call Home
- Discovery
- Inventory: simplify device ports to enclosure mapping using host and storage mapping policies.
- Zoning: simplify day to day zoning tasks with new or enhanced workflows such as Zone Database snapshots and zone policies.
- Configuration Policy Management: accelerate the deployment of new switches, hosts, and targets with enhanced features.
- Flow Management: quickly identify issues with device ports with new IO Health and Latency widget
- Dashboards and Reports
- Events and Violations
- Topology
- UI/UX and Usability changes: enhanced overall UI/UX usability features in Inventory, Topology, Flow Management, Dashboards and Reporting

Defect fixes included in this release are listed in the Defect Tables section of this document.

## 3.3 New Hardware Platforms Supported in SANnav Management Portal v2.3.1

Support for the following hardware platforms has been added in SANnav Management Portal v2.3.1.

- None

## 3.4 New Blades Supported in SANnav Management Portal v2.3.1

The following new blade platforms have been added in SANnav Management Portal v2.3.1.

- None

## 3.5 SANnav Management Portal Server Platform Support and OS Support

### 3.5.1 SANnav Management Portal v2.3.1 OVA Support

SANnav v2.3.1 continues to support deploying SANnav Management Portal as an Open Virtual Appliance (OVA).

SANnav v2.3.1 OVA now packages Rocky Linux v8.8.

- Deployment of the OVA file is supported on vCenter 8.x (and ESXi 8.x) officially.

**NOTE** Extraction of the SANnav OVA image using vCenter 7.x *should* work but has not been tested or qualified with SANnav v2.3.x.

- OVA is currently available only for SANnav Management Portal and **not** for SANnav Global View.
- Upgrade and Migration from SANnav v2.3.0 to SANnav v2.3.1 is to be performed inline since the OS kernel is the same (8.x based).
- Upgrade and Migration from SANnav v2.2.2x to SANnav v2.3.1 cannot  be performed inline (disruptive OS change, CentOS to Rocky)
- Instead of automatically starting the installation on the first login, the script `install-sannav.sh` must be manually run after successfully setting up the VM (same as SANnav v2.3.0).
- By default, firewalld is disabled in the OVA deployed VM (same as SANnav v2.3.0).
- SANnav v2.3.1 OVA deployment will enforce changing the root password of the operating system at the first login. A new root password must be entered by the user deploying SANnav v2.3.1 OVA.
- While deploying SANnav 2.3.1 OVA, if a valid DNS IP address is not available, use IP address 127.0.0.1 (IPv4) or ::1 (IPv6).

**ATTENTION** Make sure to strictly follow the *SANnav MP Installation and Upgrade Guide* before attempting the upgrade and migration from SANnav Management Portal v2.2.2x OVA to SANnav MP v2.3.1 OVA.

#### 3.5.1.1 Important Consideration when Upgrading from SANnav MP v2.3.0 to SANnav MP v2.3.1 (OVA Only)

When upgrading from SANnav v2.3.0 to SANnav v2.3.1, it is recommended to first upgrade SANnav software using an inline OVA upgrade and then to upgrade the OS on the SAN nav host/server.

If, for any reason, the OS on the SANnav host/server was upgraded first prior to upgrading SANnav software to v2.3.1, then the user must modify a specific SANnav script otherwise the upgrade procedure will fail.

The next two subsections explain the recommended upgrade procedure and the work around in case the recommended upgrade procedure was not followed.

##### 3.5.1.1.1 Recommended Upgrade Procedure from SANnav v2.3.0 to SANnav v2.3.1 in OVA

- First, upgrade SANnav MP from v2.3.0 to v.2.3.1
- Second, upgrade the Rocky OS using the Linux command `dnf -y upgrade`

**NOTE** This will bring the OS to Rocky 8.9 on the host. SANnav v2.3.1 will still package Rocky 8.8 inside the SANnav v2.3.1 VM, and a message will be shown to the user that the OS (Rocky 8.9) is not qualified or tested. This message may be disregarded.

##### 3.5.1.1.2 Workaround if Recommended Upgrade Procedure was Not Followed

If Rocky OS is upgraded (to 8.9) on the SANnav host/server using the `dnf -y upgrade` command before upgrading SANnav fromv2.3.0 to v2.3.1, then the *procedure below must be followed to proceed with the SANnav upgrade to v2.3.1 otherwise the upgrade procedure will fail:*

- Edit the script in `<Install Home>/bin/lib/check-os-version.sh` before attempting SANnav v2.3.1 upgrade as follows:
  - Line 38: Change from `local supportedNonTestedOSVersions=("rocky-8.6")` to `local supportedNonTestedOSVersions=("rocky-8.6" "rocky-8.9")`
  - Line 147: Change from `local ovaSupportedNotTestedVersions=("rocky-8.6")` to `local ovaSupportedNotTestedVersions=("rocky-8.6" "rocky-8.9")`

**NOTE** In this scenario as well the same message will be shown to the user that the OS (Rocky 8.9) is not qualified or tested. This message may be disregarded.

#### 3.5.1.2 OVA and Rocky Linux CVEs Process

While Brocade ensures that CVEs on the OS (Rocky Linux) are addressed at the time of releasing SANnav v2.3.1, it is possible that some specific Rocky Linux 8.8 CVEs are only found and disclosed after SANnav v2.3.1 has been released and before a patch on SANnav v2.3.1 is issued.

**NOTE** In the event this occurs, it is the end user's responsibility to update Rocky Linux with OS security patches on the SANnav server and OS if necessary to address new CVEs. *If that is not possible due to internal constraints such as internet access and security, contact Brocade Support.*

### 3.5.2 SANnav Management Portal v2.3.1 OS Support (VM and Bare Metal)

SANnav Management Portal v2.3.1 was fully qualified and tested with the following versions of RHEL:

- RHEL releases **8.8** and **9.2**.

Note that SANnav v2.3.1 is the first release to officially support RHEL 9.x based OS releases,

**NOTE** When installing SANnav on an untested or unqualified OS version, (i.e., 8.2, 8.3, 8.5, 8.6, 8.7, 8.9, 9.3), the installation script displays a warning message indicating that the SANnav Management Portal installation will proceed on an untested and unqualified OS version. Explicit end user acceptance is required for SANnav Management Portal installation to proceed. While it may be possible to successfully install SANnav on these OS versions, if an issue(s) occur while using SANnav it may be necessary to upgrade/downgrade to a fully qualified and tested OS version and reproduce the issue(s) to receive support.

The following table shows the various OS types and versions and the associated support in SANnav v2.3.1 Cells marked with (Blocked) indicate that the SANnav v2.3.1 installation/upgrade will not proceed and exit, while cells marked (Not Blocked) indicate the SANnav v2.3.1 installation/upgrade will proceed with explicit user acceptance that SANnav will run on an untested and unqualified OS Release. The Disaster Recovery (DR) support is also shown in the table for completeness.

| OS Type and Version | VM or BM (Bare Metal) | OVA | DR Support |
|---|---|---|---|
| RHEL 7.9, 8.0, 8.1, 9.0, 9.1 | No (Blocked) | No | No (Blocked) |
| CentOS 7.9 | No (Blocked) | No | No (Blocked) |
| RHEL 8.8, 9.2 | Yes | No | Yes - VM & **BM (new)** |
| RHEL 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.9, 9.3 | No (Not Blocked) | No | No (Not Blocked) |
| Rocky Linux 8.8 | No (Blocked) | Yes | Yes (OVA only) |
| Rocky Linux 8.8 and higher | No (Blocked)* | No | No (Blocked) |

***Refer to section 3.5.1.1.1 Recommended Upgrade SANnav 2.3.0 to 2.3.1 in OVA Procedure**

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

- Language = English and Locale = US

Other Languages and Locales are **not** supported.

## 3.5.3 Disaster Recovery (DR) New Features

- DR support on bare metal (BM) servers is **new** in SANnav v2.3.1. DR was only supported on VM and OVA deployments up to SANnav v2.3.0.
- Up to SANnav v2.3.0, users needed to uninstall the entire SANnav application to remove or reset the DR configuration in the Active server. With SAN nav v2.3.1, users can now execute `reset-dr-primary.sh` script on the Active server which will clear all disaster recovery configurations and restart the SANnav server. In addition, the script `reset-dr-primary.sh` script may be executed at any time if there is a failure while setting-up the Active SANnav server.
- While setting up the DR standby server, user can now choose to not auto-rehost the SANnav license during a planned or unplanned failover. This will save time while testing the planned failover to make sure DR operations will work properly should a disaster or outage happen.
- When the DR script `setup-dr-standby.sh` is executed, it will prompt the user for 3 items:
  - Option to automatically rehost the SANnav license after failover (yes or no, default is no)
  - The email server address
  - To and from e-mail addresses
- Email notifications on disaster recovery standby server can now be configured, updated, and disabled after completion of the DR setup.
  - Execute `setup-dr-email-notifications.sh` script after disaster recovery on the standby server setup to update email notification settings

**ATTENTION** The *SANnav Management Portal Installation and Upgrade Guide, 2.3.x* document provides step-by-step procedures in eight different use cases (VM/BM or OVA, revertive failover or not, planned, or unplanned combinations) to perform DR functions. Make sure to refer to this section of the document before proceeding with setting up Disaster Recovery in SANnav MP.

## 3.5.4 Other Installation and Deployment Features

### 3.5.4.1 SSL Certificate Expiry Notice

Starting with SANnav v2.3.1, a SANnav Application Event is raised 30 days before the SANnav SSL certificate expires.

After that, and within the 30-day window, an event is sent daily asking the user to replace the current SSL certificates with new ones.

The following SANnav Application Events are raised for SANnav certificates expiration:

- SSMP-SMON-1005 – Warning – 30 to 6 days before expiration.
- SSMP-SMON-1006 – Major – 5 days to 3 days before expiration.
- SSMP-SMON-1007 – Critical –2 days before expiration.

With SANnav v2.3.1, the SAN administrator user can generate and replace the current (valid or expired) SSL certificates with a set of new self-signed certificates by running the script `$INST_HOME/bin/generate-and-replace-self-signed-certificates.sh`

**NOTE** It is recommended to use Certificate Authority (CA) signed certificates (instead of self-signed certificates) and install them on the SANnav server for the highest security protection.

**ATTENTION** SANnav SSL certificate expiration will impact and interrupt features such as Streaming and Secure Syslog.

### 3.5.4.2 SANnav File System Permissions Change

With SANnav v2.3.0, all files under SANnav installation directory had Linux permissions 775 (rwx-rwx-r-x).

With SANnav v2.3.1,all files and folders under the SANnav installation directory now belong to UID/GID `sannavmgr` (UID/GID 56900) with file permissions set to 770 (`rwx-rwx----`) as shown in one folder example below:

```
drwxrwx---  2 sannavmgr sannavmgr  4096 Oct 16 19:18 templates
```

### 3.5.4.3 Stop and Start SANnav with Operating System

With SANnav v2.3.1, when an administrator performs a graceful reboot of the OS on the machine where SANnav server is running, the SANnav application will be gracefully stopped and restarted properly after the OS reboots successfully.

### 3.5.4.4 Host Time Zone Check

SANnav needs a valid Time Zone set in operating system to operate properly. Starting SANnav v2.3.1 if the time zone settings are deleted accidentally, the SANnav server will not start.

An error message will be shown asking the administrator to set the time zone using the command `timedatectl set-timzone <TIME_ZONE>`

## 3.5.5 FIPS-140-Enabled OS

SANnav MP v2.3.1 is supported on FIPS-140-enabled RHEL (VM or bare metal) or Rocky (OVA). Please refer to RHEL or Rocky specific OS version for the exact command(s) to enable FIPS mode.

Note that SANnav itself is **not** FIPS-140 certified. SANnav v2.3.1 may be installed and run on an officially supported RHEL version with FIPS-140 enabled.

- On bare metal and VM deployments, FIPS-140 mode may be enabled prior to installing SANnav.
- On OVA deployment, FIPS-140 mode must be enabled post installation.

- It is possible to enable FIPS after running SANnav in non FIPS-140 enabled OS by stopping the SANnav server, enabling FIPS-140 mode at the OS level, then starting the SANnav server again.

### 3.5.6 SE Linux Support

SANnav Management Portal v2.3.1 is **not** supported on Security Enhanced versions of Linux (SE Linux) in ***Enforcing*** or ***Permissive*** mode on either Rocky or RHEL. The only SE Linux mode supported is ***Disabled***.

If SE Linux is found to be enabled (either ***Enforcing*** or ***Permissive***) during SANnav installation, the installation script will stop and exit. Enabling SE Linux post SANnav installation is **not** supported as mentioned above.

**NOTE** Contact Brocade Technical Support for more information and details on SE Linux support.

## 3.6 Summary of New and/or Enhanced Software Features

### 3.6.1 Security and Infrastructure

#### 3.6.1.1 Chassis Password Management for FOS maintenance Account

Up to SANnav v2.3.0 it is possible to bulk select multiple chassis and request SANnav to change the password for FOS user **admin** on all user selected chassis to the user provided password.

With SANnav v2.3.1, this functionality has been extended to support the same functionality for FOS user **maintenance**.

**NOTE** This feature is supported for FOS v9.1.1 or higher only.

**NOTE** Changing the FOS *default* **maintenance** password the first time on a factory shipped chassis is not allowed from SANnav for security reasons. A message will be shown asking the user to first change the switch default **maintenance** account in FOS CLI before changing it with SANnav subsequently.

#### 3.6.1.2 vCenter Account and Password Change

With SANnav v2.3.1, it is now possible to select a single vCenter discovered instance (no bulk change) in SANnav and change the account (username) and/or the password for SANnav to subsequently login to that vCenter instance using the new credentials. Note that this will trigger rediscovery of the vCenter instance in SANnav.

