SANnav™ Management Portal v2.3.0

SANnav Management Portal v2.3.0 Release Notes (Digest Edition)

Version 3 (Digest Edition)

Table of Contents

Chapter 1: Preface 5
1.1 Contact Technical Support for your Brocade® Product 5
1.2 Related Documentation 6

Chapter 2: Locate Product Manuals and Release Notes 7
2.1 Locate Product Manuals on Broadcom.com 7
2.2 Locate Product Manuals and Release Notes on the Support Portal 7
2.3 Document Feedback 8

Chapter 3: Release Contents 9
3.1 Brocade SANnav Management Portal v2.3.0 Release Overview 9
3.1.1 Upgrade to SANnav v2.3.0 Important Considerations 9
3.2 What's New in SANnav Management Portal v2.3.0 9
3.3 New Hardware Platforms Supported in SANnav Management Portal v2.3.0 10
3.4 New Blades Supported in SANnav Management Portal v2.3.0 10
3.5 SANnav Management Portal Server Platform Support and OS Support 10
3.5.1 SANnav Management Portal v2.3.0 OVA Support 10
3.5.2 SANnav Management Portal v2.3.0 OS Support (VM and bare metal) 11
3.5.3 FIPS-140 Enabled OS 12
3.5.4 SE Linux Support 12
3.5.5 Port Range Customization 12
3.5.6 2-Socket CPUs and CPU Speed Now a Recommendation 13
3.5.7 Package .yaml File 13
3.5.8 Other Installation and Deployment Features 13
3.5.9 URL Change for Broadcom Portal 13
3.6 Summary of New and/or Enhanced Software Features 14
3.6.1 Security and Infrastructure 14
3.6.2 FOS Certificates Management 15
3.6.3 FOS Firmware Platform Specific Download (PSD) Management 15
3.6.4 Call Home 16
3.6.5 Chassis Password Management 17
3.6.6 Discovery 17
3.6.7 Inventory 17
3.6.8 Zoning 18
3.6.9 Configuration Policy Management 22
3.6.10 Dashboards and Reports 24
3.6.11 Events and Violations 26
3.6.12 Alarm Enhancements 27
3.6.13 Topology Enhancements 28
3.6.14 Flow Management 29
3.6.15 UI/UX and Usability Changes 31
3.7 Features Deprecated with SANnav Management Portal v2.3.0 31
3.8 Features Removed from SANnav Management Portal v2.3.0 32
3.9 Important Considerations when Upgrading to SANnav v2.3.0 33
3.9.1 Flow Management 33
3.10 SANnav Management Portal v2.3.0 Supported SAN Switches 33
3.10.1 Platform Support and FOS Support – New Policy 33

Chapter 4: Brocade SANnav Management Portal Deployment 35
4.1 Server Requirements 35
4.2 Client Requirements 36
4.3 Software Upgrade... 36

Chapter 5: Licensing 37
5.1 Removal of Trial Period with SANnav v2.3.0 37
5.2 Removal of 30-Day Grace Period (Available After License Expiration)............................... 37
5.3 New License File Expiration Date 38
5.4 Export Renewal Request 38

Chapter 6: Scalability 39
6.1 SANnav Management Portal v2.3.0 Scalability 39

Chapter 7: Important Notes.. 40
7.1 General 40
7.2 Infrastructure, Installation, and Migration 40
7.3 Firmware Management and Support Save 42
7.4 Discovery and Performance Management 43
7.5 SANnav Backup, Disaster Recovery and Support Data Collection 43
7.6 SANnav Telemetry Registration with FOS.. 44
7.7 SNMP and Syslog registration with FOS 44

Chapter 8: Security Vulnerability Fixes 45

Chapter 9: Defects 53
9.1 Known Issues in SANnav Management Portal v2.3.0.. 53
9.2 Defects Closed with Code Change in SANnav Management Portal v2.3.0 54
9.3 Defects Closed without Code Change in SANnav Management Portal v2.3.0 57

Revision History... 59

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: ▪ Case Management ▪ Software Downloads ▪ Licensing ▪ SAN Reports ▪ Brocade Support Link ▪ Training & Education	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at http://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:

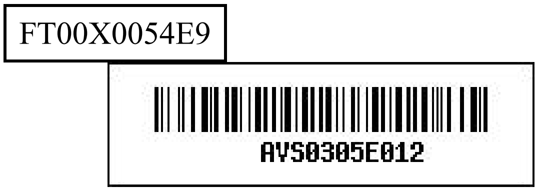
- General Information
  - Technical support contract number, if applicable
  - Switch model
  - Switch operating system version and SANnav version
  - Error numbers and messages received
  - SANnav Support Data Capture (SSDC) and Switch supportSave command output and associated files

  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

AVS0305E012

  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 `licenseIdShow` command to display the license ID.

1.2 Related Documentation

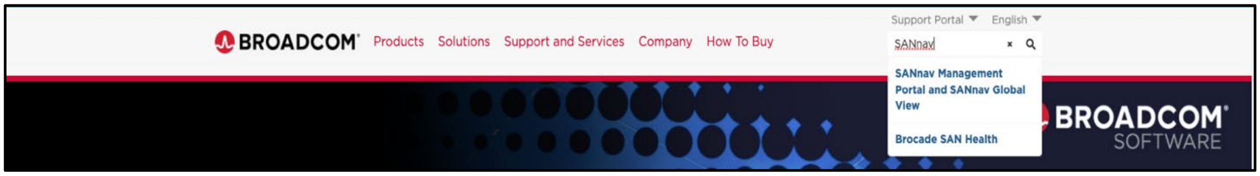
White papers, data sheets are available at www.broadcom.com. Product documentation for all supported releases is available on the support portal to registered users. Registered users can also find release notes on the support portal.

Chapter 2: Locate Product Manuals and Release Notes

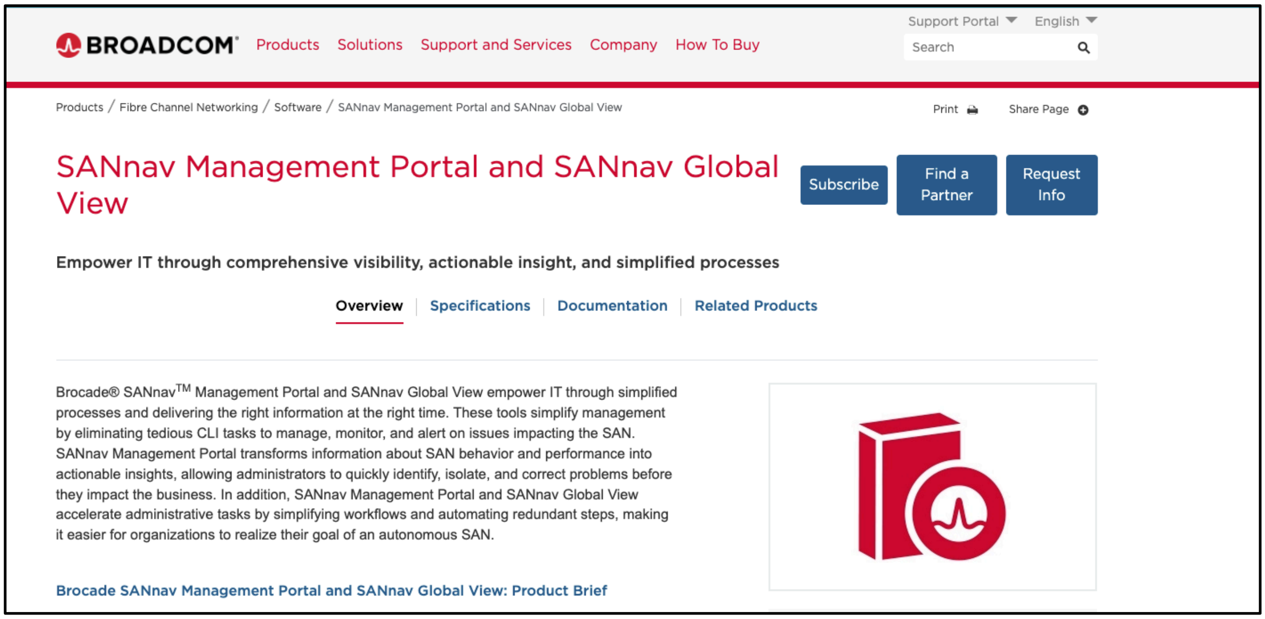
2.1 Locate Product Manuals on Broadcom.com

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

1. Go to https://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™ 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 https://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 v2.3.0 Release Overview

Brocade SANnav Management Portal v2.3.0 is a major software release introduced to support Fabric OS® (FOS) v9.2.x and to provide new or major feature enhancements.

This chapter highlights the new features, support, capabilities, and changes in the SANnav Management Portal v2.3.0 release. Note that this document applies only to the Brocade SANnav **Management Portal** product. There is a separate Release Notes document for the Brocade SANnav **Global View** v2.3.0 release.

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

3.1.1 Upgrade to SANnav v2.3.0 Important Considerations

Broadcom recommends customers stay on the latest current SANnav target path version for highest levels of stability.

Customers should consider upgrading to SANnav v2.3.0 instead of the current target path version in the following cases:

1. Plan to upgrade SAN switches to run FOS v9.2.0 which require SANnav v2.3.0 or later, and/or
2. Strongly benefit from new SANnav v2.3.0 features.

3.2 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 & 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 & Latency widget
- Dashboards & Reports
- Events & 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 v2.3.0

Support for the following hardware platforms has been added in SANnav Management Portal v2.3.0.

- Brocade 7850

3.4 New Blades Supported in SANnav Management Portal v2.3.0

The following new blade platforms have been added in SANnav Management Portal v2.3.0.

- Brocade FC 64-64

3.5 SANnav Management Portal Server Platform Support and OS Support

3.5.1 SANnav Management Portal v2.3.0 OVA Support

SANnav v2.3.0 continues to support deploying SANnav Management Portal as an Open Virtual Appliance (OVA).

SANnav v2.3.0 OVA no longer packages CentOS Operating System (CentOS) v7.9 due to the End of Support of CentOS 7.9.

SANnav v2.3.0 OVA now packages ***Rocky Linux v8.6***.

- Extraction of the OVA file is supported on vCenter 7.x (and ESXi 7.x) as shown below. No other OVA extraction method is officially supported.

NOTE Extraction of the SANnav OVA image using vCenter 8.0 *should* work but has not been tested or qualified

ESXi version	Extraction Method	Supported
6.5	vCenter 6.5	No
6.7	vCenter 6.7	No
6.5	vCenter 6.7	No
6.7	vCenter 6.5	No
7.0	vCenter 7.0	Yes
8.0	vCenter 8.0	No (*)

(*) vCenter 8.0 not officially tested or qualified

- OVA is currently available only for SANnav Management Portal and **not** for SANnav Global View.
- Since the OS is different in previous releases (CentOS 7.9), any migration path to SANnav v2.3 in OVA deployment (Rocky Linux 8.6) cannot be performed "in line" and will require a full extraction of the OVA file.
- When upgrading from SANnav v2.2.1 to SANnav v2.3.0 in OVA deployment (and only in this case), it is required to perform an OVA in-line upgrade from SANnav v2.2.1 to SANnav v2.2.2 first, and then to upgrade to SANnav 2.3.
- Instead of automatically starting the installation on the first login, users must invoke the script "*install-sannav.sh*" after successful VM setup (this is different from the behaviour in previous releases of SANnav)
- By default, "*firewalld*" will be disabled in the VM deployed after OVA extraction.
- The SANnav v2.3.0 *SANnav MP Installation and Upgrade Guide* has been updated and contains detailed instructions on how to install and deploy SANnav v2.3.0 for the first time as an OVA or how to upgrade from previous SANnav releases (SANnav v2.2.1.x and SANnav 2.2.2.x) deployed as OVA to SANnav v2.3.0 deployed as an OVA.

