SANnav Management Portal 2.1.1

Brocade SANnav Management Portal 2.1.1 Release Notes

Version 1.2 (Digest Edition)

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

Table of Contents

Chapter 1: Release Contents

1.1 Brocade SANnav Management Portal 2.1.1 Release Overview

SANnav 2.1.1 is a minor maintenance release of Brocade’s two Fibre Channel SAN management software products, **Brocade SANnav Management Portal** and **Brocade SANnav Global View**.

Brocade SANnav Management Portal 2.1.1 is a software maintenance release introduced in order to support Fabric OS (FOS) 9.0.1 and to provide minor feature enhancements on SANnav Management Portal 2.1.0x.

This chapter highlights the new features, support, capabilities, and changes in the SANnav Management Portal 2.1.1 release. Note that this document applies only to the Brocade SANnav **Management Portal** product. There is a separate Release Notes document for the Brocade SANnav **Global View** 2.1.1 release.

NOTE Within this document, SANnav Management Portal might also be referred to simply as "SANnav".

1.1.1 What’s New in SANnav Management Portal 2.1.1

New feature enhancements in SANnav Management Portal 2.1.1 release include the following:

- LDAP Global Active Directory support (Global Catalog)
- Introduction of new Gen7 Flow Inventory and Investigation
- VM and bare metal installation on RHEL 8.2 and CentOS 8.2
- OVA support on CentOS 8.2 including migration from previous releases
- Removing dependence on IP Forwarding setting in all SANnav installations
- Support for FOS MAPS enhancements (SFP monitoring & BSL ASC data upload failure)
- Secure HTTPS streaming schema registration between SANnav and FOS
- Incremental feature enhancements
    - Inventory
    - Discovery
    - Switch support save FRU Dump
    - Zoning
    - Events Management
    - Installation scripts enhancements and user messages changes
    - SANnav Backup and Restore optimizations
- Usability enhancements

The defect fixes included in this release are listed in the defect tables section of this document.

1.2 New Hardware Platforms Supported in SANnav Management Portal 2.1.1

No new hardware platforms were added in SANnav Management Portal 2.1.1.

1.3 New Blades Supported in SANnav Management Portal 2.1.1

No new blade platforms were added in SANnav Management Portal 2.1.1.

1.4 SANnav Management Portal Server Platform Support and Infrastructure

1.4.1 SANnav Management Portal 2.1.1 OVA Support

SANnav 2.1.0 introduced new support for Open Virtual Appliance (OVA) deployment. Starting with SANnav Management Portal 2.1.0, customers can deploy SANnav Management Portal Base or Enterprise Editions as a virtual appliance (.ova file).

- SANnav 2.1.1 packages CentOS Operating System (OS) version 8.2 and requires ESXi hypervisor version 6.7 in order to be extracted.
- Migration from SANnav Management Portal 2.1.0/2.1.0a OVA to SANnav 2.1.1 Management Portal OVA is supported
- Extraction of the OVA file is supported on vCenter 6.5 or 6.7
  - ovftool is no longer supported.
- OVA is currently available only for SANnav Management Portal and **not** for SANnav Global View.

1.4.2 SANnav Management Portal 2.1.1 OS Support (VM and Bare Metal)

SANnav Management Portal 2.1.1 introduces support of new versions of RHEL and CentOS 8.2. Official versions of supported RHEL and CentOS are:

- RHEL 7.8, 8.1, 8.2
- CentOS 7.8, 8.1, 8.2

NOTE Starting with SANnav Management Portal 2.1.1, the installation script allows users to install SANnav Management Portal on an OS version that has the last digit (minor release) number greater than 2 for 8.x or greater than 8 for 7.x (e.g. RHEL or CentOS 8.**3** or 7.**9**). The installation script displays a warning message indicating that the SANnav Management Portal installation will proceed on an untested and unqualified OS version. Explicit customer acceptance is required in order for the SANnav Management Portal installation to proceed.

NOTE The use of SANnav on a higher release level of RHEL/CentOS that has not been explicitly qualified or tested is supported unless an issue is found to be caused by the RHEL/CentOS OS upgrade. SANnav issues that only occur when using an unqualified version of RHEL or CentOS will be addressed at Brocade's discretion.

NOTE SANnav Management Portal cannot be installed on Security Enhanced versions of Linux (SE Linux) on both CentOS and RHEL

NOTE For both CentOS and RHEL, 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 currently not supported.