#### 3.6.1.3 Installation and Upgrade/Migration as sudo

- Prior to SANnav v2.3.x, only the **root** user could install and manage the SANnav server. **sudo** privileged users could not install/upgrade/run/manage SANnav server.
- With SANnav v2.3.x, users with **sudo** privileges can now install and manage SANnav server (in addition to the **root** user).
- **sudo**-privileged users can install and manage SANnav server by prefixing the script execution with **sudo**: `sudo ./install-sannav.sh.`
- After installing SANnav v2.3.x, additional **sudo** users may be added to manage SANnav by executing the script `add-user-to-sannavmgr-group.sh`. This script can be executed by **sudo** user.

**NOTE** The user to be added must have **sudo** privilege already. This script simply adds that user to the list of users that can manage and run SANnav.

#### 3.6.1.4 Running SANnav Containers with No root or sudo Privileges

- With SANnav v2.3.x, docker containers will run as a new user **sannavmgr** with UID/GID 56900. This new user does not require **sudo** privileges.
- For security reasons, user **sannavmgr** cannot be used for remote SSH login to the SANnav server.
- During SANnav v2.3.x installation or upgrade/migration, this user **sannavmgr** with UID/GID 56900 will be created. Make sure it is available prior to starting SANnav v2.3.1 first time installation.

**ATTENTION** UIDs 56900 is not configurable in SANnav v2.3.0 and v2.3.1. If UID and GID 56900 is occupied by another user on the SANnav host, the installation or upgrade will fail.

- UID 1000 was required in prior SANnav releases, and is still required for SANnav v2.3.x to receive streams from FOS. SANnav will create UID/GID 1000 with username/group name as **sannavstreaming**. If UID/GID are occupied by another user name and group name, then whatever username/group name is associated with UID/GID 1000 will be used.

#### 3.6.1.5 Important OS-Level Customization for User sannavmgr (UID 56900)

- The SANnav server needs ports lower than 1024 for running some of its services.
- Due to this, the Linux ip_unprivileged_port_start parameter is set to `0` to allow **sannavmgr** to run services on ports lower than 1024.

#### 3.6.1.6 Change SANnav Server Security Password

With SANnav v2.3.x, it is now possible to change the SANnav password post installation.

The SANnav Server Security password is used to encrypt SSL private key and to secure Kafka Keystore and Kafka truststore.

Prior to SANnav v2.3.x, this SANnav Server Security password cannot be changed post SANnav installation or upgrade.

With SANnav v2.3.x, this password can be changed by an authorized and privileged user after installation or upgrade completes. Invoke the SANnav console script `manage-sannav-configurations.sh`.

- This script has been renamed to `manage-sannav-configuration.sh` in SANnav v2.3.x from `sannav-management-consol.sh` in previous releases.

#### 3.6.1.7 Nested LDAP Groups

- With SANnav v2.3.x, it is now possible to fetch SANnav Groups (Authentication Groups) even if they are defined in a nested fashion. This was not possible with SANnav releases prior to SANnav v2.3.x.
- To fetch the complete hierarchy, the user can import the nested hierarchy from the topmost outer group.

#### 3.6.1.8 MFA and SSO Support with SAML 2.0-Compliant Protocol

SANnav v2.3.x now supports SAML 2.0 integration with various Identity Providers (IdP). SANnav v2.3.x should work seamlessly with any IdP complying with SAML 2.0 REST specifications.

SANnav v2.3.x has been specifically tested and validated with the following SAML 2.0 Identity Providers:

- Okta
- Microsoft Azure (SANnav MP and GV are now available in the Azure Gallery)
- Microsoft ADFS
- Keycloak

#### 3.6.1.9 Secure Syslog Registration with FOS

Since FOS v8.2.x, there is a validation/authentication of the hostname (FQDN or IP address – IPv4 or IPv6) with HTTPS certificates on FOS. SANnav v2.3.x secure syslog reception will ensure the following:

- Third-party or self-signed HTTPS certificates are used when registering:
  - FQDN
  - IPv4 or IPv6 addresses
- For secure syslog to work properly with custom (third-party signed) certificates, a FQDN must be configured on the SANnav host server before SANnav installation.
  - If the FQDN has not been configured on the SANnav server, then SANnav falls back to using IP address.
- After upgrade and migration, a previously registered secure syslog with an IPv4 or IPv6 address will be replaced with the SANnav FQDN if an FQDN was defined for the SANnav host
- If a switch (SwitchA) is discovered in a SANnav server (ServerA) and if an attempt is made to discover SwitchA in another SANnav server (ServerB), then the syslog HTTPS certificate will be automatically imported in ServerB, and secure syslog will no longer be functional in ServerA.

### 3.6.2 User Management Enhancements

#### 3.6.2.1 Email Addresses to External Authentication Users

When an external Authentication (LDAP, RADIUS, SAML2.0) is used, the user accounts (username only, password is not stored in SANnav for external users) are automatically created upon successful login for the first time in SANnav.

Prior to SANnav v2.3.1, these accounts were not editable to add email addresses. This prevented these external users from receiving event notifications via email.

SANnav 2.3.1 now enables the fields Tags, Description, Email and Phone number Fields to be configured and used to forward event notifications and reports by email to those external users.

In addition, any external user may configure their own personal information (including email) under **User Preferences > Personal Info UI** form.

#### 3.6.2.2 User Deletion Behavior Change

When a user is deleted from the SANnav database, the Filters that were associated with that user will be associated with the default **System** user.

Any other user can then save these System filters (Save As …) to retain them or delete them if no longer needed.

### 3.6.3 Fault Management Enhancements

#### 3.6.3.1 Default Filter to Exclude Unacknowledged SANnav Application Events

Prior to SANnav v2.3.1, SANnav events cannot be suppressed using an Event Action Policy. This may cause unwanted events to be displayed when too many such SANnav events are triggered. Most of the time, these messages should be suppressed.

In the absence of suppress action, SANnav 2.3.1 provides an out-of-the-box default filter that excludes all acknowledged events. The default filter is called Exclude Unacknowledged Events and can be seen under the Filters view.

Users can now create a new Event Action Policy (EAP) to acknowledge unwanted SANnav events by using this new default Exclude Unacknowledged Events filter when creating the EAP.

### 3.6.3.2 SANnav Events Message ID Reference View

Under **SANnav > Fault Management** menu tab, a new entry called SANnav Events has been added. When clicking on this new view, a reference table with columns Message ID, Severity, Feature, and Event Summary will be shown.

The intent of this new reference table is to help users to easily search and identify the correct Message IDs to be used when creating/updating Events filters and Event Action Policies.

### 3.6.3.3 Custom Description Forwarding Filter and SANnav Custom Description

With FOS, certain traps do not contain the key fields Severity and Description. The following traps are left empty in the FOS MIB definition:

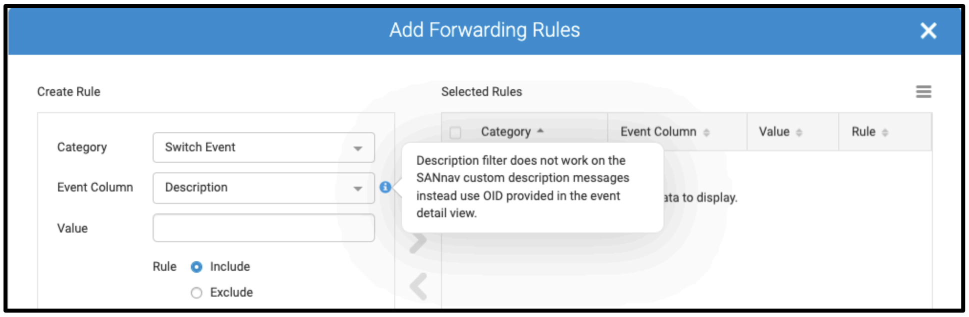
- connUnitPortStatusChange
- swStateChangeTrap
- swPortMoveTrap
- fruStatusChanged
- fruHistoryTrap
- swFabricSegmentTrap
- swDeviceStatusTrap
- swZoneConfigChangeTrap
- cpStatusChanged
- swFault

When SANnav receives these kinds of traps, it will customize the Severity and the Description attributes before displaying them in the SANnav Events list view. However, when using the SNMP Forwarding feature of SANnav to forward such traps to an external SNMP collector system, they will be sent as is (raw).

In SANnav v2.3.1, the Description customization prepends the text `SANnav custom description:` at the beginning of the description field to indicate that these have been customized by SANnav.

In addition, an information message (i) has been added when creating a new Forwarding Filter next to the Description field to clarify that the user should use the OID field instead of description for these types of traps.

This information message appears when user creates a Forwarding Filter, and add a Forwarding Rules where the Category is set to Switch Event and the Event Column is set to Description. In this case the (i) message will appear:



Add Forwarding Rules

Create Rule

Category: Switch Event

Event Column: Description

Value:

Rule: ● Include ○ Exclude

Selected Rules

| Category | Event Column | Value | Rule |
|---|---|---|---|

ata to display.

Description filter does not work on the SANnav custom description messages instead use OID provided in the event detail view.

### 3.6.3.4 Event Filter Logic Simplification

Prior to SANnav v2.3.1, the logic for filters when multiple Category values are selected always resulted in 0 results. For example, if a user created a filter with two different Categories and two different Event Columns for the filter, the filter would lead no results prior to SANnav v2.3.1. This is because prior to SANnav v2.3.1 rules created with multiple Categories resulted in zero records fetched as per SANnav logic.

SANnav v2.3.1 uses a new logic to group by Categories first and then group by the Event Columns and uses an OR operation in between to yield the desired/expected results.

#### 3.6.3.5 Event Action Policy Filter Behavior Modification

In the Event Action Policy filters, a new message has been added to explain the new behavior of the EAP filter with regards to Exclude behavior as follows:

> *Include and exclude rules are applied per category. All events that fulfill the criteria defined by Include rules will be s elected first, then events fulfilling the criteria defined by the Exclude rules will be removed from that Include rules. The All option for Category is deprecated as its use may lead to unexpected results in some situations. Refer to the SANnav Management Portal User Guide for details.*

#### 3.6.3.6 Trap Forwarding Enhancements

Since raw traps are used for forwarding, SANnav versions prior to SANnav v2.3.1 default to Info Severity if the SNMP trap sent by FOS does not have a severity associated with it. This behavior results in traps not being forwarded if a filter is used based on custom severity.

SANnav v2.3.1 enhances the SNMP trap forwarding to take the custom severity into account while applying forwarding filters.

### 3.6.4 Call Home Enhancements

#### 3.6.4.1 IBM Call Home

##### 3.6.4.1.1 New Customer Details (First and Last Name)

The IBM Call Home Center in SANnav 2.3.0 has been enhanced to add the following customer details:

- First Name
- Last Name
- Phone Number
- Alternate Phone Number
- Email
- SANnav Server Location

In SANnav v2.3.1 the fields First Name and Last name above have been enhanced to support the following special characters: `.\_-!@#$%^()` and the white space ‟ ‟ character.

##### 3.6.4.1.2 Test Call Home to Include all Three Chassis Serial Numbers

The IBM test Call Home email has been modified to now includes all three chassis serial numbers in the body of the email, so it is the same as production Call Home email:

- Factory Serial Number
- Supplier Serial Number
- Chassis Serial Number (this field has also been added to the production email; it was missing before)

### 3.6.4.2 Dell Secure Connect Gateway (SCG) (Dell SRS Replacement)

Starting with SANnav v2.3.1 onwards, Dell SRS will no longer be supported. It is replaced by a new Dell SCG software.

SRS will be renamed to SCG in the Dell Technologies Call Home details page in the SANnav UI and in associated SANnav application events.

When upgrading and migrating from prior versions to SANnav v2.3.1, the SRS gateway details previously configured, including the chassis that were associated with the SRS center, will be preserved and the associated with a new SCG entry instead. If modifications need to be made after upgrade and migration, they may be done form the Dell SCG details page.

**ATTENTION** SANnav v2.3.1 has been tested and validated with SCG version 5.20.00.10. Other releases have not been tested with SANnav v2.3.1 and therefore are not supported by SANnav v2.3.1.

#### 3.6.4.2.1 Dell SCG Keep Alive

In addition to migrating from Dell SRS to Dell SCG, SANnav v2.3.1 adds a keep alive support for Dell Technologies SCG Call Home Center.

The Keep Alive RESTful services from SCG allows the SANnav management application to ping SCG every 15 minutes using secure RESTful services. SCG creates an alarm if the Keep Alive update is not updated within the threshold period. This feature is useful for monitoring functioning of the SCG Call Home Center.

### 3.6.4.3 NetApp Call Home

NetApp's automation case creation tool relies on the *Chassis Factory Serial Number* in the subject line to check for valid entitlement. Up to SANnav v2.3.0, the title of the email for NetApp Call Home Center included the *WWN Factory Serial Number* instead.

SANnav v2.3.1 now includes the *Chassis Factory Serial Number* in the e-mail subject line for NetApp Call Home Center. Other fields in the subject are untouched.

In addition to updating the subject line, the following serial number is also be added to the body of the NetApp Call Home e-mail:

- Chassis Serial Number

**NOTE** Factory Serial Number and Supplier Serial Number were already in the email.

### 3.6.4.4 License Serial Number in Call Home Email (Brocade and NetApp Only)

SANnav License Serial Number will be included in the Call Home e-mail for Brocade and NetApp Call Home Centers. A new entry in the body of the email will be added under the Management Server Information section of the email follows:

- Management Server Information
  - Server Name = sannav-portal-v231
  - Server IP = <IP Address>
  - Server Version = 2.3.1 build <xyz>
  - SANnav Active License Serial Number : <Serial Number>

### 3.6.4.5 Call Home Status Indication by Last Notification Sent

A new column has been added in each Call home centre list page called Last Notification which will indicate when the last notification was sent from SANnav to the Call Home Center.