ATTENTION Note the change in behavior in the case of SANnav v2.3.0 OVA: the installation or upgrade of SANnav after successful OVA extraction does not start automatically. The installation/upgrade script "install-sannav.sh" must explicitly be invoked and run after successful extraction.

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.x OVA to SANnav MP v2.3.0 OVA.

3.5.1.1 OVA and Rocky Linux CVEs Process

While Brocade ensures that CVEs on the OS (Rocky Linux) are addressed at the time of releasing SANnav v2.3.0, it is possible that some specific Rocky Linux 8.6 CVEs are only found and disclosed after SANnav v2.3.0 has been released and before a patch on SANnav v2.3.0 is issued. In the event this occurs, it is the customer'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, contact Brocade Support.

3.5.2 SANnav Management Portal v2.3.0 OS Support (VM and bare metal)

For bare metal and VM deployments, CentOS **7.9** and RHEL **7.9** are *no longer supported* for SANnav installation and deployment.

End users running SANnav v2.2.1x/v2.2.2x in VM or bare metal on CentOS 7.9 or RHEL 7.9 and planning to upgrade to SANnav v2.3.0 must upgrade OS to supported RHEL versions (8.4 or 8.6). Refer to the *SANnav Management Portal v2.3.0 Installation and Upgrade Guide* for the procedure details.

SANnav Management Portal v2.3.0 officially supports the following versions of RHEL:

- RHEL releases 8.4 and 8.6.

NOTE RHEL 9.x is not supported for SANnav v2.3.0 installation. It is not possible to install SANnav MP v2.3.0 (and below) on a VM or bare metal server running RHEL 9.0. The SANnav installation will exit and will not proceed.

When installing SANnav on an untested or unqualified OS version, (i.e., 8.2, 8.3, 8.5, 8.7 and 8.8), 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 issues occur while using SANnav it may be necessary to migrate to a fully qualified and tested OS version and reproduce the issues to receive support.

The following table shows the various OS types and versions and the associated support in SANnav v2.3. Cells marked with (Blocked) indicate that the SANnav v2.3.0 installation/upgrade will not proceed and exit, while cells marked (Not Blocked) indicate the SANnav v2.3.0 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 bare metal	OVA	DR Support
RHEL 7.9, RHEL 8.0, 8.1	No (Blocked)	No	No (Blocked)
CentOS 7.9	No (Blocked)	No	No (Blocked)
RHEL 8.2, 8.3, 8.5, 8.7, 8.8	No (Not Blocked)	No	No (Blocked)
RHEL 8.4, 8.6	Yes	No	Yes (VM only)
RHEL 9.x	No (Blocked)	No	No (Blocked)
Rocky Linux 8.6	No (Blocked)	Yes	Yes (OVA only)
Rocky Linux 8.7 and higher	No (Blocked)	No	No (Blocked)

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 FIPS-140 Enabled OS

SANnav MP v2.3.0 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 v2.3.0 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.

3.5.4 SE Linux Support

SANnav Management Portal v2.3.0 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.

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

3.5.5 Port Range Customization

A port range will be requested during SANnav v2.3.0 installation for the ports used by SANnav services. This port range is a range of 100 consecutive ports. All 100 ports in the range must be available for SANnav use *exclusively*.

The port range is between 1 to 65535, the default range is 12000-12099.

- The complete range of 100 ports must be free and available for SANnav usage.

- An error is thrown if any port within the range is not free.
- For OVA deployments, the user may not control the port range during installation, it is defaulted to 13000 to 13099.

3.5.5.1 Important Consideration for DR (Disaster Recovery) Deployments

- When the DR script "**`setup-dr-standby.sh`**" is executed, a check is made to ensure the port range that is allocated on the primary node is also available in the standby node. If any of the ports in the specified range on the primary node are not available on the standby node, the script will exit. The user is expected to free up the ports and to run the setup-dr-standby.sh script again.

3.5.6 2-Socket CPUs and CPU Speed Now a Recommendation

Up to and including SANnav v2.2.x, there was a "hard" requirement for two or more CPU sockets on the SANnav MP or GV server. Similarly, there was a requirement for the CPU clock speed to be at least 2000MHz. With SANnav v2.3.0, both items are now a *recommendation* and no longer a requirement.

If the installation scripts or upgrade and migration scripts detect a server with only 1 socket, or CPU clock speed lower than 2000 MHz, the scripts will warn the user on the console and proceed.

- This does not reduce the number of vCPUs required (16 vCPU for 48GB platforms and 24 vCPU for 96GB platforms).
- The vCPU requirements remain independent of the number of sockets.

3.5.7 Package .yaml File

- SANnav v2.3 installation will now package a complete YAML file containing a description and documentation of all SANnav REST interfaces supported.
- The YAML file is called *external-api.yaml* and lives under conf/northbound/api under the SANnav HOME directory.
- YAML file can be loaded into any YAML editor such as:
  - swagger (https://editor.swagger.io/)
  - postman (https://www.postman.com/)

3.5.8 Other Installation and Deployment Features

- Starting with SANnav v2.3.0, the upgrade/migrations scripts will detect the currently installed SANnav version and path.
  - The user installing SANnav is prompted for confirmation before proceeding to ensure the path is correct.
- Important OS level customization for user "sannavmgr"
  - SANnav needs ports lower than 1024 for running some of its services.
  - Due to this, Linux *""ip_unprivileged_port_start"* parameter is set to "0" to allow "sannavmgr" to run services on ports lower than 1024.

3.5.9 URL Change for Broadcom Portal

SANnav contacts the Broadcom web portal for multiple functions as follows:

- To rehost the SANnav Active server License to the Standby server in case of Disaster Recovery (DR) failover
- To retrieve an updated or renewed SANnav license when the license renewal is due.
- To fetch TruFOS certificates for the managed switches which require a TruFOS certificate to operate.

With SANnav v2.3.0 the URL for contacting Broadcom has changed to a new endpoint.

Customers need to make sure the URL "`https://api.broadcom.com`" is not blocked and is accessible by the SANnav server to make sure that the above items will continue to function without any issue.

NOTE Previous versions of SANnav (prior to SANnav v2.3.0) used the URL end point "`https://enterprise.broadcom.com`"

3.6 Summary of New and/or Enhanced Software Features

3.6.1 Security and Infrastructure

3.6.1.1 Installation and Upgrade/Migration as “sudo”

- Prior to SANnav v2.3.0, only the “root” user could install and manage the SANnav server. “sudo” privileged users could not install/upgrade/run/manage SANnav server.
- With SANnav v2.3.0, 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" (e.g., sudo ./install-sannav.sh)
- After installing SANnav v2.3.0, additional “sudo” users may be added to manage SANnav by executing the script ”add-user-to-sannavmgr-group.sh” (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/run SANnav.

3.6.1.2 Running SANnav Containers with No “root” or “sudo” Privileges

With SANnav v2.3.0 docker containers will run as a new user “*sannavmgr*” with UID 56900. This new user does not require “sudo” privileges.

- During SANnav v2.3.0 installation or upgrade/migration, this user “*sannavmgr*” with UID 56900 will be created.
- If UID 56900 is occupied by another user on the SANnav host, the installation or upgrade will fail. The script expects UID 56900 to be available and it is not configurable in this release.
- User “*sannavmgr*” cannot be used for remote SSH login to the SANnav server (for security)

UID 1000 required in prior SANnav releases, is still required for SANnav v2.3.0 to receive streams from FOS. It is preferred that the UID 1000 is associated with the username “*sannavstreaming*”. If not, then whatever username is associated with UID 1000 will be used. UID 1000 must be already created or available prior to installing SANnav.

3.6.1.3 Change SANnav Server Security Password

With SANnav v2.3.0, it is now possible to change the SANnav password post installation.

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

Prior to SANnav v2.3.0, this SANnav Server Security password cannot be changed post SANnav installation or upgrade.

With SANnav v2.3.0, this password can be changed by an authorized 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 v2.3.0 from “*sannav-management-consol.sh*” in previous releases.

3.6.1.4 Nested LDAP Groups

- With SANnav v2.3.0, 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 v2.3.0.

- To fetch the complete hierarchy, the user can import the nested hierarchy from the topmost outer group.

3.6.1.5 MFA and SSO Support with SAML 2.0 Compliant Protocol

SANnav v2.3.0 now supports SAML 2.0 integration with various IdP (Identity Providers). SANnav v2.3.0 should work seamlessly with any IdP complying with SAML 2.0 REST specifications.

SANnav v2.3.0 has been specifically tested and validated with the following SAML 2.0 Identity Providers:

- Okta
- Microsoft Azure
- Microsoft ADFS
- Keycloak

3.6.1.6 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 v2.3.0 secure syslog reception will ensure that:

- 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 (e.g., “SwitchA”) is discovered in a SANnav server (e.g., “ServerA”) and if an attempt is made to discover “SwitchA” in another SANnav server (e.g., “Server B”), then the syslog HTTPS certificate will be automatically imported in “ServerB”, and secure syslog will no longer be functional in “ServerA”

3.6.2 FOS Certificates Management

SANnav v2.2.x provided a new feature to manage FOS HTTPS chassis certificates using “wildcard” SSL certificates. In that implementation, it was the user’s responsibility to create keys and CSR requests (outside of SANnav).

SANnav v2.3.0 enhances this feature by providing tools for customers to manage multiple certificates on multiple Chassis (no shared key, aka as “non-wildcard”). SANnav supports following functionality to manage a single certificate signed on a single chassis running FOS v9.1.1 or above (only)”

- Generate CSRs
- View and Export CSRs
- Import signed certificates and push them to the correct chassis.

ATTENTION FOS 9.1.1 or above is required to use this feature, both in the shared key use case (wildcard) or no shared key use case (non-wildcard)

3.6.3 FOS Firmware Platform Specific Download (PSD) Management

3.6.3.1 Allow Firmware Image to be Imported in a SANnav Server Folder

With SANnav v2.3.0 a new option is added to allow users to import the FOS PSD images into a SANnav server folder instead of importing into the local client folder as is available in prior releases of SANnav. There are now two options:

- SANnav client Local folder (existing behavior)

- SANnav Server folder (new option in SANnav v2.3.0

3.6.3.2 Control the Order of FOS Firmware Download for Multiple Chassis

A new option is now provided in SANnav v2.3.0 to control the order in which SANnav performs the FOS firmware download to multiple chassis. This applies whether using an “Internal” (SANnav) SCP/FTP server or an “External” SCP/FTP server. The options available to control the order of FOS firmware download in SANnav v2.3.0 are:

- SANnav Defined (default, same as previous releases)
- All Parallel
- All Serial

3.6.4 Call Home

3.6.4.1 Configure Call Home Notification Interval

This feature is useful to avoid sending call home for temporary loss of switch reachability.

This is achieved through a new user interface option under SANnav→ Call Home configuration → Notifications Policy. With SANnav 2.3.0, a new feature is provided to set a “buffer time” before triggering a Call Home email only for “switch not reachable” events.

- The default value of the timer is 15mn. To notify Call Home immediately, change this value to 0.

3.6.4.2 IBM Call Home

3.6.4.2.1 New Customer Details

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

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

To comply with GDPR requirements, a Personal Data Collection Agreement must be agreed upon by the user setting the IBM Call Home Center.