1.4.3 Removal of dependency on IP Forwarding set to ON

Starting with SANnav Management Portal 2.1.1, the SANnav Management Portal server will no longer be dependent on having the OS parameter IP Forwarding set to on (i.e. True).

As a result, specific SANnav Management Portal ports must be explicitly listed in the IP Table OS file.

1.5 Summary of New Software Features

The following sections highlight the new feature additions or enhancements in various areas of SANnav Management Portal 2.1.1.

For detailed descriptions of these features and capabilities, refer to the *Brocade SANnav Management Portal User Guide*.

1.5.1 LDAP Global Catalog Support

Starting with SANnav Management Portal 2.1.1, it is now possible to define an LDAP Global Catalog server as opposed to adding single LDAP servers.

SANnav Management Portal allows Administrators to configure an LDAP Global Catalog server in order to define SANnav Management Portal users and their respective authentication, AORs (Area Of Responsibility), and RBAC (Role Based Access Control).

1.5.2 Flow Management

Starting with SANnav Management Portal 2.1.1, Flow Management provides flow monitoring and management capabilities for Gen 7 platforms. These capabilities enable a SAN administrator to gather the necessary information to actively manage SAN fabrics. This feature provides enhanced visibility into the behaviors and metrics necessary to resolve problems and, often, to avoid them.

Flow Management provides the following:

- View inventory of flows (IT and ITL/ITN) along with their related details such as whether the flow is an NVMe flow or a SCSI flow:

  - For SCSI: L = LUN number
  - For NVMe: N = Same space ID
- Investigate flows to view historical and real-time performance statistics in graphical form.
- Generate various Flow inventory reports as well as Time Series and Top N Reports.

NOTE Gen7 Flow Collections are not supported in SANnav Management Portal 2.1.1. Gen6 Flow Collections continue to be supported (IT Flow Collections only).

1.5.3 SANnav Management Portal 2.1.1 Northbound Streaming enhancements

The following new features are introduced in SANnav Management Portal 2.1.1:

- Gen7 Flow (IT/ITL/ITN) telemetry data is now streamed through the same interface as was done for Gen6 IT flows in SANnav 2.1.0x.

NOTE There is no change in the AVRO information model schema compared to SANnav Management Portal 2.1.0x

NOTE There are no new REST interfaces in SANnav Management Portal 2.1.1 compared to SANnav Management Portal 2.1.0x

1.5.4 Inventory

The following new features are introduced in SANnav Management Portal 2.1.1:

- Easy navigation to Investigation view for all ports in a trunk
- Troubleshooting: D-Port testing enhancements

1.5.5 Event Management

The following new features are introduced in SANnav Management Portal 2.1.1:

- Global search on the MAPS Violations page

1.5.6 Zoning Management

The following new features are introduced in SANnav Management Portal 2.1.1:

- Addition of HBA/Storage vendor in various Zone Management feature screens
- Cleanup of mixed member zones
- Specific error message in case of fabric-wide lock
- Zoning dialogs/views to show device status (offline/online)

1.5.7 Discovery

The following new features are introduced in SANnav Management Portal 2.1.1:

- Shortcuts to accept Fabric changes from appropriate Inventory pages
- Better guidance/notification for SNMP registration failures
- Showing Switch/AG counts in Fabric list view
- Addition of Switch type in Fabric details view
- Alternate Switch IP address column added in fabric list and details page
- Display of IPv4 address when switch is discovered via IPv4 in dual stack (IPv4/IPv6) environment
- Warning message for the fabric and switch un-monitor operation

1.5.8 Switch Support Save

The following new features are introduced in SANnav Management Portal 2.1.1:

- Support for new FRU Dump when taking a Switch Support Save
- Fabric Name column added in Switch Support Save and FOS Version management List pages. This column is a comma-separated list in cases where a chassis belongs to multiple fabrics and is fully searchable from SANnav Management Portal.
- While generating a switch support save by selecting **Internal SANnav Server**, the support save will be generated in the SANnav Management Portal internal server.
  - For single chassis selection, a single folder with extension ".zip" will be created
  - For bulk chassis selection, a single folder will be created which in turn, when expanded, will contain a support save for each of the selected chassis.