The intent of this new column is to help customers determine if the Call Home Center is working properly.

### 3.6.5 Discovery

**ATTENTION** FOS v9.2.1 has introduced a new authentication mechanism for machine-to-machine interfaces using an OAuth protocol Federated Identify Provider (Azure). SANnav v2.3.1 does not use this method of authentication and continues to use traditional username and password to discover fabrics.

**ATTENTION** Fabric Discovery with RSA based FOS usernames and password are not supported in SANnav. Specifying an RSA based username and password for the seed switch in the Fabric Discovery dialog will result in SANnav discovery failing with the message `seed switch authentication failed`.

#### 3.6.5.1 Display SNMP Auth and Priv Protocol Details

In the **SANnav > SAN Monitoring > Fabric Discovery** list page which shows the list of Discovered Fabrics, clicking on the Fabric name will show the details of the Fabric with a table showing the list of Logical Switches in this Fabric. In this list, two new columns are now added in SANnav v2.3.1:

- Auth Protocol value (e.g. HMAC_SHA512)
- Priv Protocol value (e.g. CFB_AES256)

#### 3.6.5.2 Display SNMP Authentication Failures

Prior to SANnav 2.3.1, during Fabric discovery, SANnav checks if the SNMP account to be used by SANnav exists on the switch.

If the SNMP user does not exist on the switch, SANnav adds it to the switch using SANnav default predefined credentials (not visible to the user).

If the SNMP user already exists on the switch, SANnav does not overwrite the existing configuration using its default predefined credentials on the switch if the SNMP credentials do not match. Because of this mismatch all the SNMP communication fails.

To resolve this issue, SANnav v2.3.1 will first detect if there are SNMP credentials mismatch and if a mismatch is found between the SANnav predefined configuration and the switch, SANnav will overwrite the SNMP configuration on the switch if the SNMP Manual configuration is not selected and a firmware download is not in progress in that switch.

In some cases, the SNMP communication may fail due to the security settings on the switch (SNMP access control and security level). To detect these problems, SANnav will check the SNMP access control and security level when the FOS version on the switch is equal to or higher than 8.2.1b since FOS does not support this for older versions.

#### 3.6.5.3 Restrict SANnav Versions Allowed to Discover Specific FOS Versions

Prior to FOS v9.2.1, FOS allowed SANnav to discover a switch no matter what the SANnav version is. There was no version restriction from FOS to allow SANnav to discover a given switch.

Starting with FOS v9.2.1 and higher, FOS will only allow discovery by only specific SANnav versions. Attempts to discover the switch with a non-supported SANnav version will be denied by FOS v9.2.1 and later.

For example, FOS v9.2.1 can only be discovered by SANnav v2.3.1 or higher.  Attempting to discover FOS v9.2.1 switch with SANnav v2.3.0 or v2.2.2xa will be rejected by FOS v9.2.1. Refer to the *FOS Administration Guide* for more information.

#### 3.6.5.4 More Prominent Message when Deleting a Logical Fabric from SANnav

When deleting a Logical Fabric of any type from SANnav 2.3.1, the user will be shown a more prominent message with a red triangle and an explanation of the side effects of deleting the Logical Fabric from SANnav.

## 3.6.6 Inventory

### 3.6.6.1 Device Port to Device Enclosure Mapping Policy Enhancement

This feature was introduced in SANnav v2.3.0 to define policies to map device ports (host ports and storage ports) to enclosures (hosts and storage) in a stateless and idempotent manner (can be run multiple times and at any time). The policy contains rules to determine this mapping at runtime.

In the menu **SANnav > SAN Monitoring > Inventory Settings** a tab called Host and Storage Naming Policy was introduced in SANnav v2.3.0 to control and manage the device ports to enclosure mapping formation.

In this tab there are four main items:

1. SANnav Automatic Host Enclosure
2. Automatic Storage Enclosure

   – These two items determine whether the SANnav automatic device port-to-enclosure mapping formation should be enabled or not. By default, Host Auto Enclosure is enabled and Auto Storage Enclosure is disabled.

3. Manual Host Naming Policy
4. Manual Storage Naming Policy

   – These two items allow to control how SANnav should determine the mapping between the device ports and their associated container enclosures using specific naming components, such as zone alias, Node Symbolic Name, Port Symbolic Name, etc., and regular expressions (regex grammar) to pick only a certain character from the value of the component.

   – In SANnav v2.3.1, under each item Manual Host Naming Policy and Manual Storage Naming Policy (items 3 and 4 above), a new option menu called Case Conversion with values None, Uppercase, Lowercase is added to control the case of the formed enclosure name.

### 3.6.6.2 Enclosure Map/Unmap REST API Change

Prior to SANnav v2.3.1, when all device ports are removed after performing an unmap from the manual enclosures using a REST call, the empty enclosures were not deleted. However, when this same operation is performed from the SANnav UI, the enclosures are deleted.

With SANnav v2.3.1, after either map or unmap operation through REST URL, empty enclosures will be deleted so that REST and UI operations are consistent in behavior.

### 3.6.6.3 Offline Device Ports and Manual Enclosures

When a device port associated with a manual enclosure goes offline and either tracking is disabled, or changes are accepted, releases prior to SANnav v2.3.1 will remove the association between the device port and the manually formed enclosure. The user must manually re-map the device port to the manual enclosure again when the device port comes back online.

SANnav v2.3.1 stores the mapping between the device port and the manual enclosure in the offline device ports view when the device port goes offline, irrespective of whether the track changes are on or off. When the device port returns online, SANnav v2.3.1 will remove the corresponding offline device port mapping entry, and the device port gets automatically mapped to the manual enclosure present in the offline device port mapping.

This generic enhancement addresses all use cases irrespective of device port connectivity to either a Native Switch or an AG switch.

**NOTE** If a given device port went offline before upgrade and migration to SANnav v2.3.1 and later came back online after the upgrade and migration to 2.3.1 was done, then those ports must be manually remapped after upgrade and migration to SANnav v2.3.1.

## 3.6.7 Zoning

SANnav v2.3.0 offered several enhancements and new features related to effectively managing Zoning. These features may be used whether automation is used to manage Zoning in customer environment or not.

SANnav v2.3.0 Zoning features provided the following key features to manage SAN Zoning effectively:

- Manage up to five Zone DB snapshots of the entire Zone Database of a Fabric in SANnav
- Provide new option to create I-* or *-T Zoning Policy with multiple Principals, as opposed to one peer zone per principal as is the case up to SANnav v2.2.2)
- Enhance Policy-Based Zoning to provide option to only save to Defined Zone Config (no Activation)
- Provide new Zoning System Policy
- Display affected Zone tree entities when deleting Zones or Zone Aliases

SANnav v2.3.1 adds more features and enhancements to the existing Zoning introduced in SANnav v2.3.0 with the enhancements listed in the next subsections.

### 3.6.7.1 Fabric Zone DB Snapshots Enhancements

There are two enhancements implemented for Zone Database snapshots in SANnav v2.3.1.

The first enhancement increases the limit of number of snapshots for a given Fabric from 5 to 20 in SANnav v2.3.1 with the same behavior (oldest snapshot overwritten when limit is reached).

The second enhancement is a behavior change from SANnav v2.3.0 when restoring a zone database snapshot in SANnav v2.3.1 as explained below:

- In SANnav 2.3.0, restoring a snapshot with an effective configuration involves the following two steps:
  1. Disable the effective zone configuration in the fabric
  2. Submit the snapshot content to replace the zone database and activate the zone configuration from the snapshot

This approach could result in momentary traffic disruption due to step 1, as the default zone policies can come into effect between steps 1 and 2.

With SANnav v2.3.1, the Fabric Zone DB snapshot restore operation with the activate option checked will not disable the Fabric's effective zone configuration

**CAUTION** It is strongly recommended to take a snapshot of the Fabric Zoning Database when the Effective and Defined zone configurations are identical, that is when the Defined Zone Configuration is in the *Defined (Copy*) state. If the Defined Configuration is not the same as the Effective, that is in *Defined (Modified)* state, then care must be taken when restoring this snapshot in the future. The Defined Configuration is always used to restore the Effective Configuration in the Fabric no matter its state, Defined (Copy) or, Defined (Modified).

**CAUTION** Users are not allowed to *edit* a Fabric Zoning Database snapshot when restoring the Fabric Zoning Database from an existing snapshot. Restoring the Fabric Zoning Database from a user modified snapshot content (JSON backup file) is not supported and may void support from Broadcom.

### 3.6.7.2 Bulk Deletion of Zone Configurations

When decommissioning large arrays and cleaning up the zone databases for multiple Fabrics, there is a need to be able to delete multiple Zone Configurations in one shot. This has been added in SANnav v2.3.1.

This operation is only supported from the Zone Configuration view (not the Zone Inventory) and only when the seed switch is running FOS version 9.0 or higher.

### 3.6.7.3 Zoning Policy Enhancements

New Zoning preferences were introduced in SANnav v2.3.0 which allowed users to define system wide behavior and choices for managing Fabric Zoning with SANnav. The following five new items are available in SANnav v2.3.0:

- Allow Mixed Zones creation/editing/deletion
- Allow for preferred default zone type on creation (Standard or Peer)
- Allow for preferred Zone Policy default creation Type (I-T, I-*, *-T)
- Zone naming scheme
- Zone Alias naming scheme

With SANnav v2.3.1 for both the zone naming policy and the zone alias naming schemes, a new Case Conversion option menu called Case Conversion with values None, Uppercase, Lowercase is added to control the case of the formed zone alias and/or zone names.

### 3.6.7.4 Import Zone Alias Enhancements (Conflict Resolution)

Importing zone aliases from a CSV file involves creation of new zone aliases and modifying existing zone aliases. The workflow up to SANnav v2.3.0 may lead to unintended behavior at times as conflicts may occur when importing zone aliases that already exist in the fabric zone database.

To resolve this side effect, the Import zone aliases workflow has been changed in SANnav 2.3.1 as follows:

- Allow importing zone aliases that do not exist in the live fabric
- Show conflicting zone aliases and skip importing them and proceed with importing other aliases from the CSV file

When conflicts are detected, a new UI will show the conflicts to the user when importing the CSV file. SANnav will not attempt to merge or resolve conflicts automatically. Instead, the user will have to decide to either skip the conflicts and resolve them through either changing the zone aliases in the fabric zone database using zone alias operations in SANnav (if the zone aliases menu if CSV file is correct) or modify the zone aliases in the CSV file and re-import again (if the zone aliases in fabric zone database are correct)

#### 3.6.7.4.1 Import Aliases into SANnav that Were Exported from Brocade Network Advisor (BNA)

When importing the aliases that are exported from BNA, the import will fail with the following message in SANnav v2.3.1:

```
Importing zone aliases failed. Invalid file header. The header should match
"Member WWN / D,P", "Zone Alias", "Tags", "Description"
```

To import aliases exported from BNA, the BNA exported file must be modified to include the following header (first row in the CSV file exported from BNA) and then proceed with importing the file into SANnav v2.3.1.

```
"Member WWN / D,P", "Zone Alias", "Tags", "Description"
```

### 3.6.7.5 Zoning UI to Bring User Selection in Context

This is a minor usability enhancement where in environments with large zone sets, it is difficult to read the details of a Zone when using the Show Details for a Zone.

In SANnav v2.3.1, the UI for Show Details of a Zone has now been changed to only show the zones selected by the user (and only those) in context. In SANnav v2.3.0, all zones (even the ones not selected by the user) were shown, which caused a usability issue when the list of entities is large

### 3.6.8 Configuration Policy Management

FOS v9.2.0 introduced a new Adaptive Quiet time feature to reduce the number of MAPS violations raised by FOS over a period. Refer to the *FOS 9.2.1 Administration Guide* for more details on this feature.

This feature was not supported in SANnav v2.3.0.

SANnav v2.3.1 supports this feature by introducing a new option to select Adaptive Quiet Time under the Configuration Blocks for Chassis. A new option to select Adaptive Quiet Time is now available.

Note that, the Quiet Time at the Logical Switch level for FOS versions prior to FOS 9.2.0 is still supported. The Configuration Policy Manager feature contains a data model to derive which FOS version supports the new Adaptive Quiet Time and which do not.

## 3.7 Flow Management

SANnav v2.3.1 Flow Management feature introduces more changes on top of existing SANnav v2.3.0 Flow Management feature changes. To keep a holistic picture, a summary of the SANnav v2.3.0 Flow Management changes is introduced in this document.

### 3.7.1 SANnav v2.3.0 Flow Management Summary

SANnav v2.3.0 Flow Management feature has undergone several important changes, specifically:

- Gen 6 collections and associated reports removal
- Flow Management support on large deployment platforms only (no support on small platforms)
- Deprecated Reports (now removed in SANnav v2.3.1)

Gen7 platforms running FOS v9.2.0 and higher can send MAPS rules violated statistics for IO Health and IO Latency categories to SANnav. SANnav receives the violated counts for all different types of flows (IT/ITL/ITN/VITL/VITN).

#### 3.7.1.1 New IO Health and IO Latency Widget

Based on the flow violations streamed to SANnav, a new widget is derived and calculated to determine the device ports that are impacted by violated flows (Initiator Host Ports and Target Storage Ports).

The new widget is available as a dashboard widget which gets updated every five minutes and kept for the last two hours. This widget is meant as a troubleshooting widget to determine (five minutes refresh cycle) which device ports are impacted by violated flows indicating possible traffic issues such as errors, congestion, and/or oversubscription on these ports.

While a fabric scope may be selected for this widget, fabric scope and filter are not honoured in the dashboard widget view.