3.6.4.2.2 Test Call Home to Include Switch Information

- A new “Send Test Call Home” option has been added to the chevron menu in the table for sending a Call Home test email with chassis information (Serial Number and other information)
- If a user clicks on the "Send Test Call Home" button on the IBM Call Home Center instead of invoking it in the chevron menu on the list of Chassis, the following message will be shown:
  - This test email will contain general information only and will not contain the chassis information. If you want to send a test Call Home email with the chassis serial number and type, select the chassis in the chassis table and trigger Send Test Call Home option by clicking the down-arrow available next to each chassis.

3.6.4.3 Brocade Call Home: Reply Email Behavior

The Reply Email field in the Brocade Email Call Home centre must be set to a valid email address that exists in the Broadcom Support Portal. Instructions on how to upgrade for customer access can be found here:

- https://knowledge.broadcom.com/external/article?articleId=258609.

Failure to enter a valid email address will result in Call Home emails not being processed under the correct company name.

3.6.5 Chassis Password Management

In SANnav v2.3.0, a new column ("Discovery User") in the SANnav → Security → Chassis Password Management table view is added to show the switch user account(s) which SANnav has used for discovering the switch(es)

The column “Discovery User” will display a value even if a switch has been discovered by an external user defined in RADIUS or LDAP.

This additional information is also shown in the Chassis detailed view as a separate “Discovery User” attribute.

3.6.6 Discovery

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”.

3.6.6.1 New SNMP Authorization Protocol value HMAC_SHA512

A new additional Authorization Protocol option “HMAC_SHA512” will be provided In the Fabric Discovery detailed page for a given switch in the Fabric. FOS releases prior FOS v9.2.0 do not support this value (HMAC_SHA512).

3.6.7 Inventory

3.6.7.1 Device Port to Device Enclosure Mapping Policy

This new feature allows 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 run time.

The menu SANnav → SAN Monitoring → Inventory Settings has now a new Tab called “Host & Storage Naming Policy”. This new tab is introduced to control and manage the device ports to enclosure mapping formation (new feature in SANnav v2.3.0).

In this new tab there are four main items:

1. SANnav Automatic Host Enclosure
2. Automatic Storage Enclosure
   - These two new 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 Policy
   - These two new items that allow to control how SANnav should determine the mapping between device ports logging in to the Fabric 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 certain character from the value of the component.

3.6.7.2 Offline Device Ports

SANnav allows importing pre-provisioned device ports (offline ports) using either REST interfaces or through a UI Import operation. Up to SANnav v2.3.0, there is no way to view these imported device ports in the SANnav Inventory.

With SANnav v2.3.0, a new option menu under the Inventory to view these Offline Device Ports is provided. When any of these ports comes online by connecting them to the Fabric, then they will be moved from the Offline Device Port Inventory to the specific Host or Storage Port inventory tables.

3.6.7.3 NPIV Ports and Physical Ports in Different Device Enclosure

Previous versions of SANnav did not properly manage Hosts or servers where the NPIV Ports and the Physical HBA Ports belong to different Host enclosures. This case is specific to VIO or AIX Servers typically but could happen in the case of Storage as well.

To support this properly, changes in the SANnav Inventory modeling were made. The changes introduced in the SANnav Inventory to handle this use case are as follows (all use cases can be performed in bulk):

- New column called “Port Type” (in the Storage Port list view and reports)
- Change the column called “Device Type” to “Port Type” (in the Host Port list view and reports)
- Overwrite “Port Type” from “Physical” to “Virtual (NPIV)” (and vice versa)
- Change “Port Role” attribute values to “Initiator” or “Target” (in both Host Port and Storage Port tables)

Refer to section 3.6.14 Topology as these changes are visible in the Topology contexts for these special Hosts or Storage devices.

3.6.7.4 Miscellaneous Inventory Changes

- The columns names and values of entities are now consistent within and across products (SANnav Management Portal and SANnav Global View). This applies for Fabric, Chassis, Switch, Switch Ports, Host, Host Ports, Storage, Storage Ports. In particular, the word “attached” has been changed to “connected” for these columns.
- A new column “FDMI Name” is now added to the Host Port and Storage Port Inventory tables.
- The length of the Host and Storage names (enclosures) is extended to 256 characters in SANnav v2.3.0 (from 32 characters in previous releases).
- The Inventory drop down menu option showing the SAN entities (Fabrics, Switches, Switch Ports, Devices, Device Ports, VMs, Offline Ports) has been reorganized in SANnav v2.3.0 for better readability.
- Enhanced error checking (header, invalid data, file type, etc.) when importing mapping file (.csv) for Device Port to Device Enclosure mapping.
- The Health Details for Fabrics, Switch, Host and Storage “donut” score graphic shows only one color in SANnav v2.3.0 as opposed to two colors in previous releases.

3.6.8 Zoning

SANnav v2.3.0 offers 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 complement automation features and provide 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

3.6.8.1 Fabric Zone DB Snapshots

Up to five different Zone DB snapshots of any SANnav managed Fabric may be created and stored in SANnav database. The oldest snapshot is overridden if more than 5 snapshots exist for a given Fabric (e.g. 6th snapshot will override oldest snapshot).

- If snapshot is identical to an existing one, a new snapshot is not taken (checksum).
- User may view (graphical view) the contents of any snapshots once successfully created by SANnav.
- User may delete any of the five snapshots at any time. No bulk delete.
- User may export any snapshots in JSON file and import a JSON file representing a Zone DB snapshot of a given Fabric.
- User can restore any of the five snapshots to the Fabric (or to another Fabric via import)
  - There is no ability to "compare" snapshots in this release. A user can only view any given snapshot before restoring it.
  - User has option to activate now or later, the restored snapshot on Fabric.

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 Zoning Database snapshot when restoring the Fabric from an existing snapshot. Restoring the Fabric from a user modified JSON backup file is not supported and may void support from Broadcom.

3.6.8.1.1 Important Considerations when Restoring a Zone Database Snapshot for a Given Fabric

When restoring a Zone Database (Zone DB) snapshot on a given fabric the following behavior should be noted:

1. When "Activate" checkbox selected (checked)
   - This operation will remove all zone configurations, zones, and zone aliases from the fabric and will copy all zone configurations, zones, and zone aliases from the snapshot to the fabric and effective zone configuration <effective_configuration_name> (Defined Copy) from the snapshot will be activated and will replace the fabric's effective zone configuration <current_effective_configuration_name >
2. When "Activate" option is not selected and the default zoning policy of the fabric is set to "No access"
   - This operation will remove all zone configurations, zones, and zone aliases from the fabric and will copy all zone configurations, zones, and zone aliases from the snapshot to the fabric and the fabric's effective zone configuration <current_effective_configuration_name > will be deactivated.

     CAUTION This will result in connectivity loss between all hosts and storages in the fabric.
3. When activate option is not selected (checked) and the default zoning policy of the fabric is set to "All access"
   - This operation will remove all zone configurations, zones, and zone aliases from the fabric and will copy all zone configurations, zones, and zone aliases from the snapshot to the fabric and the fabric's effective zone configuration <current_effective_configuration_name > will be deactivated.

3.6.8.2 Multiple Principals for Policy Based Zone Creation and Activate Later

Up to SANnav v2.2.x, when a user created a Peer Zone through SANnav Policy based zone creation (starting from Host Port or Storage Port Inventory), one peer zone per principal member was created.

In SANnav v2.3.0, the user will have the ability to specify through an option in UI to instead create one Peer Zone with as many principals as specified in the policy.

This will result in the creation of a single Peer Zone with N host/storage ports as peer members and M storage/host ports as principal members (or vice versa).

Note the two important points below:

- To add members to an already created peer zone, user must provide the *same* Zone Name in the peer zone upon creation.
- A new checkbox "Activate" is now provided in the UI. The default state of the new "Activate" button is "checked" to retain the previous SANnav v2.2.x behavior. If "unchecked" by the user, the zones are created or modified and added to the Defined Configuration. An explicit Activate is required to activate the new zones in the Fabric.

3.6.8.3 New Zoning Preferences

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

1. Allow Mixed Zones creation/editing/deletion.
2. Allow for preferred default zone type on creation (Standard or Peer)
3. Allow for preferred Zone Policy default creation Type (I-T, I-*, *-T)
4. Zone naming preferences or policies
5. Zone Alias naming preferences or policies

Note that these five new zoning policies preferences are not "*enforced*" by SANnav. They are "*permissive*" and may be overridden by the user at any time.

3.6.8.3.1 Allow Mixed Member while Creating/Updating a Zone

This new preference will allow users to create, update or delete Zones with mixed-member types. That is, zones that contains any mix of zone members. This was not allowed in prior releases of SANnav.

The zone members can now be any of the following types within the zone when this preference is selected:

- Zone Alias
- PWWN
- D, P notation

3.6.8.3.2 Preferred Default Zoning Type

Once this preference in the Policy is set (Peer for example), then any Zone creation from any menu in the SANnav Zoning page will default to Peer.

3.6.8.3.3 Preferred Default Zone Policy Type

Once this preference in the zoning policy (aka Simplified Zoning) is set (*-T for example), then the policy based Zone creation will default to *-T for any zone creation.

3.6.8.3.4 Zone Naming Policy and Zone Alias Naming Policy

The new Zone Naming and Zone Alias Naming policy allow users to control the names of Zones and Zone Aliases when creating zones or zone aliases using the SANnav zoning policy (aka Simplified Zoning).

The names of the zones or zone aliases are controlled via naming components and a grammar expressed using "regex" expressions much like it is provided in the mapping of Device ports to Enclosures, see section "3.6.8.1 Device Port to Device Enclosure Mapping Policy".

The *Zone and Zone Alias names* ***common*** naming components are:

- Host (the name of host enclosure to which the zoned host port belongs)
- Storage (the name of storage enclosure to which the zoned host port belongs)
- Fabric (the name of the Fabric to which the device ports are connected to)
- Text (a user defined fee text with character restrictions)

The *Zone* names ***specific*** naming components are:

- Zone Alias (the zone alias of each of the zone members. If peer zone, the first principal member is selected

The *Zone Alias* names ***specific*** naming components are:

- Connected F-Port (the name of the F-Port to which the device port is connected to)
- Switch (the name of the switch to which the device port is connected to)
- PWWN

3.6.8.4 Display Affected Zone Tree Entities when Deleting Zones or Zone Aliases

When deleting a zone or a zone alias in any Fabric Zone DB tree, there may be consequences, side effects or impact on other objects in the Zoning tree that may be associated with the deleted zones or zone aliases.

A typical use case is when a Storage or Host enclosure needs to be fully decommissioned, and the user wants to make sure that all elements of the Zoning tree are completely dereferenced safely and accurately. In those cases, this feature provides a clear graphical display of these consequences or impacts so that the user is fully aware of these before deleting in bulk the zones or zone aliases.

As an example, if the user selected multiple zone aliases to be deleted from a Fabric, SANnav will display the following information graphically:

- All the Zone Aliases will be removed from the zones to which they belong (modified zones will be shown)
- If the Zone Alias to be deleted is the last one in the Zone, then the Zone will also be deleted (deleted zones will be shown)
- The Zone Configuration to which the modified zone is attached will also be modified (modified zone configuration will be shown)
- If the Zone to be deleted is the last zone in the Zone Configuration, then the Zone Configuration will also be deleted (deleted zone configuration will be shown)

NOTE Bulk Deletion of Zone objects or Zone Alias objects in SANnav requires switches running **FOS 9.0x or above**.

3.6.9 Configuration Policy Management

With SANnav v2.3.0, several usability enhancements and workflow enhancements are provided in Configuration Policy Management.

Managing multiple Switch/Chassis configurations parameters and MAPS rules via CLI or automation scripts is tedious, error prone and cumbersome. Instead, it is recommended to use this feature.