1.5.9 Usability Enhancements

The following usability enhancements are introduced in SANnav Management Portal 2.1.1:

- Persistent column settings within and across user sessions (i.e. login after logout)
- 2-column sorting using shift-click on the second column
- Custom column sorting to honor column type semantics (where applicable)
- Movable pop-up dialogs
- Resizable dialogs (select dialog windows only)
- Consistent use of Action menu across the application
- Consistent menus in embedded tables and detailed views
- Consistent use of available screen space for detailed tables
- Sorting capability on Fabric Name in Firmware management and Switch support save list view (SANnav Management Portal only)

1.6 SANnav Management Portal 2.1.1 Unsupported Features

The following features are not supported in Management Portal 2.1.1:

- IPv6 Support in the OVA installation

1.7 SANnav Management Portal 2.1.1 Deprecated Features or Support

The following features or support have been deprecated in SANnav Management Portal 2.1.1 and will be removed in the next release:

- **SANnav > SAN Monitoring > Network Scope** (note: this is the custom network scope. It will be changed in a future release by allowing a Filter on Dashboards and Reports)
- Offline zoning
- Support for Broadcast Zones
- The following widgets have been deprecated from the Dashboard templates and will be removed in the next release of SANnav Management Portal:
  - Initiator Port OORV
  - Target Port OORV
  - ISL Port OORV

1.8 SANnav Management Portal 2.1.1 Supported SAN Switches

- SANnav Management Portal 2.1.1 allows management of any supported Brocade Fibre Channel switch operating with Fabric OS v7.4.0 or later.
- SANnav Management Portal 2.1.1 supports all versions of Fabric OS that are supported in SANnav Management Portal 2.1.0x (FOS 7.4 up to FOS 9.0.0x) and adds support for FOS 9.0.1 in this release.

Gen 7 Switches	• Brocade G720 • Brocade X7-4 • Brocade X7-8
Gen 6 Switches	• Brocade G610 • Brocade G620 • Brocade G620 (switchType 183) • Brocade G630 • Brocade G630 (switchType 184) • Brocade X6-4 • Brocade X6-8 • Brocade G648 Blade Server SAN I/O Module • Brocade 7810 Extension Switch • Brocade MXG610s Blade Server SAN I/O Module
Gen 5 Switches	• 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 6545 Blade Server SAN I/O module • Brocade 6546 Blade Server SAN I/O module • Brocade 6547 Blade Server SAN I/O module • Brocade 6548 Blade Server SAN I/O module • Brocade 6558 Blade Server SAN I/O module • Brocade 7840 Extension Switch • Brocade DCX 8510-4 • Brocade DCX 8510-8 • Brocade Analytics Monitoring Platform
Gen 4 Switches	• Brocade 300 • Brocade 5424 Blade Server SAN I/O module • Brocade 5430 Blade Server SAN I/O module • Brocade 5431 Blade Server SAN I/O module • Brocade 5432 Blade Server SAN I/O module • Brocade 5450 Blade Server SAN I/O module • Brocade 5460 Blade Server SAN I/O module • Brocade 5470 Blade Server SAN I/O module • Brocade 5480 Blade Server SAN I/O module • Brocade NC-5480 Blade Server SAN I/O module • Brocade 7800 Extension Switch

Chapter 2: Brocade SANnav Management Portal Deployment

2.1 Server Requirements

SANnav Management Portal 2.1.1 can be deployed either on a single bare-metal host, virtual machine (VM) or as an Open Virtual Appliance (OVA). The following tables provide details of server requirements in each case.

VM or bare metal Installation						
Max Switch Ports Under Management (Base or Enterprise)	**Operating System**	**Host Type**	**Minimum CPU**	**Minimum number of CPU Sockets**	**Memory**	**Hard Disk**
600 Ports (Base) 3000 (Enterprise)	RHEL 7.8, 8.1, 8.2 (*) CentOS 7.8, 8.1, 8.2 (*)	Bare metal/ VMware ESXi VM	16 cores, 2000 MHz	2	48 GB	600 GB
15000 (Enterprise)	RHEL 7.8, 8.1, 8.2 (*) CentOS 7.8, 8.1, 8.2 (*)	Bare metal/ VMware ESXi VM	24 cores, 2000 MHz	2	96 GB	1.2 TB

NOTE (*) SANnav Management Portal 2.1.1 may be installed on future minor versions of RHEL and CentOS, but they are not certified or tested. For example, RHEL and CentOS 7.9, 8.3, or 8.4. The use of SANnav on a higher release level of RHEL/CentOS that has not been explicitly qualified or tested is supported unless an issue is found to be caused by the RHEL/CentOS OS upgrade. SANnav issues that only occur when using an unqualified version of RHEL or CentOS will be addressed at Brocade's discretion.