SANnav v2.3.0 runs an algorithm to determine the severity of the impacted host ports or storage ports as one of the following:

- Severely Degraded
- Degraded
- Marginally Degraded

##### 3.7.1.1.1 Investigate Violated Flows and F-Ports from IO Health and Latency Widget

When the widgets shows the device ports that are impacted by having flows going through them that are violated (severity is one of Severely Degrade, Degraded or Marginally Degraded) it is possible to drill down on the severity bar to view the violated flows.

Upon drill down, a table will show the violated flows and the flow attributes and last sample metrics aggregated over the last two hours. From this table, it is possible to investigate any Flow or to investigate the entry and exit F-ports associated with the flow. With this feature, a user may view the flow metrics and the physical port (F-port) metrics to detect any correlation or relation.

#### 3.7.1.2 Flow Telemetry Chassis Registration

In a customer environment there could be millions of flows going through the fabric at any time. SANnav does not collect flow telemetry statistics through streams of data for all these possible flows.

To manage flow scale which can be quite large, the SANnav user must determine which chassis to receive flows from. *By default, no flow streams are received until the user registers for flow telemetry streaming reception*.

To control and manage which chassis will SANnav receive flow telemetry streams (both flow metrics and flow violated metrics) from, a new menu under **SANnav > SAN Monitoring > Flow Telemetry Registration Management** is introduced. This menu is only available on large platforms as stated earlier.

When invoked, this menu will list all currently managed chassis and whether the Chassis is registered for sending flow telemetry data to SANnav.

The user may select up to 150,000 flows total which is the current flow scale supported and tested/validate in SANnav v2.3.0. When there are more than 150,000 flows registered SANnav will not allow any more chassis registration.

Each type of switch or Director chassis has a specific limit that is platform dependent. Refer to the *FOS v9.2.0 Administration Guide* and the *SANnav v2.3.0 User Guide* for details on supported flows per hardware platform.

**CAUTION** Flow Management is only supported on large platforms (96-GB RAM, 24 vCPUs, 1.2-TB storage). If a SANnav server with a Base license is upgraded to a large platform, then Flow telemetry chassis registration menu will be available, but this configuration has not been tested or validated.

### 3.7.2 SANnav v2.3.1 Flow Management Changes

The following section highlights the changes introduced in SANnav v2.3.1 and FOS v9.2.1 for Flow Management feature.

**ATTENTION** Please consider the following points below for SANnav v2.3.1 Flow Management feature changes

- **SANnav v2.3.1 does not support flows from any Fabric OS release other than Fabric OS v9.2.1.**
  - SANnav v2.3.1 consumes IT flows (only) streams with FOS v9.2.1 (only) at 5 minutes interval.
  - SANnav v2.3.1x no longer consumes ITL/ITN or VITL/VITN flows from any hardware platform.
  - Upgrades and migrations to SANnav v2.3.1 will not migrate previous flow data (including ITL/ITN and VITL/VITN flows). See *Important Considerations When Upgrading to SANnav v2.3.1*.
- FOS 9.2.1 will support IT flows (only, no ITL/ITN or VITL/VITN flows) streaming to SANnav combining IT flow statistics and violations in one *new* consolidated and optimized Kafka data schema.
  - SANnav v2.3.1 Flow Inventory continues to display VM and LUN columns however, they will never be populated.
  - Filters: using filters with LUN or VM values will lead 0 flows as a result. Only IT filters will yield results.

- SANnav v2.3.1 Investigation View for Flows changes include the following:
  - Investigation view for Flows is available for IT Flows only and for FOS v9.2.1 only.
  - Real-time flow investigation view (10-second interval) has been removed as FOS v9.2.1 no longer supports collections, which is required to provide the real-time flow investigation.
  - Six-hour visibility (Inventory and Investigation views for any flow IT/ITL/ITN/VITL/VITN) has been removed.
  - Investigation intervals can either be five minutes (native FOS stream) or one hour (aggregated by SANnav).
- The SANnav IO Health and Latency Flow Widget continues to be available in SANnav v2.3.1, however, it will process and compute affected device ports for IT Flows only (no ITL/ITN/VITL/VITN flows) and for FOS v9.2.1 platforms only.
  - The SANnav IO Health and Latency widget only processes IT flow violations on Gen 7 platforms running FOS v9.2.1 only.
  - The SANnav IO Health and Violation widget is not supported on any Gen 6 platforms for any FOS version.
- Flow scale for SANnav v2.3.1 is 160,000 IT Flows on large platforms.
- With an Enterprise license, Flow Management is only supported on large server configurations (96-GB RAM, 24 vCPUs, 1.2-TB storage).
- The SANnav Northbound streaming for Flow topics have been removed from SANnav v2.3.1.

# 3.8 REST Interfaces

## 3.8.1 REST Interfaces

Two new REST interfaces have been introduced in SANnav v2.3.1.

The first REST interface is a GET URL to obtain the SANnav version information. The structure returned contains the following data as an example:

- "version": "2.3.1"
- "build": "build 1"
- "generatedOn": "12-20-2023"
- "productBrandName" : "SANnav Management Portal"
- "oemName": "BROADCOM"

The second REST interface is also a GET URL to obtain the SANnav security password and lockout settings. The data structure returned by this call is shown below as an example:

- "minimumLength": "8"
- "uppercaseLetters": "0"
- "lowercaseLetters": "0"
- "digits" = "0"
- "specialCharacter": "0"
- "maximumRepeat": "2"
- "maximumSequence": "1"
- "passwordExpires": "true"
- "lockoutAttempts": "3"

- "lockoutDuration": "15"
- "passwordAge": "0"
- "historyCount": "0"
- "warningPeriod": "0"
- "inactiveLockoutTime": "30"
- "dashboardKeepAlive": false

## 3.8.2 Miscellaneous Enhancements

### 3.8.2.1 SANnav Backup Policy and Auto Purge/Delete of SANnav Backups

A New Policy to delete/purge SANnav scheduled backups (currently on demand) is provided in SANnav v2.3.1.Options to retain scheduled backups for 5, 10, or 15 days before purging them is provided.

This new purge schedule applies only to scheduled backups and not manually or on-demand taken backups. Those are excluded from the new purge schedule and is the reason why, after migration, the previous unwanted backups must be removed manually.

The time at which the backup is purged depends on the time at which it was scheduled to be taken with a possible buffer of 30 minutes. For example, if a backup was generated previously by the schedule at 3:00 PM and the purging is scheduled in five days, then the backup will get purged in five days at either 3:00 PM or 3:30 PM. This buffer is randomly added to avoid SANnav having to run all tasks at the same time.

SANnav v2.3.1 backup files will now be assigned to user (UID) **sannavmgr** and group (GID) **sannavmgr** (as opposed to root in previous releases) with Linux permissions 770 (`rwxrwx---`).

**NOTE** The backup files taken prior to SANnav v2.3.1 are upgraded and migrated however, their file permissions are left as is (that is, owned by root). It is the user’s responsibility to manually delete these backup files if they are no longer needed.

### 3.8.2.2 Switch Support Save: Show Clear Reason for Failure

With SANnav v2.3.1, a clear and explicit reason for failure will be shown when taking a switch support from SANnav save fails. There are various reasons why a Switch Support Save might fail from SANnav. This field will provide for additional details.

### 3.8.2.3 SANnav Support Save Simplification

SANnav Support Data collection provided several options when taking a *partial* SANnav Support Data Capture (SSDC) (aka SANnav supportsave) prior to SANnav v2.3.1

With SANnav v2.3.1, users will be able to select either Full or Partial SSDC for one day from the UI. When selecting Partial, the only option available is whether to take an HTTP capture. All other options have been removed. Users will not have the option to select anything if taking the SSDC from the SANnav CLI console.

The name of the Support data collection format is shown below:

```
<SANnav_host_name>-<SMP>-<GUI/CLI>-<Full/Partial>-<Timestamp>.tar.gz
```

#### 3.8.2.3.1 Inclusion of Summary Info in SANnav Support Data Collection (SSDC)

SANnav Support Data will include a summary file for quick and easy debugging by the support team. A file called `sannav-summary.txt` will be generated and will have general, host, memory, network, IP tables and other SANnav details included and present inside the SSDC file.

#### 3.8.2.4 Change High Granular Data Frequency from 2 Seconds to 10 Seconds

With FOS v9.2.1 and higher, the streaming interval of performance stats will change as follows:

- FC port metrics streaming frequency is changed to 10 seconds from the current 2 seconds.
- FCIP Tunnel, FCIP Circuit, Eth port and GigE port streaming is changed to 10 seconds from the current 5 seconds.

The investigation view for scheduled ports will show data points spaced at 10-second intervals instead of 2 seconds in previous releases.

The investigation view for scheduled Tunnels/Circuits will show data points spaced at 10-second intervals instead of 5 seconds in previous releases.

There are no impact or changes on historical port or tunnels/circuits Investigation.

## 3.9 USF-Related SANnav Features

Unified Storage Fabric (USF) is a new capability in FOS v9.2.1 and SANnav v2.3.1, enabling the deployment of IP Storage (IPS) along with Fibre Channel (FC) Storage. IPS services include support for iSCSI, NVMe/TCP, and NAS. It has the advantage of the performance, reliability, and security of the traditional FC SAN while consolidating and simplifying management. Additionally, it leverages the existing investments in FC and IP Networks and enhances the performance and reliability of the IPS.

In the next sections, SANnav enhancements to support IPS Fabric discovery, IPS Fabric creation, and end to end IP device configuration will be explained. In addition, monitoring of IPS Fabric and various other functions within SANnav have been enhanced to support management of IPS Fabric and will be highlighted briefly in this section.

The fundamental principle used in SANnav to fully manage USF and IPS Fabrics has been to ensure that the IPS functionality is seamlessly integrated within existing SANnav paradigms. New paradigms are only introduced in SANnav when required, for example to provision and manage new L2/L3 entities such as VLANs, VRFs, and static routes.

To properly deploy, configure, monitor, and debug end-to-end IP Device connections through an IPS Fabric, a basic understanding of the following IP networking is expected:

- VLAN
- VRF
- IP Routing
- ARP
- LAG
- DHCP
- DNS

Refer to the USF section of the *SANnav Management Portal v2.3.1x User Guide* for more details on this entire feature as well as the *Brocade Fabric OS Administration Guide.* The following sections will only cover a brief introduction and overview of the new features for USF and IPS Fabric management.

### 3.9.1 Hardware Support for IPS

IP Storage Logical Switch is supported in Gen 7 chassis (X7-4 or X7-8) running Fabric OS (FOS) version 9.2.1 with FC64-48 blades.

Ethernet ports are only allowed on FC64-48 blades. However, the E-Ports to establish IPS LS connectivity maybe selected on either FC64-48 or FC64-64 blades or on ports on the core blades (ICL ports can also be used as an E-Port for IP Storage fabric).

The following range of AnyIO ports on the FC64-48 blade with appropriate optics are supported for transitioning to Ethernet ports:

- Ports from 16 to 23
- Ports from 32 to 39
- Ports from 40 to 47

### 3.9.2 IPS Fabric Management in SANnav

IPS Fabric management in SANnav follows the same principles used for FC and FICON Fabric management. There are two ways in which Fabrics can be added to SANnav. The first is through Fabric Discovery (brownfield) and the second is through Logical Fabric creation workflow in SANnav (greenfield).

#### 3.9.2.1 IPS Fabric Discovery (Brownfield Workflow)

The same workflow used to discover a FC or FICON Fabric in SANnav such as an FC Fabric or a FICON Fabric applies for discovering IPS Fabric. There is no change in the input required in the UI to discover an IPS Fabric.

There are two visible changes when the Fabric is discovered successfully. First, a new Logical Role attribute is added to indicate whether the Logical Switch is of type Logical FC or Logical IP (for UPS and IPS Fabrics). Second, a new attribute Type with values (FC or IP) has also added for the Discovered Fabrics view in SANnav.

#### 3.9.2.2 IPS Fabric Creation (Greenfield Workflow)

A new Tab called IP Storage Fabrics in the **SANnav > SAN Configuration > Logical Fabric Management** has been added to initiate the creation/editing/deletion of IPS Fabrics. The workflow to create an IPS Fabric is very similar to that used for creating Logical Fabrics (for FC Fabrics) or FICON Fabrics (for FICON Fabrics).

The most notable difference is the fact that the user needs to specify which AnyIO ports to assign to the IP Logical Switches (IP LS). There are restrictions for IPS creation such that only one IP LS per Chassis is allowed in the SANnav v2.3.1 and FOS v9.2.1 releases along with other restrictions which are described in detail in the USF section of the *SANnav Management Portal User Guide* as well as the *Brocade Fabric OS Administration Guide.*

### 3.9.3 End-to-End IP Device Connectivity Provisioning in SANnav (Day 1)

This section discusses the workflows used in SANnav to configure and provision IP device connectivity through one IPS Fabric.

If an IPS Fabric is deployed in a redundant manner through a second IPS Fabric, then the same steps performed on the first IPS Fabric to provision end-to-end device connectivity must be performed a second time on the second IPS Fabric to achieve redundant end-to-end paths through both IPS Fabrics.

The key and important points to note in this section are detailed and described in the USF section of the *SANnav Management Portal User Guide*. They are summarized below:

- It is highly recommended to use the reference architecture (dual fabric multipath topology).
- While any combination of IP device connectivity is allowed in both FOS v9.2.1 and SANnav v2.3.1, the only *recommended and test/validated* IPS configuration is the topology where IP servers are connected through L3TOR switches to the IPS Fabric and where the IP Storage ports are directly attached/connected to the IPS Fabric.
- It is important to have a topology diagram representing the end-to-end device connectivity drawn before proceeding to the provisioning steps in SANnav. An example is provided in the Getting Started with IP Storage section of the *SANnav Management Portal User Guide.*
- Another important and fundamental aspect in SANnav 2.3.1 and FOS v9.2.1 is that since there is no device name server in FOS v9.2.1 for IP devices (such as iSNS, for example), the device ports discovery by SANnav cannot be performed as is done for traditional FC-connected devices and will require user intervention and data input.