Note the deprecation of the traditional (legacy) MAPS Policy Management. It is strongly recommended to use the new SANnav Configuration Policy Management instead which provides much better workflows for managing configuration (chassis and logical switches) parameters and MAPS policies and rules generically and in an abstracted and simplified way.

3.6.9.1 Global Search and Bulk Edit for SANnav MAPS Block Rules

Typical use cases around managing MAPS rules involve searching for MAPS rules; edit them in bulk; and add them in a new or existing SANnav Custom MAPS Policy

- Use Case 1: Change/replace the rule name(s) for certain rules from the default name (e.g. defALL_100G_QSFPCURRENT_10) to a customized name (e.g. CompanyName_100G_QSFPCURRENT_10)
- Use Case 2: Change/replace the Action list for multiple rules in one shot (e.g. all MAPS rules need to have following action specified : RAS Log, SNMP Trap, E-mail)

To address these two use cases, two new features are introduced in SANnav v2.3:

- MAPS Block global search: searches for specific string in all MAPS rules.
- Bulk edit of MAPS rules:
  - Edit rule names in bulk.
  - Edit rules action list in bulk.

To support these two new features, the User Interface for managing MAPS blocks had to be redesigned. Therefore, in SANnav v2.3.0, the UI to manage MAPS rules has been redesigned and enhanced for better usability to search and replace both rule names and action lists.

3.6.9.2 Configuration Policies to be Managed by Users Having ALL_FABRICS_AOR

- With SANnav v2.3.0, only users having the “ALL_FABRICS_AOR” AOR (that is visibility to all managed Fabrics) and “Config Mgmt-RW” role privileges will be able to *create, view, edit and delete* SANnav Configuration Policies.
- Any user can with “ALL_FABRICS_AOR” AOR and “Config Mgmt-RW” role privileges can view/edit/delete a policy that was created by *another* user also having the ALL_FABRICS_AOR AOR and “Config Mgmt-RW” role privileges.
- Any user can with “ALL_FABRICS_AOR” AOR and “Config Mgmt-RW” role privileges can view/edit/delete a policy that is marked as belonging to the “System” user (special case when user is deleted or privileges changed)
- Users with the ALL_FABRICS_AOR AOR but only “Config Mgmt-Read” role privilege may only *view* the Policy but not *edit* it.
- Users with “Config Mgmt-RW” role privileges but not having “ALL_FABRICS_AOR” AOR many are not able to *view* or *edit* the policy.
- When a user that created the Configuration Policy is deleted and no longer exists in SANnav, the policies created by that user will be assigned to the SANnav “System” user. Similarly, the block sets which were created by the deleted user will be retained in SANnav and their ownership will change to ‘System’ user.

- Policies and blocksets created by SANnav Global View user cannot be edited or deleted from SANnav Management Portal by any user and can only be viewed by a user having “ALL_FABRICS_AOR” AOR and “Config Mgmt-RW” role privilege.

ATTENTION Users who created Configuration Policies in previous releases of SANnav and who did not have the “ALL_FABRICS_AOR” AOR will not be able to edit the respective policies after upgrade and migration. Only users with the “ALL_FABRICS_AOR” AOR and “Config Mgmt-RW” role privilege will be able to edit their policies.

3.6.9.3 Enhanced Switch RMA Workflow

The Switch RMA use case to replace a failed switch has been enhanced to initiate the Switch RMA from the Discovery page for ease of use. With SANnav v2.3.o a new menu called “RMA Restore” is now available to initiate the RMA restore. The rest of the workflow is the same as for previous releases.

3.6.9.4 Enhanced “Check Failed” Error Message

When the drift detection fails for any reason, the message “Drift Check Failed” Error message will be enhanced to show the reason for why the drift check failed when the user clicks on the “View drifts’ option menu.

The possible reasons for why the drift check fails are:

- Switch has reached its max limit of connected SANnav applications.
- Switch is not reachable.

3.6.9.5 Add (i) to Help User When Configuring (FOS) Dynamic Port Names in SANnav

With FOS v9.x release, a new feature was introduced called “Dynamic Port Names”. With this feature, FOS automatically names the Fabric Ports with a naming convention made from specific character strings such as “S.T.I.C.A.F.R”. Refer to the FOS Administration Guide and manual for details on this feature.

With SANnav v2.3.0 new Configuration Policy, the configuration block for “Port Configuration” supports an enhanced information message to show the meaning of these character strings for better usability and ease of use. In addition, SANnav will perform a check to ensure the string formed is valid and supported by FOS.

3.6.9.6 New SNMP v3 Authorization Protocol SHA-512 in SNMP Configuration Block

SANnav v2.3.0 Configuration Policy SNMP v3 Configuration block will support the new FOS v9.2.0 authentication SNMP v3 protocol value “HMAC_SHA512 when specifying SNMP block (USM accounts).

3.6.9.7 New IP Filter Configuration Block

With FOS v9.2.0, the default FOS IP Filter policies have been modified to disable ports 80 and 22 which were enabled in previous releases. To handle this, SANnav will have a dropdown option menu in the IP Filter configuration Block to show the pre-FOS v9.2.0 default IP Filter values and the FOS v9.2.0 and higher default IP Filter values. The two new option menus are:

- FOS v9.1.x or lower
- FOS v9.2.x or higher

3.6.9.8 Drift Detection Cycle Changed to Once Every Hour

With prior releases, the automatic SANnav scheduled drift check will trigger every 15 minutes. With SANnav v2.3.0, the SANnav scheduled drift check is now every hour.

3.6.10 Dashboards and Reports

3.6.10.1 Health Summary Dashboard Enhancements

With SANnav v2.3.0 the following enhancements are provided for the Health Summary Dashboard (HSD) feature:

- Identify and Alert on Fabrics with zone policy set to “All Access” and there is no Effective zone configuration. By default, value of score deduction is -5
- Deduct points when a Switch is not part of any enabled Call Home. By default, value of score deduction is -5
- Export Details of affected Health Factors and Recommendations in HSD Export. This will only be available in the main system HSD (no other custom dashboard created with HSD individual widgets). The exported data is in .csv format that looks like the JSON data which is sent by the equivalent existing REST interface to get the HSD details.
- Previous releases of SANnav checked for redundant path (across 2 fabrics) from a host port to the zoned storage port. With SANnav v2.3.0, a new factor is added to deduct points if a host port is missing a resilient path (within a Fabric) to the zoned Storage port. The default is five points for no resilient path and five points for no redundant path.
  - Turn off (uncheck) the resilient check factor if your environment does not have resilient path to zoned storage by design.

3.6.10.2 New SFP Metrics Time Series Report

A new global SFP Report is provided in SANnav v2.3.0 to display time series data of optical parameters for FC ports managed by SANnav. The report will contain all SFP meta data and FC port connectivity information and contains the following SFP metrics for each FC port:

- Voltage (mV)
- Current (mA)
- Rx Power (dBm, uW)
- Tx Power (dBm, uW)
- Temperature (Celsius)

NOTE Only fabric filters are supported. Other filters such as Switch, Switch Port etc. if applied to this Report Template will be ignored as is done for other reports.

NOTE All offline zone members (members which are not connected to fabrics but zoned) will be ignored in the generated report.

3.6.10.3 New and Enhanced Reports

With SANnav v2.3.0 there are a few reports that have been enhanced to provide better usability or formatting and a few new reports that have been added.

The following *important* assumptions apply to all reports in general as explained below.

- The user’s AOR (Fabrics that the user can manage) is honored while generating a report.
- If a Fabric is Unmonitored at the time of report generation, it will be ignored.
- Even though the SANnav User Interface allows the user to specify arbitrary filters such as Switch filter, Switch Port filter, etc., for most SANnav reports, only the filter of type Fabric is honored. The other applied filter types will simply be ignored during the report generation.
- All offline zone members (members which are not connected to fabrics but zoned) are ignored.

3.6.10.3.1 New Device Connectivity Report

A new report template widget named “Device Connectivity” is provided in SANnav v2.3.0. This report considers zoning information (standard, peer, LSAN) to generate a complete connectivity map in .csv format for each device port managed by SANnav.

The Device connectivity Report displays end to end connectivity between each SANnav managed host port and storage port based on the current Effective zone configuration in each managed Fabric.

This report is useful to get a complete device end to end connectivity in a table (.csv) format for various inventory-like use cases. Note that the only supported format to export the report is .csv.

NOTE If there is no effective zone configuration defined in the fabric, the device connectivity report will not be created for that fabric.

3.6.10.3.2 Enhanced Chassis Report

In SANnav releases prior to SANnav v2.3.0, SANnav chassis report template creation showed four tables (Chassis, Chassis Blades, Chassis Fans and Power Supplies)

When the report was generated, SANnav UI would display 1 table (for all chassis), and for each Chassis, it displayed one table for Blades, one table for Power Supplies and one table for FANs.

As an example, for five Director chassis, 16 sections were shown in the UI report:

- 1 table for all chassis (name, WWN, IP, Health, State, Model, etc.)
- 5 tables for FRU/Blades (section repeated for each chassis)
- 5 tables for Fans (section repeated for each chassis)
- 5 tables for Power Supplies (section repeated for each chassis)

However, when the Chassis report was exported in .csv, only four distinct .csv files were generated as follows:

- 1 file for all Chassis properties (name, WWN, IP, Health, State, Model, etc.)
- 1 file for FRU/Blades (for all chassis)
- 1 file for Fans (for all chassis)
- 1 file for Power Supplies (for all chassis)

With SANnav v2.3.0, the UI report now matches the four .csv files exported (only four sections, Chassis, Blades, FANs, and Power Supplies as opposed to 16 in the example above).

3.6.10.3.3 Time Series Report Enhancements

3.6.10.3.3.1 Metadata Connectivity Information in Report Template

Time series reports for Port Utilization, Port Errors, and Port Traffic have been enhanced with the addition of three new columns in the generated CSV file. These three columns are:

- Connected Device
  - Host name or Storage name
- Connected Port
  - If F-Port: Zone Alias or empty
  - If E-Port, EX-Port, N-Port: switch port name or empty
- Connected Port PWWN
  - If F-Port: PWWN of connected device port
  - If E-Port, EX-Port, N-Port: PWWN of connected switch port

3.6.10.3.3.2 Generate One .csv File (All Entities)

In SANnav releases prior to SANnav v2.3.0, a time-series widget report generated one .csv file for each instance of the widget SAN entity (chassis/ port/ tunnel/circuit/flow).

For example, in the case of a time series port widget, if the user selected 100 ports, then 100 individuals .csv files were generated for time series data (one per port). The user was then expected to consolidate these files using SANnav provided scripts.

With SANnav v2.3.0, a single .csv file which contains all the time series data for all the 100 ports is now generated.

3.6.10.3.4 Consolidation of Top-N Port <Measure> into One Top-N Port Metrics

With SANnav v2.3.0, 11 Top performance widgets have been consolidated into one single widget named “Top Port Metrics”. Exporting the report will generate one .CSV file with all 11 metrics as new columns.

The 11 consolidated individual widgets are:

1. Top Port Utilization Percentage
2. Top Port BB Credit Zero
3. Top Port C3 Discard Rx Timeout
4. Top Port C3 Discard Tx Timeout
5. Top Port C3 Discards
6. Top Port CRC Errors
7. Top Port Link Failures
8. Top Port Link Resets
9. Top Port PCS Block Errors
10. Top Port Signal Losses
11. Top Port Sync Losses

The name of the consolidated Report Template widget is now:

- Top Port Metrics (aggregates all 11 widgets above into one single widget and report)

NOTE The 11 individual widgets are still available in SANnav v2.3.0 and can still be used individually.