- To provision an end-to-end IP device connectivity requires two parts performed by potentially two different Administrator roles (who may be the same person).
  - The first part is to be performed by the **SAN Administrator** who will provision all aspects in the SAN and IPS Fabric through SANnav (or CLI).
  - The second part is to be performed by a **Network Administrator** responsible for connecting and configuring (through the L3TOR CLI console) the L3TOR switches and LAGs to the IPS Fabric as well as the Host subnets attached behind the L3TOR that need to access IP Storage ports on the other end of the IPS Fabric.
  - This section focuses on the SAN Administration tasks and highlights through remarks or notes the tasks that the **Network Administrator** must perform on the L3TOR switches.

**ATTENTION** When provisioning end-to-end IP Device Connectivity through one fabric (FabricA), if redundancy is required through a second Fabric (FabricB) because the IP devices are redundantly connected through two IPS Fabrics, then the complete provisioning steps described below need to be performed on both FabricA and FabricB in SANnav, one fabric at a time.

### 3.9.3.1 Launch Point to Configure IPS Fabric Device Connectivity

The launch point for all tasks related to IPS end to end device connectivity is under a new menu tab in **SANnav > SAN Configuration > IP Storage Fabric Configuration.**

When this menu is launched, the user lands in the IPS Port Connectivity Tab described below. By default, the first time that this menu is launched, the user must select an IPS Fabric on the right side of the IPS Connectivity table. If no IPS Fabric has been provisioned this table (and other tabs) will be empty.

There are 5 tabs shown when the IP Storage Fabric Configuration menu is launched. The order of provisioning for these tabs follows the standard SANnav paradigm, that is from right to left. The user is expected to navigate from the right-most tab to the left-most tab to properly configure the device connectivity through an IPS Fabric as follows:

1. IPS Port Connectivity tab
2. Connected Subnet tab
3. VRF tab
4. VLAN tab
5. Routing tab

The next subsections will briefly explain the tasks that the user is expected to perform in each tab above.

### 3.9.3.2 IPS Port Connectivity View: Provisioning End Devices in SANnav

Once the **SANnav > SAN Configuration > IP Storage Fabric Configuration** is clicked, the IPS Port Connectivity tab is shown. If the Fabric context has been set before, it is persisted and the last Fabric used is shown. If the Fabric context has not been set before, a specific IPS Fabric scope must be selected.

This IPS Port Connectivity table represents the inventory of all the AnyIO ports attached to the Fabric that are available for IP device connectivity or that are used to interconnect/link/trunk IP LS switches (E-Ports).

These ETH ports have been previously provisioned (during IPS Fabric creation or discovery) as ETH ports. An ETH port is an AnyIO port whose protocol has been configured/provisioned to ETH, indicating that it is used for IP Device connectivity (server or storage). An E-Port belonging to the IPS Fabric is an FC port used to connect to another E-Port in another IP LS in the IPS Fabric.

This table allows operations to properly configure and provision the end devices connected to the IPS Fabric. As mentioned previously, since there is no name server in FOS v9.2.1 and SANnav v2.3.1, the user is expected to provision through this IPS Port Connectivity UI the L3TOR connected to the IPS Fabric as well as the IP Storage Ports directly attached to the IPS Fabric.

The L3TOR is likely connected to the IPS Fabric using a LAG that contains multiple individual links. This LAG object also needs to be provisioned as part of provisioning the L3TOR in SANnav.

In the IPS Connectivity view, an important column is the Configuration Status column. There are a few key values for this state:

- **Available**: means that the Any IO port is not provisioned to have an attached device to it (L3TOR or IP Storage port) and is available to use.
- **Configured**: means all the required objects have been provisioned from SANnav and the IPS Fabric side. It does not mean that the end to end IP device connectivity is working properly.
- **Auto Config**: applies for E-Ports and means that the AnyIO it has been automatically configured to E-Port (for an ISL connection).
- **Partially Configured**: typically applies to LAG objects and is a transient state.
- **Provisioned**: when the Connected Type device has been entered but not the rest of the data (Subnet/VRF/VLAN/static routing).This is also a transient state.

When any row is in the Configured state, it means all the required objects have been provisioned from SANnav and the IPS Fabric side. It does not mean that the end to end IP device connectivity is working properly.

**NOTE** The Network Administrator will also need to provision the L3TOR and LAG in the L3TOR switch.

### 3.9.3.3 Provisioning Connected Subnets

After the IPS device port connectivity (devices, device ports, and LAGS) has been provisioned, the user is expected to provision the subnets.

There are two types of subnets: Intermediate Subnet and Destination Subnets.

In most typical deployments, one Intermediate Subnet is to be created for the L3TOR switch connected via LAGs to the IPS Fabric and as many Destination Subnets as there are host subnet attached to the L3TOR that need to access the storage ports.

For example, if there is one L3TOR switch with two host subnets connected to it, then the following subnets will need to be provisioned so that the hosts in each subnet can be routed to the proper storage ports on the other side of the IPS Fabric:

- One Intermediate Subnet for the storage ports attached directly to the IPS Fabric
- Two Destination Subnets, one for each host subnet attached to the L3TOR

### 3.9.3.4 Provisioning VRF

Once the Subnets have been provisioned, optionally Virtual Routing and Forwarding (VRF) needs to be provisioned. By default, VRF 0 is the default VRF created by FOS.

Unless it is required to partition various independent traffic flows on the same IPS Fabric to segregate the traffic from multiple devices on the same single IPS Fabric, there is no need to provision VRFs. An example would be to use VRF 0 for a certain set of applications and VRF 1 for another set of applications and all traffic is carried over the same IPS Fabric with no interference between traffic on VRF 0 and VRF 1.

If VRF function is required, then up to four VRFs may be provisioned in one single IPS Fabric.

#### 3.9.3.5 Provisioning VLANs

Once the subnets and the optional VRF objects have been created, the next step is to provision the VLANs. There are two types of VLANs objects used, VLAN and Interface VLAN (or Intermediate VLAN).

In most cases, when a set of storage ports directly attached to the IPS Fabric need to communicate to host subnets behind an L3 TOR, then one Interface VLAN and one VLAN would need to be created.

- The VLAN object is to be created for the direct attached devices, most typically, storage ports.
- The Interface VLAN would need to be created for the L3TOR device attached to the Fabric.

Note that the fundamental difference between VLAN and Interface VLAN is that when creating a VLAN object storage port directly attached to the IPS must be specified, while when creating an Interface VLAN, a subnet or a link must be added instead of ports.

**NOTE** The Network Administrator will also need to provision the VLAN objects on the L3TOR switch.

#### 3.9.3.6 Provisioning Static Routing

Once the VLAN objects have been created, the last and final step is to specify the static route for the storage ports to reach the host subnets behind the L3 TOR switch.

From SANnav, one static route per host subnet behind the L3TOR needs to be created. So, with the example of two storage ports directly connected to the IPS Fabric and two host subnets behind the L3TOR switch, two static routes need to be provisioned:

1. One static route for the storage ports to reach the first host subnet
2. One static route for the storage ports to reach the second host subnet

**NOTE** The static route provisioned in SANnav is a one way static route, that is, from the storage ports to the host subnets behind the TOR. The route from each of the host subnets behind the L3TOR to the storage ports needs to be configured by the Network Administrator on the L3TOR.

#### 3.9.3.7 Exporting a Complete IPS Device Connectivity End-to-End

Once all the provisioning on the SANnav has been performed (all five tabs have been fully completed) it is important to go back to the IPS Port Connectivity tab to Export the complete IPS end-to-end device connectivity. This export function is not like an Inventory Export where only the data in the inventory being viewed is exported. Here, all data is exported including IPS Port Connectivity but also subnets, VRFs, VLANs, and static routes.

This feature is useful to get a complete end-to-end view of each IPS Fabric port and what is connected to it. The SAN Administrator may then exchange this file with the Network Administrator to make sure all data is consistent and matches on the L3TOR side. Note that the reverse can occur as well. That is, the Network Administrator provides to the SAN Administrator the Host Subnets, LAGs, VLANs and static routes configured from IP side so that the SAN Administrator configures the SAN portion accordingly.

**NOTE** When all the provisioning steps above have been completed, the column Configuration Status in the IPS Connectivity view should be set to Configured state. Troubleshooting end-to-end IP device connectivity

In SANnav v2.3.1, there are no features to troubleshoot IP Device end-to-end connectivity such as `ping` or other means. FOS v9.2.2 CLI however provides a set of commands to do so. Since these commands are interactive, it is not recommended to use SANnav switch CLI to send those. Instead SSH to the FOS switch to run these commands directly.

## 3.9.4 Day 2 Provisioning Use Cases for IP Device Connectivity

The Day 1 operations described above are to be performed for the initial setup for IP device connectivity and involves **Creation** of multiple objects in SANnav and FOS.

The Day 2 activities and typical use cases involve application life cycle management operations on the objects created in Day 1. Typical operations involve editing of these objects from SANnav and to FOS.

There are four use cases for Day 2 as explained below.

### 3.9.4.1 Add Storage Ports to an Existing End-to-End Connection

As is the case for SAN zoning, it may be required to add storage ports due to an existing zone in FC for better performance and to scale the application. The same is true for IPS device ports, it may be required to add more storage ports to an existing end-to-end application.

The SAN Administrator configures any IO port as direct-attached storage in the IPS Port Connectivity view and add the port to the storage VLAN in the SANnav VLAN tab. There is no need to add a new static route. There is nothing for the Network Administrator to do.

### 3.9.4.2 Add a New Server under an Existing Host Subnet

It may be required to add a new server under a host subnet to access the same storage already provisioned Day 1. To add a new host inside an existing Host subnet, there is nothing to do if the subnet has available IP addresses. If the host subnet has a CIDR of 24, up to 255 hosts IP addresses can be added in the subnet.

The Network Administrator configures the IP address of the host to be added to an available one. There is nothing for the SAN Administrator to do.

### 3.9.4.3 Add a New Storage Subnet Connected to the IPS Fabric

If either the maximum number of storage ports in a subnet limit is reached or if it is required to manage different storage subnets, then it may be required to create a new subnet for storage.

In this case, the Storage Administrator follows the same steps described to provision the storage ports in Day 1 activities. There is no need to add new static routes by the SAN Administrator. The Network Administrator will need to add a new static route on the L3TOR to reach the newly added storage subnet.

### 3.9.4.4 Add a New Host Subnet Connected to the L3TOR Switch

In some cases, if the number of hosts exceeded the number of allowed hosts, and new hosts need to access the storage ports already configured in Day 1, it may be required add a new host subnet behind the L3TOR switch in SANnav and define (add) a new static route for the storage VLAN ports to reach new host subnet.

In this case, both the SAN Administrator and the Network Administrator perform tasks. The SAN Administrator defines a static route to reach storage VLAN for the new host subnet. The Network Administrator configures a new host subnet behind the L3TOR switch and define a new static route for the new host subnet to reach the existing storage subnet.

### 3.9.4.5 Add Links to an Existing LAG between the L3TOR Switch and the IPS Fabric

With scale and many devices connected, congestion between the L3TOR switch and the IPS Fabric may occur.

In this case, it may be required to add more links to LAG between the L3TOR and the IP LS created on Day 1. In this case, both the SAN Administrator and the Network Administrator need to perform tasks to add ports to the LAG on each of their respective end. In SANnav, the SAN Administrator can simply invoke **Add Port(s) to LAG** from the IPS Port Connectivity view on any port already part of the LAG created in Day 1.

#### 3.9.4.6 Other Use Cases for Day 2

There are other use cases for Day 2 operations. Refer to the *SANnav Management Portal v2.3.1x User Guide* for details on how to achieve these use cases in the SANnav UI:

- Removing storage ports from a VLAN (operations by SAN Administrator only)
- Removing a server from a host subnet (operations by Network Administrator only)
- Removing an entire host subnet behind the L3TOR (operations by both SAN Administrator and the Network Administrator)
- Removing ports from a LAG (operations by both SAN Administrator and the Network Administrator)

### 3.9.5 Topology Contexts for IPS Fabrics

The following topology contexts are supported for IPS Fabric and USF:

- IPS Fabric context
- IP LS Switch context

Viewing any of these contexts will display appropriate IPS topology. Assuming the user has properly created or discovered the fabric and provisioned end to end IP device connectivity correctly, then the topology will reflect device connectivity through the IPS Fabric.

There are new icons and badges in topology for IPS Fabric and IP LS switch contexts. Key ones to mention here are the Subnet icons to represent the host subnets behind a L3TOR, L3TOR switch, L2TOR switch and a few others. Refer to the *SANnav Management Portal v2.3.1x User Guide* for details.

**ATTENTION** SANnav v2.3.1 does not support IP Hosts or IP Storage as a context, therefore it is not possible to display redundant and resilient host subnets connected to two fabrics with storage ports on the other side in topology as can be done for traditional FC devices.

### 3.9.6 CLI-Based Discovery of IP Devices (Not Recommended)

This approach is like the IPS Fabric Discovery brownfield approach, but instead applied for device connectivity discovery. In this approach, the user has provisioned using FOS CLI all required entities such as subnets, VRFs, VLANs, and static routes.

SANnav will then discover automatically (no action required) all the IPS objects created and will add them to the associated tabs.

The Configuration State status of the ISP Port Connectivity view will be a key column to pay attention to in these cases. To complete the end-to-end provisioning and view a consumable SANnav topology, the user will likely have to complete the provisioning steps in SANnav. This is the reason why this approach is not recommended although it is supported.