3.6.10.3.5 Reports – Email Address Usability Enhancement

If a system e-mail address has not been provided to automatically email the user generated reports, a new pop-up dialog will indicate to the user that a SANnav email address must be setup. Go to SANnav > Services > SANnav Email Setup to configure a system e-mail.

3.6.11 Events and Violations

3.6.11.1 Automatically Create SANnav Event Action Policy (EAP) Filter from a Given Event

For events that contain a valid “Message ID” an Event Action Policy (EAP) filter can be automatically created in SANnav v2.3.0. This eliminates the need to remember the Message ID to create the EAP filter.

A new drop-down menu option is available for each Event that contains a valid Message ID to create a new Event Policy. The new menu is called “Create Event Policy”.

When clicking on this, a new EAP filter dialog is shown pre-populated with the correct Message ID filter. The user then only needs to provide the rest of the information, that is, list of switches to apply the EAP on, and Action to take on this and subsequent Events, such as “Suppress” or “email” or any valid SANnav action.

It is possible to create an EAP Filter in bulk for up to 10 user selected Events. A special SANnav naming convention is used to name the EAP filter which can be overridden by the user.

- Single Event - examples of generated SANnav EAP names:
  - SANnav_EM_1034_1
  - SANnav_EM_1034_2
  - SANnav_EM_1035_2
  - Etc.
- Multiple Events - examples of generated SANnav EAP names (10 at most in a single bulk operation)
  - SANnav_Multiselect_1
  - SANnav_Multiselect_2
  - Etc.

3.6.11.2 Raise a Single SANnav Application Event for Bulk Operations

With releases of SANnav prior to v2.3.0, one application event was raised for each object involved in the bulk operation. The generated SANnav Application Event in case of bulk operations indicated Success, Failure or Partial Success of the operations without specifically listing for which entity the operation failed and for which it succeeded.

With SANnav v2.3.0, a single application continues to be raised, however the user can now invoke a ‘Show Details” option menu on the Events page to view the details of the operation when it applies to multiple entities.

The Bulk Application Event Details applies currently for the following bulk operations:

- Bulk Zoning operations: Bulk delete of Zones and Zone Aliases
  - Message IDs: SSMP-ZONE-1003, SSMP-ZONE-1009, SSMP-ZONE-1059, SSMP-ZONE-1060
- Bulk Inventory operations: Port Enable/Disable/Persistent Disable
  - Message IDs: SSMP-INVT-7038,SSMP-INVT-7039

3.6.11.3 Add ALL as a Value for Violations and Events Filters

With SANnav v2.3.0, the Filters for Violations and Events now support the value “**ALL**” for the following filter attributes:

- “*Category*” (for both Events and Violations)
- “*Event Column*” (for Events filters and Forwarding filters) – ALL option valid only if *Category* is not set to ALL.

3.6.11.4 New Category for vCenter Events

In the SANnav Events page under Fault → Events the column “Category” has now a new value for events received directly from a SANnav defined vCenter server.

It is also possible to filter on this new Category value to display these specific vCenter Events.

When upgrading from previous releases of SANnav, the Category “vCenter” will be displayed accordingly (as vCenter) for events received prior to upgrading to SANnav v2.3.0.

3.6.12 Alarm Enhancements

With SANnav v2.3.0, a new enhancement is provided to auto escalate the Alarm object severity based on the event persisting for a specific amount of elapsed *time*. This is provided in addition to an existing auto escalation of the Alarm severity based on event *count*.

In SANnav v2.3.0, two Alarm objects will provide this time-based severity escalation as follows:

- Loss Of Signal (LOS) Alarm
  - The default severity for this alarm is "*Warning*" and the escalation sequence is as follows:

    - After 60 minutes from the time the alarm last occurred, the severity will be raised to "*Major*" if the events persist.
    - After 120 Minutes from the time the alarm last occurred, the Alarm severity will be raised to "*Critical*" if the events persist.
- Oversubscription Alarm
  - The default severity for this alarm is "*Major*" and the escalation sequence is as follows:
    - After 30 minutes from the time the alarm last occurred, the Alarm severity will be raised to "*Critical*" if the events persist.

3.6.13 Topology Enhancements

3.6.13.1 Hosts with Only Contain NPIV Ports as a Topology Context

This feature works in conjunction with the feature described in the Inventory section 3.6.7.3.

In release prior to SANnav v2.3.0, any host or server for which the Physical port and NPIV ports exist on different host enclosures, the topology would not show connectivity information for such hosts incorrectly. This is typical in environment having IBM VIO servers or HP AIX servers.

With SANnav v2.3.0, when the Host selected as a context is a host that only contains NPIV ports, SANnav will display a new “*Virtual Port”* group node (one group for all the NPIV ports mapped to a single physical Port PWWN).

Every “Virtual Port Group” node will have a menu item called “*Show Virtual Ports*” which will launch the existing “Virtual Ports Dialog” which will display only the virtual ports present in this group.

When a given port is a virtual port whose parent physical port resides in another host, the “Show Properties” of the Virtual Port will now show additional information to identify the physical port information by adding the following four new properties to the Virtual Port Properties:

- Physical Port Host
- Physical Port WWN
- Physical Port Zone Alias
- Physical Port FC Address.

In addition, at the Host level, there is a new menu called “Show all Virtual Ports” which will display the virtual ports and their relationship with their contained physical port PWWN. The Show Virtual Ports menu will display a table with the following column for each virtual port in the Host:

- Existing Columns
  - WWN
  - Zone Alias
  - FC Address
- New Columns in SANnav v2.3.0:
  - Physical Port Host
  - Physical Port WWN
  - Physical Port Zone Alias
  - Physical Port FC Address
  - Connected Switch Port
  - Connected Switch
  - Connected Fabric

3.6.13.2 New Menu “Show in Topology” for Trunks and Extension Tunnels

With SANnav v2.3.0, a new menu is added to each ISL/IFL/F-Port Trunk or Extension Tunnel called ‘Show in Topology”.

When invoked, this menu will display the source and end ports of the Trunk or the Tunnel in context in SANnav Topology.

3.6.13.3 Enhanced Device Port Connectivity through Cascaded AGs

With releases priori to SANnav v2.3.0, when a device (host or storage) is connected through a pair of switches in AG mode in a cascaded fashion (cascaded AGs), the SANnav Topology does not explicitly display the entry switch port in the Fabric.

With SANnav v2.3.0, the properties of the device port attached to the AG will now list three new properties to clearly identify the Fabric entry switch port. This is done with three new properties in the device port:

- Edge Switch Port WWN
- Edge Switch Port Name
- Edge Switch Name

3.6.13.4 Add “Filter by Zone” to Host and Storage Topology Contexts

A new Zone sub-context will be enabled when a Storage/Host is selected as a primary context. This is equivalent to using the “Filter by Zone” menu on a Host or Storage port. This is provided for ease of use and consistency.

3.6.14 Flow Management

SANnav v2.3.0 Flow Management feature has undergone several important changes. Refer to section on features removed and features deprecated in this document for more details. Specifically:

- Gen 6 collections and associated reports removal
- Flow Management support on “large” deployment platforms only (no support on “small” platforms)
- Deprecated Reports

With SANnav v2.3.0 and FOS v9.2.0 new features are introduced for managing flows in SANnav and are described in the following sections.

3.6.14.1 Support FOS v9.2 Flow Violations Streaming

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).

The Flow Violation streaming is not supported on all FOS hardware platforms. Refer to the SANnav Management Portal User Guide for details of which platform are support Flow Management features.

The Flow investigation view will show these new violations in the time series graph. For example, for the Read Exchange Completion Time (RD ECT), in addition to the existing “RD ECT Max” and “RD ECT Average” metrics, a new metric called “RD ECT Violated IO %” will display a time series graph of the percentage violated IOs for the RD ECT measure. The same example extends for all violated measures:

- ECT (R/W) Violated %
- FRT (R/W) Violated %
- Pending IOs (RD/WR) Violated %
- Abort Violated %
- Reserve Violated %
- Total IO Errors Violated %
- Timeouts Violated %

3.6.14.2 New IO Health and IO Latency Widget

Based on the flow violations streamed to SANnav v2.3.0, 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 in memory for the last two hours. This widget is meant as a troubleshooting widget to determine (five minutes refresh cycle) what are the device ports 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

3.6.14.2.1 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.

3.6.14.3 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 150K flows total which is the current flow scale supported and tested/validate in SANnav v2.3.0. When there are more than 150K 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.

NOTE Flow Management is only supported on “large” platforms (96GB RAM, 24 vCPUs, 1.2TB storage) with an Enterprise license. Flow Management is not supported for Base licenses (even in cases where the Base license has been installed on a "large” server configuration).

3.6.15 UI/UX and Usability Changes

Several UI/UX changes have been implemented in this release. A few highlights of the usability UI/UX changes are listed below. Refer to the *SANnav Management Portal User Guide* for complete details and screenshots.

- All Table Actions for any components in SANnav will be moved under the “hamburger” menu as per new UX Design Guidelines.
- There are three major areas where this “hamburger” menu is shown for a table:
  - Main table (e.g., Switches Page)
  - Embedded table (e.g., Switch Port table on the switch Detail page).
  - Expanded table dialog (e.g., Switch Port table Expansion on the switch detail page)

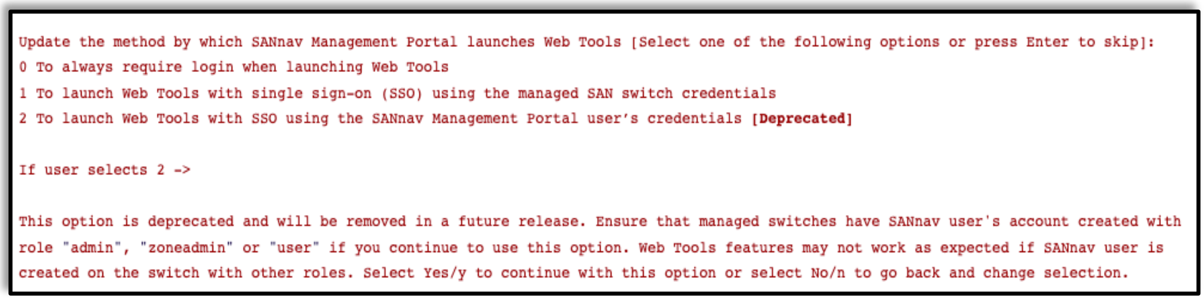
3.6.15.1 Usability Changes in Extension Tunnels/Circuits Configuration

- Circuit configuration
  - Extension Circuit “Maximum Bandwidth” and “Minimum Bandwidth” are now expressed in MB/sec and is consistent across all Extension hardware platforms and SANnav user interface screens.
  - With SANnav v2.3.0, a new “VLAN ID” attribute is added to both source switch and destination switch to allow a user to specify different VLAN configuration on the source and destination switches. This applies to both non HA and HA use cases.
    - **NOTE:** The L2Cos fields will be disabled (greyed out) if the VLAN IDs are not specified.

3.7 Features Deprecated with SANnav Management Portal v2.3.0

The following features are deprecated in SANnav v2.3.0. “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” is now deprecated. This feature allows a switch centric MAPS policy management. Broadcom recommends using the SANnav → SAN Monitoring → “Configuration Policy Management” feature instead as it addresses most common use cases workflows in more efficient manner.
- Launching WebTools using SANnav user’s credentials is deprecated in SANnav v2.3.0. This is the option number 2 in the installation scripts as shown below. Note that this option (Option 2) only works if the SANnav user is a Local user (not a remote user such as LDAP or any other authentication protocol).



```
Update the method by which SANnav Management Portal launches Web Tools [Select one of the following options or press Enter to skip]:
0 To always require login when launching Web Tools
1 To launch Web Tools with single sign-on (SSO) using the managed SAN switch credentials
2 To launch Web Tools with SSO using the SANnav Management Portal user’s credentials [Deprecated]

If user selects 2 ->

This option is deprecated and will be removed in a future release. Ensure that managed switches have SANnav user's account created with
role "admin", "zoneadmin" or "user" if you continue to use this option. Web Tools features may not work as expected if SANnav user is
created on the switch with other roles. Select Yes/y to continue with this option or select No/n to go back and change selection.
```

- The following nine Reports are deprecated with SANnav MP v2.3:
  1. Time Series – Flows
  2. Top Flows – IO Exceptions
  3. Top Flows – Other (non-Read/Write) commands
  4. Top Host Port Pending IOs
  5. Top Storage Port Pending IOs

6. Top Storage Port Data Rate
7. Top Storage Port ECT
8. Top Storage Port FRT
9. Top Storage Port IOPS

3.8 Features Removed from SANnav Management Portal v2.3.0

The following features are no longer available with SANnav v2.3.0:

- Starting with SANnav v2.3.0, SANnav Trial License is no longer available. Customers wishing to trial SANnav software may download and install previous versions of SANnav as follows:
  - 90-day trial license was available with all SANnav releases through v2.2.0x
  - 30-day trial license available with SANnav v2.2.1x and v2.2.2x
- SANnav MP and GV license 30-day grace period (available after license expiration) has been removed.
  - When the SANnav license expires, all SANnav functions will be restricted following the expiration date.
  - SANnav will continue to run and monitor the environment, but UI will not be available (except for the ability to install a new license)
  - The 30-Day Grace period will continue to be available up through SANnav v2.2.x releases.
- D-Port Test feature
  - The *scheduling* option for D-Port testing from the Switch Port Inventory has been removed. It is still possible to perform D-Port testing on switch ports, however, the request can no longer be scheduled (on-demand only.
  - Due to the large amount of time it takes to run the Diagnostics tests (D-Port test), the number of concurrent ports (bulk) that can be selected for running the D-Port test is now limited to *8 ports* (E_Port or F_Port)
  - Note that *Electrical and Optical Loopback Tests* are also removed from FOS 9.2.0. Link Traffic Test is the only available test for FOS 9.2.0
- Collection Management is no longer available. Up to SANnav v2.2.2.x the menu under “SANnav→SAN Monitoring→Collection Management” that allowed customers to view and manage Gen6 IT Flow Collections (only Gen6 and not Gen7, and only IT and not ITL/ITN or VITL/VITN) is removed in SANnav v2.3.0.
- As part of the removal of Gen6 IT collection management, the following associated two reports are also removed from SANnav v2.3.0 consequently:
  - Top Flow Gen6 Collection report
  - Gen6 Flow Collections time series report
- With SANnav v2.3.0 Flow Management will only be supported on “large” platforms that is platforms with 96GB RAM/24vCPUs/1.2 TB storage. Flow Management is no longer supported on “small” platforms with 48GB RAM/16vCPU/600GB storage.

3.9 Important Considerations when Upgrading to SANnav v2.3.0

This section highlights key points to consider during upgrade and migration from previous releases of SANnav MP to SANnav MP v2.3.0.

If any or all these considerations is a concern, then customers are advised to stay on the previous release (i.e., SANnav v2.2.x) and to not upgrade/migrate to SANnav v2.3.0.

Refer to the *SANnav Management Portal v2.3.0 User Guide* under the section “Features Affected by Upgrade and Migration” for more details on behaviour changes and consideration during upgrade and migration from SANnav v2.2.x to SANnav v2.3.0

3.9.1 Flow Management

- Any flow related data from previous SANnav release will not be migrated to SANnav v2.3. This includes the flows objects themselves as well as their associated flow telemetry data.
- Flow Management functionality along with flow data will not be available post upgrade/migration to SANnav v2.3.0 on “small” platforms.
- Backing up a SANnav instance on a large platform and restoring it on a small platform running SANnav v2.3.0 is not recommended. The flow data will not be migrated on the small SANnav v2.3.0 platform as flow management is not supported on small platforms.

3.10 SANnav Management Portal v2.3.0 Supported SAN Switches

3.10.1 Platform Support and FOS Support – New Policy

Starting with SANnav v2.3.0, 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 v2.3.0.

3.10.1.1 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 Brocade G730 Brocade X7-4 Brocade X7-8 Brocade 7850	FOS v9.1.0d and later FOS v9.1.1b and later FOS v9.2.0x
Gen 6 Switches	Brocade G610 Brocade G620 Brocade G620 (switchType 183) Brocade G630 Brocade G630 (switchType 184) Brocade 7810 Extension Switch Brocade X6-4 Brocade X6-8 Brocade MXG610s Blade Server SAN I/O Module Brocade G648	FOS v9.0.1e1 and later FOS v9.1.0b and later FOS v9.1.1b and later FOS v9.2.0x
Gen 5 Switches	Brocade 7840 Extension Switch Brocade DCX 8510-4 Brocade DCX 8510-8 Brocade 6505 Brocade 6510 Brocade 6520 Brocade M6505 Blade Server SAN I/O module Brocade 6542 Blade Server SAN I/O module Brocade 6543 Blade Server SAN I/O module Brocade 6547 Blade Server SAN I/O module Brocade 6548 Blade Server SAN I/O module 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 v2.3.0 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.

Max Switch Ports Under Management (Base or Enterprise)	**Operating System**	**Host Type**	**Minimum vCPU**	**Memory**	**Hard Disk**
Small 600 Ports (Base) or, 3000 (Enterprise)	RHEL 8.4, 8.6 (*)	Bare metal/VMware ESX7.0 VM Bare metal/HyperV Windows Server 2022 VM	16 vCPUs	48 GB	600 GB
Large 15000 (Enterprise)	RHEL 8.4, 8.6 (*)	Bare metal/VMware ESXi 7.0 VM Bare metal/HyperV Windows Server 2022 VM	24 vCPUs	96 GB	1.2 TB

- (*) Other RHEL releases are not explicitly qualified or supported.
- Specifically, RHEL 8.2, 8.3, 8.5, 8.7, and 8.8 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 are not supported; the installation script exits if RHEL 8.0 or 8.1 is running on the SANnav host.
- RHEL 9.0 is not supported; the installation script exits if RHEL 9.0 is running on the SANnav host.
- 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.

Max Switch Ports Under Management (Base or Enterprise)	**Supported Hypervisor**	**Host Type**	**Minimum vCPU**	**Memory**	**Hard Disk**
Small 600 Ports (Base) or, 3000 (Enterprise)	VMware ESXi 7.0	VMware ESXi VM	16 vCPUs	48 GB	600 GB
Large 15000 (Enterprise)	VMware ESXi 7.0	VMware ESXi VM	24 vCPUs	96 GB	1.2 TB

- SANnav MP v2.3.0 OVA packages **Rocky Linux 8.6** in the .ova file
- 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 v2.3.0 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 Installation and Migration Guide* for complete details.

Supported Upgrade and Migration Paths to SANnav v2.3.0:

Current Version	New Version	Supported?	Comments
SANnav 2.1.x and earlier	SANnav v2.3.0	No	Support only Major releases up to "N-1" upgrades. N=3 for SANnav v2.3.x
SANnav v2.2.0x	SANnav v2.3.0	No	SANnav v2.2.0 was BR GA 12/15/2021. Therefore, it is not a valid upgrade path to SANnav v2.3 (over 1 year) as per Brocade support policy.
SANnav 2.2.1x	SANnav v2.3.0	Yes	To upgrade from SANnav v2.2.1 to SANnav v2.3 in OVA deployment case *only,* it is required to perform an inline upgrade to SANnav v2.2.2 first, and then proceed with upgrade to SANnav 2.3.
SANnav 2.2.2x	SANnav v2.3.0	Yes	SANnav v2.2.2.x and SANnav v2.2.2a to SANnav v2.3.0 upgrade/migration are both supported

- SANnav v2.2.2.x to SANnav v2.3.0 OVA upgrade/migration requires full extraction of the OVA and upgrade/migration due to disruptive OS change (CentOS 7.9 → Rocky 8.6)
- Refer to *SANnav Installation and Upgrade Guide* for details before attempting SANnav MP upgrade in all deployments.

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).

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 with SANnav v2.3.0

- SANnav Management Portal v2.3.0 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 versions up to and including SANnav v2.2.0 have a 90-Day Trial period embedded.
  - 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 v2.3.0
- With SANnav v2.3.0, 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 v2.3.0, the SANnav license file (license.xml file) 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 *SANnav Management Portal v2.3.0 User Guide*, section Licensing 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 v2.3.0, 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 *SANnav Management Portal v2.3.0 User Guide*, section Licensing for details on how to export the License Renewal Request file from the SANnav UI.

Chapter 6: Scalability

6.1 SANnav Management Portal v2.3.0 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. 1-hour data is stored for 30 days. 1-day aggregated data is stored for 30 days. 2-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. 1-hour data is stored for 30 days. 1-day aggregated data is stored for 30 days. 5-second samples are collected for up to 3 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 (15K ports) “large” platform only. No support on “small” platforms 100k Flows tested and validated. Up to 150K Flows maximum allowed (not blocked). Blocked > 150K flows.	
Flow statistics stored	5-minute samples are stored for up to 8 days. 1-hour data is stored for 30 days. 6-hour aggregated data is stored for 30 days. 6-hour samples are stored for 30 days. 10-second real-time data can be viewed up to 30 minutes.	
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 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.
- Applying TruFOS certificate from SANnav fails on FOS v9.1.1. Users need to upgrade to FOS v9.1.1a or use CLI to install TruFOS certificate on switches running FOS v9.1.1.
- Disaster Recovery (DR) is supported for SANnav Management Portal on VM or OVA deployments *only*. SANnav MP DR is *not* supported on bare metal deployments. DR is *not supported* on Global View (all deployments)
- 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

- 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:

    Step 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**.

    Step 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 v2.3.0 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 v2.3.0, 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 migrating to SANnav Management Portal v2.3.0 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.
- When migrating from previous releases to SANnav v2.3.0 , 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”.
- When migrating from previous releases to SANnav v2.3.0, IPSec policies configured for the Extension tunnels are not migrated. To work around this, the user has three options:
  1. Ignore the existing IPSec policies and create a new one and associate it with the tunnels.
  2. Delete and re-discover the fabrics in which the Tunnels were present to keep the existing IPSec policies.
  3. If neither option is acceptable, contact Broadcom Support.

7.3 Firmware Management and Support Save

- By default, port 22 is used for SANnav internal firmware repository. However, this port number can be changed during installation. An alternative port number can be selected for the SANnav internal firmware repository except when managing switches running an earlier Fabric OS version than v8.2.2. In the scenario, where SANnav is managing switches running an *earlier version than v8.2.2* and SANnav's server port 22 is unavailable, select the option of using an external FTP, SCP, or SFTP server for switch supportsave and firmware download functionality.
- 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>`
- A switch Supportsave or firmware download operation initiated via SCP or SFTP protocol from SANnav Management Portal for the switches running Fabric OS v9.0 and above does not require the `sshutil delknownhost` option.
- 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.
- When port 22 is used by SANnav as an SCP/SFTP port and when a user attempts to collect a switch Supportsave, the operation from SANnav Management Portal will fail in the following scenario (all 3 steps below must all be performed in the order specified for the failure to happen) for switches running Fabric OS v9.1.0x and v9.1.1:
    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 on the same host and has attempted to either perform a switch Supportsave or a firmware download for the same switch that was used in Step 1.