### 3.9.7 Investigating Any IO (ETH) Ports

AnyIO ports, whether configured as ETH ports or as E-Ports, can be investigated from the SANnav Switch Port Inventory view like any other standard fabric port. The following metrics are shown for AnyIO ports configured as ETH:

- Tx Utilization (MB/sec)
- Rx Utilization (MB/sec)
- Tx Utilization %
- Rx Utilization %

### 3.9.8 IPS Dashboards and Reports

There are no new dashboard widgets or reports for IPS in SANnav v2.3.1.

However, the existing Fabrics status widget for reports and dashboards has been modified to add the Type of Fabric (FC vs IP).

Similarly, for the Switches status widget, a new column has been added called Logical Role with values Logical FC (for FC LS) or Logical IP (for IP LS switch).

## 3.10 Features Deprecated with SANnav Management Portal v2.3.1

The following features are deprecated in SANnav v2.3.1. *Deprecated* in this context means that the feature is still available on SANnav v2.3.0, however the feature will be *removed* in a future release.

- The feature under the menu **SANnav > SAN Monitoring > MAPS Policy Management** has been *deprecated* in SANnav v2.3.0 and continues to be in the *deprecated* state for SANnav v2.3.1.
- TACACS+ server as an authentication mechanism is *deprecated* with SANnav v2.3.1. It will be removed in a future release of SANnav. Customers currently using TACACS+ as an authentication mechanism are highly encouraged to migrate to a different authentication scheme.

  **NOTE** TACACS+ authentication to the switches has also been deprecated with FOS v9.2.1.

## 3.11 Features Removed from SANnav Management Portal v2.3.1

The following features are no longer available with SANnav v2.3.1:

- Launching Web Tools using SANnav user's credentials was *deprecated* in SANnav v2.3.0 and is now *removed* with SANnav v2.3.1.
- Inventory Search REST Interface (end point `/external-api/v1/inventory/search`) has been removed. Instead use other available REST interfaces to search using filter and scope. Refer to the *SANnav REST API Reference Guide*.
- The SANnav Northbound streaming for Flow topics have been *removed*.
  - Other topics (Ports, Tunnel/Circuit, and Switch) continue to be supported and will likely be *deprecated* or *removed* in a future release.
- Real-time investigation of Flows at 10-second intervals has been *removed* form FOS v9.2.1 as well as from SANnav v2.3.1.
- Investigation at interval of 6 hours has been *removed* in SANnav v2.3.1 since there are no longer ITL/VITL flows in SANnav v2.3.1.
  - Only IT Flows may be investigated at either 5 minutes (native stream) or 1 hour (aggregated).
- Flow Management is no longer supported on small platforms for SANnav v2.3.x
- The following nine Flow-related Reports were *deprecated* with SANnav MP v2.3.0 and are now *removed* with SANnav v2.3.1:
  - Time Series – Flows
  - Top Flows – IO Exceptions
  - Top Flows – Other (non-Read/Write) commands
  - Top Host Port Pending IOs

  - Top Storage Port  Pending IOs
  - Top Storage Port Data Rate
  - Top Storage Port ECT
  - Top Storage Port FRT
  - Top Storage Port IOPS

- The SNMP MIB Foundry attribute with `Vendor Id 1991` was used for authorization by releases of SANnav before v2.3.1. In SANnav 2.3.1, support for the Foundry attribute on the RADIUS server has been removed. Customers using this specific attribute should change their RADIUS server dictionary file typically called `dictionary.NM_AAA_dictionary` to use the Brocade attribute with `Vendor Id 1588` and the attribute sequence number to `1` or any other unique number, for RADIUS authorization instead. An example is shown below for illustration, the changes to be made are shown in blue:

```
# -*- text -*-

#

#  dictionary.Brocade

#

VENDOR         Brocade  1588

BEGIN-VENDOR   Brocade

ATTRIBUTE      NM-Roles-AORs-List  1  string.

END-VENDOR     Brocade
```

Save and close the RADIUS server dictionary file. Restart the RADIUS server.

**NOTE** If Attribute sequence number `1` is already used for the other attribute for `Vendor Id 1588`, change the attribute sequence number to any unique number.

## 3.12 Important Considerations When Upgrading to SANnav v2.3.1

This section highlights key points to consider during upgrade and migration from previous releases of SANnav MP to SANnav MP v2.3.1.

If these considerations are a concern, then customers are advised to stay on the previous release (i.e., SANnav v2.2.2x or SANnav v2.3.0) and to not upgrade/migrate to SANnav v2.3.1.

Refer to the Features Affected by Upgrade and Migration section of the *SANnav Management Portal v2.3.1x User Guide* for more details on behavior changes and considerations during the upgrade and migration to SANnav v2.3.1.

### 3.12.1 Flow Management

- Upgrade and Migration to SANnav v2.3.1 will not migrate previous flow data (including ITL and VITL flow data)

**ATTENTION** Customers wishing to keep previous SANnav releases flow data (especially ITL/ITN and VITL/VITN) must remain on previous SANnav versions (v2.3.0 or v2.2.2x) and should not upgrade to SANnav v2.3.1.

- Backing up a SANnav instance on a large platform and restoring it on a small platform running SANnav v2.3.x is not recommended. The flow data will not be migrated on the small SANnav v2.3.x platform as flow management is not supported on small platforms.

# 3.13 SANnav Management Portal v2.3.0 Supported SAN Switches

## 3.13.1 Platform Support and FOS Support – New Policy

Starting with SANnav v2.3.x, support for various SAN hardware platforms and FOS versions will be reduced.

This affects support for SANnav customers as follows:

- An end user reports an issue on an unsupported hardware platform and/or unsupported FOS release.
- To receive support, the end user must reproduce the issue with a supported hardware platform and/or FOS version.

End users should upgrade to supported hardware platforms and/or FOS versions configurations before deploying SANnav MP v2.3.1.

### 3.13.1.1 Hardware Platforms and FOS Support Matrix

The officially supported matrix of supported hardware platforms and FOS versions is listed in the table below. Note that no Gen4 platform is officially supported with SANnav v2.3.0. SANnav will continue to recognize and discover/manage these no longer supported platforms, however, support may be limited in some cases.

**NOTE** Switches running unsupported FOS versions (such as FOS v7.4.x or any FOS v8.x non target path releases) may be managed by SANnav, however, issues specific to those FOS firmware versions will not be addressed by Broadcom.

| Switch Type | Hardware Model | FOS Version(s) Supported* |
|---|---|---|
| Gen 7 Switches | ▪ Brocade G720<br>▪ Brocade G730<br>▪ Brocade X7-4<br>▪ Brocade X7-8<br>▪ Brocade 7850 | ▪ FOS v9.0.1e1 and later<br>▪ FOS v9.1.1c and later<br>▪ FOS v9.2.0a and later<br>▪ FOS v9.2.1 |
| Gen 6 Switches | ▪ Brocade G610<br>▪ Brocade G620<br>▪ Brocade G620 (switchType 183)<br>▪ Brocade G630<br>▪ Brocade G630 (switchType 184)<br>▪ Brocade 7810 Extension Switch<br>▪ Brocade X6-4<br>▪ Brocade X6-8<br>▪ Brocade MXG610s Blade Server SAN I/O Module<br>▪ Brocade G648 | ▪ FOS v9.0.1e1 and later<br>▪ FOS v9.1.1c and later<br>▪ FOS v9.2.0a and later<br>▪ FOS v9.2.1 |

| | | |
|---|---|---|
| Gen 5 Switches | Brocade 7840 Extension Switch<br>Brocade DCX 8510-4<br>Brocade DCX 8510-8<br>Brocade 6505<br>Brocade 6510<br>Brocade 6520<br>Brocade M6505 Blade Server SAN I/O module<br>Brocade 6542 Blade Server SAN I/O module<br>Brocade 6543 Blade Server SAN I/O module<br>Brocade 6547 Blade Server SAN I/O module<br>Brocade 6548 Blade Server SAN I/O module<br>Brocade 6558 Blade Server SAN I/O module | FOS v8.2.3d and later |

*Not all FOS versions listed in this column are supported on all hardware model platforms. Refer to the FOS and SANnav User Guide for details of which FOS version is supported by which platform.

- For new Gen7 hardware models (7850) only FOS v9.2.0 is supported.

# Chapter 4: Brocade SANnav Management Portal Deployment

## 4.1 Server Requirements

SANnav Management Portal v2.3.1 can be deployed either on a single bare-metal host, virtual machine (VM) or as an Open Virtual Appliance (OVA). The following two tables provide details of server requirements in each case.

### VM and Bare Metal Deployments

| Maximum Switch Ports Under Management (Base or Enterprise) | Operating System | Host Type | Minimum vCPU | Memory | Hard Disk |
|---|---|---|---|---|---|
| *Small*<br>600 Ports (Base) or<br>3000 (Enterprise) | RHEL 8.8, 9.2 | Bare metal or VMware ESX 8.0 VM<br>Bare metal/HyperV Windows Server 2022 VM | 16 vCPUs | 48 GB | 600 GB |
| *Large*<br>15,000 (Enterprise) | RHEL 8.8, 9.2 | Bare metal or VMware ESXi 8.0 VM<br>Bare metal/HyperV Windows Server 2022 VM | 24 vCPUs | 96 GB | 1.2 TB |

- RHEL 8.2, 8.3, 8.5, 8.6, 8.7, 8.9, 9.3 are not officially supported but installation and running SANnav on these versions is allowed upon user acceptance with conditional support.
- RHEL 8.0, 8.1, 9.0 and 9.1 are not supported; the installation script exits if RHEL 8.0/8.1 or 9.0/9.1 are running on the SANnav host.
- ESXi 8.0 is recommended. SANnav v2.3.x has not been validated with ESXi 7.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 2.

### OVA Deployments

| Maximum Switch Ports Under Management (Base or Enterprise) | Supported Hypervisor | Host Type | Minimum vCPU | Memory | Hard Disk |
|---|---|---|---|---|---|
| *Small*<br>600 Ports (Base) or<br>3000 (Enterprise) | VMware ESXi 8.0 | VMware ESXi VM | 16 vCPUs | 48 GB | 600 GB |
| *Large*<br>15,000 (Enterprise) | VMware ESXi 8.0 | VMware ESXi VM | 24 vCPUs | 96 GB | 1.2 TB |

- SANnav MP v2.3.1 OVA packages Rocky Linux 8.8 in the .ova file
- ESXi 8.0 is recommended. SANnav v2.3.x has not been validated with ESXi 7.x but installation should work.
- The OVA deployment allows user 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 2.

## 4.2 Client Requirements

The latest versions of the following web browsers are supported for a SANnav Management Portal v2.3.1 client:

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

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

## 4.3 Software Upgrade

Refer to the Upgrade and Migration Overview section of the *Brocade SANnav Management Portal v2.3.1x Installation and Migration Guide* for complete details. The following Upgrade and Migration Paths to SANnav v2.3.1 are supported:

| Current Version | New Version | Supported? | Comments |
|---|---|---|---|
| SANnav v2.1.x and earlier | SANnav v2.3.1 | No | Support only N-1 upgrades.<br>N=3 for SANnav v2.3.x |
| SANnav 2.2.1x | SANnav v2.3.1 | No | Upgrade and migrate to SANnav v2.3.0 first. 2.2.1x is over a year ago and therefore not valid upgrade path as per Brocade policy. |
| SANnav 2.2.2x | SANnav v2.3.1 | Yes | OVA requires full extraction (OS change) |
| SANnav v2.3.0 | SANnav v2.3.1 | Yes | OVA upgrade inline |

- SANnav v2.2.2.x to SANnav v2.3.1 OVA upgrade/migration requires full extraction of the OVA and upgrade/migration due to disruptive OS change (CentOS 7.9 > Rocky 8.8)
- Refer to the *SANnav Installation and Upgrade Guide* for details before attempting SANnav MP upgrade in all deployments.

**NOTE** SANnav v2.3.1 will autodetect the source version running and will prompt the user to proceed with the upgrade/migration on the detected path or to change the path instead.

### 4.3.1 Environments Running CentOS or RHEL7.9

SANnav v2.3.x does not support installation on Centos 7.9 or RHEL 7.9.

Since there is no direct way to upgrade the operating system to a SANnav v2.3.x-supported OS (RHEL 8.8 or 9.2), the following steps for upgrading/migrating to SANnav v2.3.x should be followed:

- Take a backup of source SANnav version (e.g. v2.2.2x).
- Perform a clean and fresh installation of SANnav v2.2.2x on a VM running a supported RHEL version supported by both source and target (e.g. SANnav v2.3.1 on RHEL 8.8).
- Restore the backup taken previously
- Rehost the SANnav license if required (if the server has a new MAC address).
- Perform the upgrade/migration to SANnav v2.3.1.

# Chapter 5: Licensing

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 directors (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 purchased. The SANnav Management Portal license must be renewed and installed in a timely manner to keep the product functioning without disruption.

## 5.1 Removal of Trial Period

SANnav Management Portal v2.3.x no longer provides a trial period built into the product, which allows the product to be used for a specific duration from the day of installation, without requiring a license.

Customers wanting to trial the SANnav product may do so with previous versions of SANnav as follows:

- SANnav v2.2.1.x and v2.2.2.x have a 30-day trial period embedded.

## 5.2 Removal of 30-Day Grace Period (Available after License Expiration)

The SANnav Management Portal license 30-day grace period (available after license expiration) is now removed in SANnav v2.3.x.

With SANnav v2.3.x, when the license expires, the functionality will be restricted following the expiration date. A user will no longer be allowed to login to the server from the UI.

The SANnav server will continue to run and monitor the environment, but the UI will not be available except for the ability to install a new license.

## 5.3 New License File Expiration Date

Beginning with SANnav v2.3.x, the SANnav license file (`license.xml`) must be applied to the SANnav server within 30 days of creation of the SANnav license file.