    - To recover from this situation, log in to the switch console on which the 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>`
- 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

- If a chassis that is being used as a seed switch has the “Virtual Fabrics” attribute enabled, discovering more than four logical fabrics in that chassis is not recommended. The user is recommended to use any other switch that is part of the logical fabric as the seed switch. If users attempt to discover more than 4 logical fabrics, the discovery operation may take anywhere from 20 minutes to an hour to complete.
- It is mandatory to add a filter when generating any Time Series Flow reports; otherwise, the generated report will be empty. The UI does not enforce a filter to be applied.
- 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.
- SANnav creates a new SNMP v3 user on the switch during initial discovery. Prior to SANnav v2.2.1, this user was created with "Authorization Protocol" set to "None" and "Privileged Protocol" set to "None".
  - Starting with SANnav v2.2.1 and above, this SNMP user is created with "Authorization Protocol" and "Privileged Protocol" set to the most secure values.
  - The password provided during Fabric/Switch discovery will be used as the password values for both fields.
  - If the switch already has an SNMP v3 user with this username but with different "Authorization Protocol" and "Privileged Protocol" credentials, the SNMP credentials for the switches will need to be provided at time of Fabric Discovery. This doesn't impact SANnav upgrade and data migration.
- A switch will become *Unreachable* after upgrade 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.

- Prior to SANnav v2.3.0, the number of records included in the SANnav Support Data Collection, SSDC (*Partial* SSDC) was based on a time range selected by the user (e.g., last 7 days). With SANnav v2.3.0, the time selection has been removed from the UI and for "Partial" SANnav Support Data Collection the number of events and violations included in the SSDC are the last 10,000 records (irrespective of time) for each Events and Violations.

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 "<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, 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 v2.3.0

- **CVE-2022-40664**

Apache Shiro contains an authentication bypass vulnerability when it is forwarding or including requests using RequestDispatcher component. This could allow an attacker to gain unauthorized access to the application.

- **CVE-2022-25647**

The package com.google.code.gson:gson before 2.8.9 are vulnerable to Deserialization of Untrusted Data via the writeReplace() method in internal classes, which may lead to DoS attacks.

- **CVE-2023-21830**

Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf;
Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data.

- **CVE-2023-21835**

Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1;
Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition.

- **CVE-2023-21843**

Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data.

- **CVE-2016-1000027**

Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required. NOTE: the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.

- **CVE-2015-1315**

Buffer overflow in the charset_to_intern function in unix/unix.c in Info-Zip UnZip 6.10b allows remote attackers to execute arbitrary code via a crafted string, as demonstrated by converting a string from CP866 to UTF-8.

Brocade SANnav contains the affected open source routines, but these routines are not in the execute path accessible to users. While Brocade SANnav is not vulnerable to this CVE, a security update is being provided in SANnav version v2.3.0 to remove the vulnerable component.

- **CVE-2017-7657**

In Eclipse Jetty, versions 9.2.x and older, 9.3.x (all configurations), and 9.4.x (non-default configuration with RFC2616 compliance enabled), transfer-encoding chunks are handled poorly. The chunk length parsing was vulnerable to an integer overflow. Thus, a large chunk size could be interpreted as a smaller chunk size and content sent as chunk body could be interpreted as a pipelined request. If Jetty was deployed behind an intermediary that imposed some authorization and that intermediary allowed arbitrarily large chunks to be passed on unchanged, then this flaw could be used to bypass the authorization imposed by the intermediary as the fake pipelined request would not be interpreted by the intermediary as a request.

Brocade SANnav contains the affected open source routines, but these routines are not in the execute path accessible to users. While Brocade SANnav is not vulnerable to this CVE, a security update is being provided in SANnav version v2.3.0 to remove the vulnerable component.

- **CVE-2018-1273**

Spring Data Commons, versions prior to 1.13 to 1.13.10, 2.0 to 2.0.5, and older unsupported versions, contain a property binder vulnerability caused by improper neutralization of special elements. An unauthenticated remote malicious user (or attacker) can supply specially crafted request parameters against Spring Data REST backed HTTP resources or using Spring Data's projection-based request payload binding that can lead to a remote code execution attack.

Note: Brocade SANnav versions v2.2.1 and v2.2.2 contain the affected open source routines, but these routines are not in the execute path accessible to users. While Brocade SANnav is not vulnerable to this CVE, a security update is being provided in SANnav version v2.3.0 to remove the vulnerable component.

- **CVE-2018-17190**

In all versions of Apache Spark, its standalone resource manager accepts code to execute on a 'master' host, that then runs that code on 'worker' hosts. The master itself does not, by design, execute user code. A specially crafted request to the master can, however, cause the master to execute code too. Note that this does not affect standalone clusters with authentication enabled. While the master host typically has less outbound access to other resources than a worker, the execution of code on the master is nevertheless unexpected.

Note: Brocade SANnav versions v2.2.0, v2.2.1 and v2.2.2 contain the affected open source routines, but these routines are not in the execute path accessible to users. While Brocade SANnav is not vulnerable to this CVE, a security update is being provided in SANnav versions v2.2.2a and v2.3.0 to remove the vulnerable component.

- **CVE-2022-2625:**

A vulnerability was found in PostgreSQL. This attack requires permission to create non-temporary objects in at least one schema, the ability to lure or wait for an administrator to create or update an affected extension in that schema, and the ability to lure or wait for a victim to use the object targeted in CREATE OR REPLACE or CREATE IF NOT EXISTS. Given all three prerequisites, this flaw allows an attacker to run arbitrary code as the victim role, which may be a super user.

- **CVE-2022-41946:**

Pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using either `PreparedStatement.setText(int, InputStream)` or `PreparedStatemet.setBytea(int, InputStream)` will create a temporary file if the InputStream is larger than 2k. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system.

- **CVE-2022-22950:**

In Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service condition.

- **CVE-2023-31925**

Brocade SANnav before v2.3.0 and v2.2.2a stores SNMPv3 Authentication passwords in plaintext. A privileged user could retrieve these credentials with knowledge and access to these log files. SNMP credentials could be seen in SANnav SupportSave if the capture is performed after an SNMP configuration failure causes an SNMP communication log dump.

- **CVE-2023-31424**

Brocade SANnav web interface before Brocade SANnav v2.3.0 and v2.2.2a allow remote unauthenticated users to bypass web authentication and authorization.

- **CVE-2023-31423**

Possible information exposure through log file vulnerability where sensitive fields are recorded in the configuration log without masking on Brocade SANnav before v2.3.0 and 2.2.2a.

Notes: To access the logs, the attacker must first collect support data collection on Brocade SANnav or have access to an already collected support data collection outputs

- **CVE-2022-43937**

Possible information exposure through log file vulnerability where sensitive fields are recorded in the debug-enabled logs when debugging is turned on in Brocade SANnav before v2.3.0 and 2.2.2a

- **Azul Zulu Java Multiple Vulnerabilities (CVE-2022-21618 CVE-2022-21619 CVE-2022-21624 CVE-2022-21626 CVE-2022-21628 CVE-2022-39399)**

The version of Azul Zulu installed on the remote host is prior to 6 < 6.51 / 7 < 7.57.0.14 / 8 < 8.65.0.14 / 11 < 11.59.16 / 13 < 13.51.14 / 15 < 15.43.14 / 17 < 17.37.14 / 19 < 19.30.12. It is, therefore, affected by multiple vulnerabilities as referenced in the 2022-10-18 advisory.

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JGSS). Supported versions that are affected are Oracle Java SE: 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition.
  Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run

untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21618)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21619)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21624)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21626)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). (CVE-2022-21628)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). (CVE-2022-39399)

- **Java April 2022 CPU update**

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is affected by multiple vulnerabilities as referenced in the April 2022 CPU advisory:

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21449)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21476)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21426)

• Java July 2022 CPU update

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is affected by multiple vulnerabilities as referenced in the July 2022 CPU advisory:

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-21540)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-21541)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 17.0.3.1; Oracle GraalVM Enterprise Edition: 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability

can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-21549)

- Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Native Image (Gson)). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle GraalVM Enterprise Edition executes to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM Enterprise Edition. (CVE-2022-25647)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP (Xalan-J)). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-34169)

• Azul Zula OpenJDK update

The version of Azul Zulu installed on the remote host is prior to 6 < 6.45 / 7 < 7.51.0.12 / 8 < 8.59.0.12 / 11 <11.53.14 / 13 < 13.45.12 / 15 < 15.37.14 / 17 < 17.32.14. It is, therefore, affected by multiple vulnerabilities as referenced in the 2022-01-18 advisory.

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311,11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).(CVE-2022-21248)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector:CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). (CVE-2022-21277, CVE-2022-21366)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). (CVE-2022-21282, CVE-2022-21296)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). (CVE-2022-21283)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data.

  Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).(CVE-2022-21291, CVE-2022-21305)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition.

  Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).(CVE-2022-21293, CVE-2022-21294, CVE-2022-21340)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition.

  Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). (CVE-2022-21299)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle

GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).(CVE-2022-21341)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
(CVE-2022-21349)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition.

  Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).(CVE-2022-21360, CVE-2022-21365)

Chapter 9: Defects

9.1 Known Issues in SANnav Management Portal v2.3.0

Defect ID	Description
SANN-138248	On a setup configured for disaster recovery, data replication continues even if the sync is paused.
SANN-139712	Unable to log into SANnav client as proxy service does not start.
SANN-141437	Drift check fails occasionally for some of the switches with an error.
SANN-141996	Incorrect data is shown for traffic measures for F-port trunk.
SANN-142213	Sometimes firmware download status shows completed in SANnav even though it has not completed on the switch.
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-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).

9.2 Defects Closed with Code Change in SANnav Management Portal v2.3.0

Defect ID	Description
SANN-132747	'Add Member' dialog is empty in the Zoning page.
SANN-133624	SANnav UI shows incorrect time.
SANN-133697	Chassis Investigate view goes blank.
SANN-133807	SANnav proxy service fails to start after migration from 2.1.x to 2.2.0
SANN-133904	Migration to SANnav 2.2.0 fails.
SANN-133968	SNMP Forwarding filter is not filtering some events.
SANN-133996	Cannot log into SANnav using LDAP user.
SANN-134064	Cannot upload data from SANnav via built-in SCP/SFTP server to bsnsupport.broadcom.com site.
SANN-134178	User cannot create a peer zone using alias member type.
SANN-134194	Unable to add members to existing peer zones.
SANN-134286	When a host group is expanded in Topology, the scroll bar does not disappear even if the window is resized to make all entries visible.
SANN-134288	Storage paths for hosts are not shown in the topology view.
SANN-134305	The topology view shows an error message that the device is not accessible to the user.
SANN-134355	Zoning and a few other properties are not displayed in the Switch Port details page.
SANN-134407	PSD versions of firmware imported into the SANnav repository are incorrectly displayed as supported for all platforms.
SANN-134440	Events and Violations pages do not show data, users see the error “Failed to fetch data. Service is not available at this time.”
SANN-134444	Investigate menu option is disabled.
SANN-134466	Historical data not shown in investigation view.
SANN-134544	Sometimes host entries are listed by IP address instead of FQDN.
SANN-134812	Sometimes accept fabric changes dialog displays with no entries.
SANN-135048	The user cannot log into SANnav.
SANN-135226	Ports shown twice in switch port inventory for some switches.
SANN-135361	The final firmware download completion status not shown in SANnav even though the firmware update is successful.
SANN-135518	In rare cases, firmware download status shows completed in SANnav even though it just started on the switch.
SANN-135582	Host and corresponding VMs will not be discovered showing "conflict-host" error.
SANN-135767	Newly learned VITL/ITL flows are not shown in flow inventory.
SANN-135951	Activate and Add/Remove options missing when viewing Zone Configurations.
SANN-135990	Intermittently, trying to bulk monitor multiple fabrics results in failure.
SANN-136022	Device port is incorrectly present in multiple device enclosures.
SANN-136026	SANnav doesn't forward RAS-1007 event.
SANN-136130	Incorrect items count shown in health details popup dialog.
SANN-136150	Sometimes firmware download status shows completed in SANnav even though it has not completed on the switch.
SANN-136210	Intermittently, SANnav shows firmware download status as completed, even though it failed on the switch.
SANN-136238	Error shown while editing LSAN zones.
SANN-136265	Disaster Recovery status on the primary node is indicating that the standby node is not installed.
SANN-136289	Port recommission operation fails.
SANN-136301	'Unknown Failure' error shown during discovery.
SANN-136313	The Health Summary Dashboard shows a reduced health score for some fabrics.
SANN-136323	'Product Address' and 'Object Name' columns are retained in the Events page
SANN-136346	In rare circumstances, Installation or Migration to SANnav 2.2.0 is blocked.
SANN-136349	Violation purge fails resulting in poor performance for violation page loading.
SANN-136370	Zone configuration details pop up shows continuous spinner.

SANN-136453	Health summary dashboard and switch details page (health details section) in Inventory is incorrectly reporting HTTPS protocol is not enabled.
SANN-136480	RADIUS/TACACS authentication fails occasionally.
SANN-136572	Fabric Discovery status shows "Not registered for SNMP traps" but SANnav is able to receive the SNMP informs.
SANN-136751	Signed security certificate is replaced with self-signed certificate.
SANN-137015	Missing Redundant Paths(ISLs, ICLs) health check is failing, though redundant paths present in the fabric.
SANN-137167	Switches/Access Gateways are shown as not reachable.
SANN-137216	CLI commands run via SANnav do not execute on some switches.
SANN-137322	SANnav password age is not updated properly.
SANN-137384	Performance Data is not collected after migrating to SANnav 2.2.1.
SANN-137498	Performance Data is not available after migrating to SANnav 2.2.1.
SANN-137585	The events list shows: "EEOS license not exist, switch 0.0.0.0".
SANN-137587	Migration fails for an unsupported scenario.
SANN-137820	Inventory-Switch Ports view does not show Connected Port info.
SANN-137846	Unable to change the seed switch for a fabric. SANnav client becomes unresponsive.
SANN-137847	Pushing Configuration Policy fails
SANN-137868	Adding a tag to an end device port takes longer than expected
SANN-138006	Linux audit.log file is filled with SYSCALL events.
SANN-138083	Some SNMP traps are not forwarded when a filter is set
SANN-138113	SANnav upgrade 2.2.0 to 2.2.1 failed, SANnav 2.2.1 directory is missing after the upgrade.
SANN-138114	Access Gateways do not show updated FOS levels after firmware download.
SANN-138154	Performance data is not shown in SANnav Dashboard, Investigation View and Reports.
SANN-138362	TruFOS certificate auto-retrieval fails in SANnav.
SANN-138505	Device port type (initiator/target) does not update in certain conditions resulting in reduction of Host health score
SANN-138508	Operations fail with a message "User update failed due to an internal server error".
SANN-138969	SANnav migration from v2.2.0 to v2.2.1 reports a successful completion, but multiple services do not start.
SANN-138979	Performance data is not displayed in SANnav dashboards, investigation view, and reports.
SANN-138994	Discovery operations (re-discover, monitor, accept changes, etc.) take around 15-minutes to complete.
SANN-138995	Switch which was disconnected and then re-connected to the fabric continues to be displayed as missing.
SANN-139055	Unable to remove scheduled switch config backup
SANN-139326	The Trunk is shown as missing in SANnav. when the master port is removed from the trunk in migrated server
SANN-139588	On host with NPIV ports, if NPIV ports are removed from the HBA, then after Accept Changes the Host is no longer visible in Inventory.
SANN-139620	Switch Supportsave collection fails due to SCP/SFTP service startup issue
SANN-139713	Certificate replacement fails due to invalid date and reports certificate is expired when it is not
SANN-139788	Delete option is not shown for zone configuration.
SANN-139832	The "Last Discovered" date/time is incorrect for Switches in Fabric discovery detail view.
SANN-140024	Cannot log into SANnav client.
SANN-140191	SNMP performance data collection fails
SANN-140260	AG Devices displayed in Storage Inventory search.
SANN-140279	Host port is shown under the old host enclosure even after re-mapping.
SANN-140312	ESXi host data is missing in Inventory.
SANN-140316	Need to display warning while bulk overriding call home FRU code configuration.
SANN-140400	Health Score Computation is not skipped for unselected factors.
SANN-140490	Unable to receive SNMP informs in SANnav.
SANN-140712	ESXi host is shown as unreachable in SANnav.
SANN-140795	ISL trunk is displayed in ISL trunks page even after deleting the trunk.
SANN-140810	The file system on the SANnav server (primary node) fills up with replication data.
SANN-140856	Configuration Drifts reported for identical Configuration
SANN-140924	Performance data is not shown for F-port trunks.

SANN-140949	Unable to accept new changes on the discovery page.
SANN-141193	SANnav displays incorrect status for host ports.
SANN-141213	Multiple duplicate aliases are created on the Fabric.
SANN-141744	Blank Screen when clicking on Investigate sidebar icon.
SANN-141773	The report generator service is down.
SANN-141798	Switch supportsave upload to Broadcom support site fails.
SANN-141818	Configuration Policy Block for SNMPv3 rejects the valid passwords
SANN-141858	POST /external-api/v1/inventory/enclosures/mapping API calls fail.
SANN-141909	Configuration policy push to switch fails with an error.
SANN-142253	Inventory shows duplicate host entries.
SANN-142265	Performance Data collection fails and SNMP traps are not received.
SANN-142335	Configuration push to the switch fails with an error.

9.3 Defects Closed without Code Change in SANnav Management Portal v2.3.0

Defect ID	Description
SANN-132057	'Accept Changes' dialog shows newly added switches and devices, but connections appear 2-4 minutes later.
SANN-133054	SSL certificate expiry date is not shown in the FOS Certificate Management page.
SANN-133752	SANnav services restart occasionally.
SANN-133775	Missing data points in the historical performance graph
SANN-133776	Zone configurations not shown in zone management.
SANN-133818	Migration to SANnav 2.2 failed.
SANN-133855	Switches marked unreachable in rare situations.
SANN-134015	Cannot use port 22 on a specific NIC for internal SSH.
SANN-134110	Services fail to start after migration from 2.1.x to 2.2.0.
SANN-134208	Cannot edit vCenter password in SANnav.
SANN-134283	Unable to investigate from the selection panel.
SANN-134306	SFP power is shown in mW instead of uW.
SANN-134354	Weblinker on switch restarts after a supportftp configuration block is pushed to switch.
SANN-134370	In the fabric discovery page, the last discovery time is displayed incorrectly.
SANN-134703	SANnav client is not accessible.
SANN-134710	SNMP informs are not received in SANnav.
SANN-134760	SANnav is not listing any Host or Storage ports in the Inventory views.
SANN-134782	"No data to display" message shown for historical and real-time performance metrics in investigation mode
SANN-134793	SANnav inventory does not display OEM model names for OEM-branded Brocade switches.
SANN-134805	Scheduled support save gets aborted for some switches occasionally.
SANN-134876	Device information is not updated in SANnav views such as Inventory, Topology, and Zoning.
SANN-134930	Discovery fails showing connection timeout message.
SANN-134950	Telemetry registration fails.
SANN-134978	Cannot enable a disabled port in Inventory.
SANN-135003	Config Policy drift check fails.
SANN-135027	Upgrade on Access Gateway shows old firmware version after upgrade completion.
SANN-135038	No Flows data is displayed in inventory.
SANN-135079	SANnav does not show an application event when a switch becomes unreachable.
SANN-135089	Generated Switch Support Save files are not listed in SANnav GUI.
SANN-135361	The final firmware download completion status not shown in SANnav even though the firmware update is successful.
SANN-135456	Details of new switch are not updated in SANnav.
SANN-135539	Fabric discovery fails.
SANN-135583	Performance data is not shown for port measures.
SANN-135761	User cannot edit the list of switches on the ESRS server
SANN-135819	SANnav database service is terminated by the operating system.
SANN-135894	Fabric name change is not reflected in SANnav immediately.
SANN-135901	Discovered switch is not shown in switches tab in MAPS policy management.
SANN-135913	Migration from SANnav v2.1.1 to v2.2.0 fails.
SANN-135991	Telemetry registration failure reported in notification panel.
SANN-136115	Event and violation report generation fails intermittently.
SANN-136129	Switch health is 'Poor' for some switches.
SANN-136175	Incorrect description displayed for event regarding performance data collection failure.
SANN-136188	An incorrect failure reason is displayed for the SNMP registration failure event.
SANN-136221	Migration from SANnav v2.1.1 to v2.2.0 fails.
SANN-136242	Inventory and FOS Version Management pages do not display the correct Fabric OS version.
SANN-136272	Generated reports are not purged as per the defined policy.

SANN-136278	In rare cases, SANnav displays a timeout error in the FOS Version Management page, even though firmware download is successful on the switch.
SANN-136292	Port performance data collection fails.
SANN-136299	Incorrect information shown in "Additional Port Info" in switch port inventory list view.
SANN-136328	Duplicate host port is shown in the Inventory Host Ports page.
SANN-136331	Host port information is not updated.
SANN-136457	Firmware update operation fails from SANnav.
SANN-136477	Unable to import configuration from switch.
SANN-136479	SANnav migration fails.
SANN-136486	“Show Rule" and "Edit” operation are not available for the MAPS rule in configuration policy & MAPS rules page.
SANN-136570	Unable to discover fabrics in SANnav.
SANN-137207	Incorrect port status is shown for host and storage ports.
SANN-137347	SFP status is invalid after it fails and gets replaced.
SANN-137353	SANnav restore operation shows an error, 'port not available'.
SANN-137500	Physical port data is incorrect for virtual/NPIV ports.
SANN-138059	Fault Management service failed to start.
SANN-138128	SNMP registration fails for embedded AGs.
SANN-138152	SANnav reports that the port is not available even though the port is free.
SANN-138233	Fabric discovery fails in certain conditions
SANN-138434	'Switch port added' notification pops up frequently.
SANN-138449	MAPS policy import fails without a clear reason.
SANN-138579	Switch configuration restore via SANnav does not work.
SANN-141482	Duplicate host enclosures are created.
SANN-141886	Performance Data collection fails and SNMP traps are not received.
SANN-141931	Mapping ports to a Host takes a longer time compared to SANnav v2.1.1.
SANN-142115	Port status is incorrectly displayed in SANnav inventory.
SANN-142724	MAPS Distribution fails.

Revision History

Version	Summary of Changes	Publication Date
1.0	Initial version of Brocade SANnav Management Portal v2.3.0 Release Notes (Digest Edition).	04/28/2023
1.1	Updated sections 3.5.x, 5.1 and 7.2.	05/16/2023
2	Updates on RHEL support, no support for RSA key discovery, OVA not launching automatically after extraction, added upgrade support from SANnav v2.2.2a to v2.3 and vCenter supported hosts scale limit now 200 hosts (from 300). Updated DR ports to be opened and URL change for various SANnav functions such as TruFOS, License renewals fetch, DR rehost license. Added URL Change note. Added CVE disclosures.	09/06/2023
3	Updated sections 3.5.x, 3.6.x, 3.10 and Chapter 7.	10/20/2023

BROCADE
A Broadcom Company