- This 30-day expiration is completely independent of the SANnav subscription expiration date.

Refer to the Licensing section of the *SANnav Management Portal v2.3x User Guide* for details on how to regenerate the SANnav license file (XML file) and how to apply it to the SANnav server should this happen.

## 5.4 Export Renewal Request

With SANnav v2.3.x, a user may export (download) any valid SANnav License information into a local client file. This helps customers and OEMs with ordering a SANnav license renewal for the current license.

User may export the current Active, Active (Released) or Expired SANnav license details to renew the current license.

The Export Renewal Request menu will show the following:

- Current License Expiration Date
- Renewal License Start Date (one day after the current expiration)
- Renewal License End Date: by default, this is set to one year after the Renewal Start Date, but the user can change it to any arbitrary date in the future (duration must be between 60 Days and seven years).
  - SANnav calculates the number of days between the start and end renewal dates in days (renewal end – renewal start, expressed in days)
- The Export Renewal Request will download and generate a file (on the client specified browser default Download Folder) containing all the relevant information for the customer to request the renewal quote.
- SANnav will generate a new SRV (SANnav Renewal Verification) Code as part of the Export Renewal Request to be used when placing an order for a license renewal.
  - Example SRV Code - SRVS999D0777FMX12345

Refer to the Licensing section of the *SANnav Management Portal v2.3.x User Guide* for details on how to export the License Renewal Request file from the SANnav UI.

# Chapter 6: Scalability

## 6.1 SANnav Management Portal v2.3.1 Scalability

| 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 **Hosts managed through vCenter** discovery (***across all vCenter instances***) | 200 | |
| Maximum number of **events** stored | 2 million | |
| Maximum number of **MAPS violations** stored | 2 million | |
| **Port statistics** stored | 5-minute samples are stored for up to 30 days.<br>1-hour data is stored for 30 days.<br>1-day aggregated data is stored for 30 days.<br>10-second samples are collected for up to 3 days for a maximum of 100 user-selected Gen 6 or Gen 7 ports. These ports can be on the same switch or across multiple Gen 6 or Gen 7 switches. Data is retained for 14 days. | |
| **Extension Tunnel Statistics** stored | 5-minute samples are stored for up to 30 days.<br>1-hour data is stored for 30 days.<br>1-day aggregated data is stored for 30 days.<br>10-second samples are collected for up to three days for a maximum of 100 circuits (only supported for the SX6 Blade and 7810 switch). These circuits can be on the same switch or across multiple switches. 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<br>Up to 160,000 IT Flows (only IT Flows) maximum allowed (not blocked). Blocked > 160,000 flows.<br>Note: Six-hour investigation removed and no ITL/ITN/VITL/VITN flows in SANnav v2.3.1. No migration of flows to SANnav v2.3.1 from any other previous release | |
| **Flow statistics** stored | 5-minute samples are stored for up to seven days.<br>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 | |

# 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 100ms, then communication time-outs may occur and cause undesirable behaviour.
- When configuring the VM for SANnav installation, make sure the MTU size of the network interface is set to 1500, otherwise SANnav will not receive Port Performance data for switches running Fabric OS less than v8.2.1b.
- Cockpit web console for Linux cannot co-exist with SANnav Management Portal.
- SE Linux is not supported (Enforcing and Permissive).
- 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 application idle time.
- Disaster Recovery (DR) is supported for SANnav Management Portal only. DR is not supported for Global View.
- 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 nginx forcing the session timeout.

## 7.2 Infrastructure, Installation, and Migration

- Migration from SANnav v2.2.2x or v2.3.0 to v2.3.1 will fail when at least one of the following conditions are encountered:
  1. In SANnav versions prior to v2.2.1, SANnav docker home path was customized to something other than the default path of `/var/lib`, then later upgraded to 2.2.1 or 2.2.2x or 2.3.0 with this customized path, and then migration to v2.3.1 was attempted.
  2. Backup from a SANnav server having a different docker home path than the current SANnav server is restored and then migration to v2.3.1 is attempted e.g. backup from an OVA (which has default docker home path) is restored on a server with custom docker home path.

  Please refer to the TSB TSB-2024-291-A for more information including the workaround and recovery.
- SANnav uses a set of ports for internal communication which is available in the SANnav Management Portal Installation and Migration Guide. Please do not use those ports while customizing the SCP/SFTP server, SNMP trap, Syslog/Secure Syslog, or HTTPS communication. Doing so will result in the SANnav server not starting properly.

- Firewalld Backend **Configuration**:
  - When RHEL OS boots, the firewalld backend defaults to using nftables instead of iptables. The current version of Docker used by the SANnav Management Portal server does not have native support for nftables. Therefore, it is mandatory to change the firewall backend to use iptables instead of nftables. Follow the steps below to configure firewalld for this purpose:
    1. Disable `masquerade`
       - Ensure `masquerade` is turned off in the firewalld configuration using the following command:

         ```
         firewall-cmd --zone=<Active Zone Details> --remove-masquerade –
         permanent
         ```

         Where **<Active Zone Details>** is listed in the output of the command `firewall-cmd --list-all`.
    2. Change the firewall backend
       - Stop the firewalld using the command `systemctl stop firewalld`.
       - Edit the firewalld configuration using the command `vi /etc/firewalld/firewalld.conf` and change the `FirewallBackend=nftables` to `FirewallBackend=iptables`.
       - Start the firewalld using the command `systemctl start firewalld`.
       - Reload the firewalld using the command `firewall-cmd --reload`.
- When installing SANnav Management Portal v2.3.x and the firewall needs to be enabled, ensure the firewalld is configured before SANnav Management Portal installation. If the step to configure the firewall is missed or omitted before starting the SANnav Management Portal server, fabric, and switch discovery in SANnav Management Portal will fail (network reachability issue). If this happens, use the following procedure to resolve the network reachability issue:
  - Stop the SANnav Management Portal server using the script stop-sannav.sh present in <install_home>/bin folder.
  - Stop the Docker using the command systemctl stop docker.
  - Follow the firewalld configuration procedure as per the Firewalld Backend Configuration important note.
  - Start the Docker using the command systemctl start docker.
  - Start the SANnav GV server using the script start-sannav.sh present in <install_home>/bin folder.
- If the host on which the SANnav server is installed is rebooted and the firewall was enabled in that host, then the reboot will clear the firewall rules added by SANnav during installation. It is mandatory to run the command below before restarting the SANnav server to re-insert all the missing firewall rules:

  ```
  systemctl restart sannaviptablesetup.service
  ```
- When migrating from previous releases to SANnav v2.3.1, if a custom port is used for internal SFTP/SCP, make sure that this port is not part of the required ports list in the installation guide. If the custom port is in the required ports list, change this port to any other free port using the `change-internal-ssh-port.sh` script before starting the migration.
- SANnav product is designed to use `firewalld/iptables` to block external access to ports used for internal communications. If `firewalld/iptables` is not used, internally used ports will be exposed and may be reported as vulnerable by security scanning software. This note covers all SANnav versions and CSI patches.
- When upgrading to SANnav Management Portal v2.3.1 it is recommended that you take a backup of the current SANnav installation and generate a full support data collection before proceeding with the migration process.

- Before upgrading to SANnav v2.3.1 OVA when FIPS is enabled in the VM and the openSSL is running non-FIPS complaint version then upgrade to SANnav 2.3.1 will fail. In order to fix the problem upgrade the openSSL version in the VM to a FIPS complaint version or disable FIPS before SANnav upgrade.
- When upgrading to SANnav v2.3.1, SANnav may be using TLS v1.2. Switches that are using TLS v1.3 and are configured to use the default-strong *seccryptocfg* template cannot be discovered in SANnav. In this situation, you must configure SANnav to use TLSv1.3 as follows:
  - Stop SANnav by running the following script: <install_home>/bin/stop-sannav.sh
  - Go to the <install_home>/conf folder and edit the server.properties file. Change the tls.protocol.version property from TLSv1.2 to TLSv1.3.
  - Start SANnav by running the following script: <install_home>/bin/start-sannav.sh
  - Wait a minimum of 45 minutes for the SANnav server start-up to complete one round of discovery asset collection.
  - After 45 minutes, the status of the switch configured with default-strong seccryptocfg template should be changed to Discovered.

## 7.3 Firmware Management and Support Save

- A switch Supportsave or firmware download operation initiated via SCP or SFTP protocol from SANnav Management Portal will fail in the following scenario for switches running Fabric OS less than v9.0:
  1. User has performed a switch Supportsave or a firmware download operation at least once on that switch using SANnav Management Portal.
  2. User has uninstalled SANnav Management Portal.
  3. User has re-installed SANnav Management Portal and attempted to either perform a switch Supportsave or a firmware download for the same switch that was used in step 1.
     - To avoid this situation, before uninstalling SANnav Management Portal, take a backup of the `ssh-keypair.ser` file from the following location: `<SANnav_home>/conf/security`. After reinstalling SANnav, restore the previously backed-up file to the same location.
     - To recover from this situation, log in to the switch on which the firmware download or Supportsave was performed, and delete the SANnav Management Portal server IP address from the list of known hosts by using the following command:

       ```
       sshutil delknownhost <SANnav-server-IP>
       ```
- Importing a Fabric OS software package into the SANnav Management Portal repository will fail if the firmware package is stored on a network shared folder. The workaround for this situation is to download the firmware package to a local disk on the SANnav Management Portal server, and then import it into the repository.
- SANnav supports only strong ciphers and if switch configuration supports only weak ciphers, firmware download will not work from SANnav. Please contact Broadcom support for a workaround in case user is willing to use weak ciphers.
- Updated firmware might not show in the SANnav when one or more ports in the fabric are *bouncing*. Fix the issue to see the new firmware details in SANnav.
- SANnav has a limit of two switches for on-demand Supportsave collection if using an internal SCP/SFTP server. If more than two switches are selected in bulk, it may take a long time to complete the Supportsave collection (with internal SCP/SFTP server).
  - To work around this issue, either select only two switches at a time with an internal SCP/SFTP server or use an external SCP/SFTP server which has no switch limit.
  - Additionally, if a switch Supportsave is scheduled using the Bulk Select option, the operation may fail for some of the switches. The workaround is to use an external SCP/SFTP server, which has no switch limit.

## 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.
- A switch will become *Unreachable* after upgrading its firmware to FOS v9.2.0 or above when it was previously discovered with HTTP protocol in SANnav. To work around this, before upgrading the switch FOS firmware, configure the switch either with self-signed generated HTTPS certificate or load the custom certificate in the switch.
- 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 DSA algorithm is used for the HTTPS certificate, then SANnav cannot discover the switch because all the supported ciphers for this algorithm are no longer supported.

## 7.5 SANnav Backup, Disaster Recovery and Support Data Collection

- When SANnav Management Portal server is restored from a SANnav Management Portal backup or when performing a Disaster Recovery fail over, high granularity performance data, FCIP performance data, and flow statistics and violations are no longer collected due to a new HTTPS digital certificate that is generated in the server, which does not match with the digital HTTPS certificates on the switches.
  - To resolve this issue, un-monitor and monitor all data-streaming switches. This will update the certificates on the switches with the new certificate on the SANnav server.
- When SANnav Management Portal support data file size is greater than 5 GB, it is recommended to copy the file directly from the SANnav server rather than trying to download it using the client.
- Backups taken from a CLI script cannot be used for restoring the data. Users are required to always collect SANnav backups through the SANnav client.
- SANnav Backup generated on *large* (96GB) platform cannot be restored on *small* (48GB) platforms.
- When collecting support data collection when SANnav services are down it is recommended to use the CLI option. Running the SANnav support data collection from the Linux server machine console run at the system level console and all the system commands could be executed there to collect the required logs and data which is not possible with the UI option.
- If any of the backup files are moved, renamed, or deleted manually from the file system then SANnav will not show these files in the Outputs page.

## 7.6 SANnav Telemetry Registration with FOS

Switch telemetry configuration and profile registration is required for the switch to stream switch, port, tunnels/circuits, and flow performance data.

Use option 4 in the script `troubleshooting-sannav.sh` present in the `<SANnav-Home>/ /Portal_2.3.1_bld124/bin` folder to troubleshoot the telemetry registration issue. User can provide a comma-separated list of IP addresses of switches that are currently monitored by SANnav. This test will report Switch Telemetry Diagnostics, which will test for following:

1. Validate the ports (Firewall check on the SANnav server for the telemetry required ports)
2. Validate whether the switch supports data streaming
3. Validate the switch is bound to this SANnav Server
4. Validate the switch CA Root certificate
5. Validate Telemetry configurations and profiles.

After running the tests, if any of the test result is `Not Ok`, then there is an issue with Telemetry registration for the switch and the switch will fail to stream data. In this case, SANnav will not show switch, port, and flow stats. If the issue cannot be fixed then contact Brocade support to fix the issue.

## 7.7 SNMP and Syslog Registration with FOS

SNMP and Syslog configuration is required for the switch to send Traps/Informs/Syslog events and to collect switch, port, and tunnel performance data for switches running FOS versions that do not support streaming.

Use option 4 in the script `troubleshooting-sannav.sh` present in `<SANNAV-Home>/ /Portal_2.3.1_bld124/bin` folder to troubleshoot the SNMP and Syslog. User can provide a comma separated list of IP addresses (maximum 10) of switches that are currently monitored by SANnav. This test will report SNMP and Syslog Diagnostics, which will test for following:

1. Validate SNMP Trap Port (Firewall check on the SANnav server for the port 162 or Custom port)
2. Validate SNMP Trap Target Properties (SNMP user/settings)
3. Validate SNMP Security Level
4. Validate Retrieval of Agent's SNMP Engine ID
5. Validate SNMP GET request
6. Validate SNMP Access Control
7. Send and validate test trap
8. Validate syslog port (Firewall check on the SANnav server for the port 514 or Custom port)
9. Validate secure syslog port (Firewall check on the SANnav server for the port 6514 or Custom port)
10. Validate secure syslog CA root certificate

After running the tests, if any of the test result is `FAIL`, then there is an issue with SNMP/Syslog communication with the switch and the switch will fail to send Traps/Informs/Syslog events, and SANnav will not show switch and port statistics for switches running FOS versions that do not support streaming. If the issue cannot be fixed then contact Brocade support to fix the issue.

# Chapter 8: Security Vulnerability Fixes

This section lists the Common Vulnerabilities and Exposures (CVEs) updates included in Brocade **SANnav MP v2.3.1**.

- **CVE-2024-29950**

The class FileTransfer implemented in Brocade SANnav before v2.3.1, v2.3.0a, uses the ssh-rsa signature scheme, which has a SHA-1 hash. The vulnerability could allow a remote, unauthenticated attacker to perform a man-in-the-middle attack.

- **CVE-2024-29951**

A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a uses the SHA-1 hash in internal SSH ports that are not open to remote connection.

- **CVE-2024-29952**

A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a could allow an authenticated user to print the Auth, Priv, and SSL key store passwords in unencrypted logs by manipulating command variables

- **CVE-2024-29955**

A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a could allow a privileged user to print the SANnav encrypted key in PostgreSQL startup logs. This could provide attackers with an additional, less-protected path to acquiring the encryption key.

- **CVE-2024-29956**

A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a prints the SANnav password in clear text in support save logs when a user schedules a switch "supportsave" Brocade SANnav.

- **CVE-2024-29957**

When Brocade SANnav before v2.3.1 and v2.3.0a servers are configured in Disaster Recovery mode, the encryption key is stored in the DR log files. This could provide attackers with an additional, less-protected path to acquiring the encryption key.

- **CVE-2024-29958**

A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a prints the encryption key in the console when a privileged user executes the script to replace the Brocade SANnav Management Portal standby node. This could provide attackers an additional, less protected path to acquiring the encryption key.

- **CVE-2024-29959**

A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a prints Brocade Fabric OS switch encrypted passwords in the Brocade SANnav Standby node's support save.

- **CVE-2024-29960**

In Brocade SANnav server before v2.3.1 and v2.3.0a, the SSH keys inside the OVA image are identical in the VM every time SANnav is installed. Any Brocade SAnnav VM based on the official OVA images is vulnerable to MITM over SSH.

- **CVE-2024-29961**

A vulnerability affects Brocade SANnav before v2.3.1 and v2.3.0a. It allows a Brocade SANnav service to send ping commands in the background at regular intervals to gridgain.com and ignite.apache.org to check if updates are available for the Component. This could make an unauthenticated, remote attacker aware of the behaviour and launch a supply-chain attack against a Brocade SANnav appliance.

- **CVE-2024-29962**

Brocade SANnav OVA before v2.3.1 and v2.3.0a have an insecure file permission setting that makes files world-readable. This could allow a local user without the required privileges to access sensitive information or a Java binary.

- **CVE-2024-29963**

Brocade SANnav OVA before v2.3.1, and v2.3.0a, contain hardcoded TLS keys used by Docker. Brocade SANnav doesn't have access to remote Docker registries, and knowledge of the keys is a minimal risk as SANnav is prevented from communicating with Docker registries

- **CVE-2024-29964**

Brocade SANnav versions before v2.3.0a do not correctly set permissions on files, including docker files. An unprivileged attacker who gains access to the server can read sensitive information from these files.

- **CVE-2024-29965**

In Brocade SANnav before v2.3.1, and v2.3.0a, it is possible to back up the appliance from the web interface or the command line interface ("SSH"). The resulting backups are world-readable. A local attacker can recover backup files, restore them to a new malicious appliance, and retrieve the passwords of all the switches.

Note: The backup file contains several configuration files, including passwords, the entire database with the admin users, and the switches' configuration. An attacker with local access to the appliance can recover backup files and restore them to a new malicious appliance. The attacker can then do an air-gapped analysis by sniffing the malicious appliance's network interface and retrieving the passwords of all the switches. Reverse engineering of the custom encryption mechanism can also retrieve the passwords.

- **CVE-2024-29966**

In Brocade SANnav server before v2.3.1 and v2.3.0a, the SSH keys inside the OVA image are identical in the VM every time SANnav is installed. Any Brocade SAnnav VM based on the official OVA images is vulnerable to MITM over SSH.

- **CVE-2024-29967**

In Brocade SANnav before Brocade SANnav v2.3.1 and v2.3.0a, it was observed that Docker instances have insecure mount points, allowing reading and writing access to sensitive files.

- **CVE-2024-29968**

An information disclosure vulnerability exists in Brocade SANnav before v2.3.1 and v2.3.0a when Brocade SANnav instances are configured in disaster recovery mode. SQL Table names, column names, and SQL queries are collected in DR standby Supportsave. This could allow authenticated users to access the database structure and its contents.

- **CVE-2024-29969**

When a Brocade SANnav installation is upgraded from Brocade SANnav v2.2.2 to Brocade SANnav 2.3.0, TLS/SSL weak message authentication code ciphers are added by default for port 18082.

- **Azul Zulu Java Multiple Vulnerabilities (2023-07-18)**

Azul Zulu installed versions prior to 7 < 7.63.0.14 / 8 < 8.71.0.14 / 11 < 11.65.14 / 17 < 17.43.14 / 20 < 20.32.12 are affected by multiple vulnerabilities as referenced in the 2023-07-18 advisory.

- CVE-2023-22006
- CVE-2023-22036
- CVE-2023-22041
- CVE-2023-22043
- CVE-2023-22044
- CVE-2023-22045
- CVE-2023-22049

- **Oracle Java SE Multiple Vulnerabilities (July 2023 CPU)**

Oracle Java SE Multiple Vulnerabilities (July 2023 CPU)

- CVE-2023-22041

  **Base Score:** 5.1 MEDIUM

  **Vector:** CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

- CVE-2023-25193

  **Base Score:** 7.5 HIGH

  **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

- CVE-2023-22045

  **Base Score:** 3.7 LOW

  **Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

- CVE-2023-22049

  **Base Score:** 3.7 LOW

  **Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

- CVE-2023-22036

  **Base Score:** 3.7 LOW

  **Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L

- CVE-2023-22006

  **Base Score:** 3.1 LOW

  **Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N

- **CVE-2023-34478**

Apache Shiro, before 1.12.0 or 2.0.0-alpha-3, may be susceptible to a path traversal attack that results in an authentication bypass when used together with APIs or other web frameworks that route requests based on non-normalized requests. Mitigation: Update to Apache Shiro 1.12.0+ or 2.0.0-alpha-3+

- **CVE-2023-20863**

In Spring Framework versions 6.0.0 - 6.0.7, 5.3.0 - 5.3.26, 5.2.0.RELEASE - 5.2.23.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

- **CVE-2023-39417**

An extension script is vulnerable if it uses @extowner@, @extschema@, or @extschema:...@ inside a quoting construct (dollar quoting, '', or ""). No bundled extension is vulnerable. Vulnerable uses do appear in a documentation example and in non-bundled extensions. Hence, the attack prerequisite is an administrator having installed files of a vulnerable, trusted, non-bundled extension. Subject to that prerequisite, this enables an attacker having database-level CREATE privilege to execute arbitrary code as the bootstrap superuser. PostgreSQL will block this attack in the core server, so there's no need to modify individual extensions.

- **CVE-2023-20861**

In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

- **CVE-2023-39410**

When deserializing untrusted or corrupted data, it is possible for a reader to consume memory beyond the allowed constraints and thus lead to out of memory on the system.

This issue affects Java applications using Apache Avro Java SDK up to and including 1.11.2. Users should update to apache-avro version 1.11.3 which addresses this issue

# Chapter 9: Defects

## 9.1 Known Issues in SANnav Management Portal v2.3.1

| Defect ID | Description |
|---|---|
| SANN-145090 | Fabric state changes are not reflected in SANnav views |
| SANN-145110 | A wrong OEM model name is displayed in SANnav |
| SANN-145756 | SANnav displays different occurrence times for the notification message and the corresponding event |
| SANN-145822 | Duplicate IPSec policy is created on the switch |
| SANN-146257 | A blank dialog is seen after the EULA acceptance step during the firmware update operation. |
| SANN-146364 | FTP block push fails on Non-VF Brocade 7840 switch |
| SANN-146404 | SNMPv3 password is set incorrectly on the switch |
| SANN-146745 | SANnav database size in the file system increases |
| SANN-146964 | Created MAPS policies are not shown on the policies page |
| SANN-146968 | SNMP FFDC file is created in the switch. |
| SANN-147043 | SANnav Disaster Recovery data replication stopped |
| SANN-147045 | Able to set incorrect LDAP role configuration on the switch from SANnav |
| SANN-147079 | SANnav incorrectly reports firmware download on the switch as 'failed' even though the operation succeeded. |
| SANN-147117 | The client becomes unresponsive. |
| SANN-147120 | An incorrect warning message is displayed when replace-sannav-certificates.sh script is used to replace the server certificate. |
| SANN-147146 | The 'OK' button does not work in the MAPS page. |
| SANN-147148 | User unable to rename zone from zone inventory view |
| SANN-147151 | An error message is displayed when trying to investigate. |
| SANN-147162 | Switch configuration backup page does not render successfully |
| SANN-147303 | A duplicate PS_STATE measure is seen in MAPS rule configuration view |
| SANN-147327 | Device ports are not mapped to auto-enclosures. |
| SANN-147487 | Renaming Chassis from SANnav fails |

## 9.2 Defects Closed with Code Change in SANnav Management Portal v2.3.1

| Defect ID | Description |
|---|---|
| SANN-139712 | Unable to log into SANnav client as proxy service does not start. |
| SANN-142270 | An additional blank widget is added to the report template. |
| SANN-142368 | SANnav report generation fails. |
| SANN-142459 | Switch FID configuration backups are not listed for a replaced switch. |
| SANN-142468 | Health Summary Dashboard reduces health score for host/storage redundant paths. |
| SANN-142771 | Email alerts are not triggered for configured Event Action Policy. |
| SANN-143614 | Port investigation view does not load |
| SANN-143632 | Users cannot view or edit IPSec policies. |
| SANN-143988 | Login to SANnav application fails. |
| SANN-144482 | Configuring DR setup fails for standby server |
| SANN-144822 | In Frames and Out Frames are set to 0 while streaming performance data from SANnav. |
| SANN-144935 | The generated port performance report does not show any data |
| SANN-144959 | SANnav investigation view for FCIP Tunnels shows incorrect Rx/Tx utilization |
| SANN-145013 | SANnav does not forward SNMP traps to the configured forwarder |
| SANN-145017 | Migration from SANnav 2.1.1 to SANnav 2.2.2 fails |
| SANN-145210 | External REST API for fetching events does not work. |
| SANN-145458 | Existing IPSec policy cannot be used |
| SANN-146382 | The switch related changes are not reflected in the SANnav |
| SANN-146383 | In rare conditions, vCenter discovered in SANnav goes down |
| SANN-146396 | Switch configuration restore fails |
| SANN-146488 | Changes in the switch are not reflected in SANnav |
| SANN-146529 | SANnav reports success for firmware upgrade operation though the operation fails on the switch |
| SANN-146623 | Events and notifications related to server disk space usage are not shown in SANnav |
| SANN-146928 | All Fabrics selection does not work in the switch configuration backup page |
| SANN-147105 | Unable to send email notifications. |

## 9.3 Defects Closed without Code Change in SANnav Management Portal v2.3.1

| Defect ID | Description |
|---|---|
| SANN-141437 | Drift check fails occasionally for some of the switches with an error. |
| SANN-142213 | Sometimes firmware download status shows completed in SANnav even though it has not completed on the switch. |
| SANN-142738 | The firmware download fails with the error "server is inaccessible or firmware path is invalid". |
| SANN-142752 | Health score is deducted for both host and storage and the health details are not displayed for the enclosure in Dashboard & Inventory. |
| SANN-142755 | Drift check and configuration push fails error for RADIUS and TACACS+ blocks. |
| SANN-142806 | Host Health score computation is inaccurate for the resiliency check rule. |
| SANN-142808 | Host Health score computation is inaccurate for the redundancy check rule. |
| SANN-142810 | Importing a zone alias from the CSV file causes the loss of a zone alias from the fabric. |
| SANN-142817 | Member role changes from Principal to Peer in a peer zone. |
| SANN-142818 | Existing alias members get removed from peer zones with mixed membership types (WWN, Alias or DP, Alias). |
| SANN-145990 | SANnav continuously reports bad health status via email and notification panel for disaster recovery setup |
| SANN-146042 | Unable to discover replacement switch after RMA |

# Revision History

| Version | Summary of Changes | Publication Date |
|---|---|---|
| **1.0** | Initial version of Brocade SANnav Management Portal v2.3.1 Release Notes. **(NOT POSTED)** | 12/20/2023 |
| **2.0** | Added section 3.5.1.1.x (Important consideration when upgrading from SANnav MP v2.3.0 to SANnav MP v2.3.1 (OVA only) and updated defect list. **(NOT POSTED)** | 12/22/2023 |
| **3.0** | Fixed TOC issue (changed title from 2.3.0 to 2.3.1), added missing RHEL 8.6. **(NOT POSTED)** | 01/09/2024 |
| **4.0** | Updated Flow Management section, added Migration Docker location TSB, added defect “FWDL EULA blank message”. **(INITIAL POSTING)** | 03/05/2024 |
| **5.0** | Added CVE list for 2.3.1 (Section 8) | 05/06/2024 |

BROCADE

A Broadcom Company