NOTE RHEL/CentOS 7.7 (and below) and 8.0 are no longer supported in SANnav Management Portal 2.1.1

OVA Installation						
Max Switch Ports Under Management (Base or Enterprise)	**Supported Hypervisor**	**Host Type**	**Minimum CPU**	**Minimum number of CPU Sockets**	**Memory**	**Hard Disk**
600 Ports (Base) 3000 (Enterprise)	VMware ESXi 6.7	VMware ESXi VM	16 cores, 2000 MHz	2	48 GB	600 GB
15000 (Enterprise)	VMware ESXi 6.7	VMware ESXi VM	24 cores, 2000 MHz	2	96 GB	1.2 TB

NOTE The OVA deployment assumes a default server configuration (48GB RAM, 16 CPU Cores, 600 GB Storage) suitable for either SANnav Management Portal Base Edition (600 ports, no Directors) or Enterprise Edition up to 3000 ports. If you require an Enterprise version scaling up to 15,000 ports, you must make sure to extract the OVA to configure it with a server configuration of (96 GB RAM, 24 CPU Cores, 1.2 TB Storage). Refer to the *Brocade SANnav Management Portal Installation and Migration Guide* for details.

2.2 Client Requirements

The latest versions of the following web browsers are supported for a SANnav Management Portal 2.1.1 client:

- Chrome (on Windows, Mac)
- Firefox (on Windows, Linux)

Launching of Web Tools from a SANnav Management Portal client for Fabric OS versions above 9.0 is supported on the following browsers:

- Chrome (on Windows, Mac)
- Firefox (on Windows, Linux)

Launching of Web Tools from a SANnav Management Portal client for Fabric OS less than 9.0 is supported only on the following browsers:

- Firefox (on Windows, Linux)

2.3 Software Upgrade and Downgrade

Refer to the “Migration Overview” section of the *Brocade SANnav Management Portal Installation and Migration Guide* for complete details.

Supported Migration Paths:

Current Version (SANnav Management Portal)	New Version	Supported
SANnav 1.x	SANnav 2.1.1	NO
SANnav 2.0.x	SANnav 2.1.1	YES
SANnav 2.1.0/2.1.0a*	SANnav 2.1.1	YES

* OVA installation from these versions can be migrated to SANnav 2.1.1 OVA

Chapter 3: 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.

SANnav Management Portal has a 90-day trial period built into the product, which allows the product to be used for up to 90 days from the day of installation, without requiring a license.

Chapter 4: Scalability

4.1 SANnav Management Portal 2.1.1 Scalability

Feature	**Scalability Limit – SANnav Management Portal Base**	**Scalability Limit – SANnav Management Portal Enterprise**
Maximum number of **SAN ports managed**	600	15,000
Maximum number of **end device ports managed**	2000	40,000
Maximum number of **end device ports per fabric**	10,000	
Maximum number of **events** stored	10 Million	
Maximum number of **MAPS violations** stored	10 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. Once data collection is complete, the data is retained for 14 more 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 more days.	
Maximum number of **Flows** Supported	• Enterprise Edition (15K ports) platform: 400K Flows with 4 AMPs or 100k Flows with Gen 7 and/or Gen 6 platforms. • Base Edition (600 ports) platform and Enterprise (3K ports) platform: 8K 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 5: Important Notes

- For switches running Fabric OS v8.2.1 or later that are monitored by both SANnav Management Portal and Brocade Network Advisor, make sure that the historical data collection is disabled in Brocade Network Advisor.

- By default, port 22 is used for SANnav internal firmware repository, but this port number can be changed during installation. If port 22 is not available, an external FTP, SCP, or SFTP server for switch supportsave and firmware download functionality must be used. For switches running Fabric OS versions earlier than 8.2.2, if a port number other than 22 is picked for SSH, then an external FTP, SCP, or SFTP server for switch supportsave and firmware download functionality must always be used.

- 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 9.0:
  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 9.0 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.

- 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 required that the network latency does not exceed 100 ms between SANnav clients to the SANnav Management Portal server and between SANnav Management Portal server to the switches. If the latency is higher than 100ms, then communication time-outs may occur and cause undesirable behaviors.

- When the 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.

- When the SANnav Management Portal server is restored from a SANnav Management Portal backup, high granularity performance data, FCIP performance data, and flow statistics and violations are no longer collected due to a new digital certificate that is generated in the server, which does not match the digital certificates on the switches. To fix this error, un-monitor and monitor all data-streaming switches. This will update the certificates on the switches with the new certificate on the SANnav server.

- Due to a design change, the event filters created during SANnav 2.0 will not be migrated in SANnav 2.1.1. They must be re-created. All other filters (Inventory filters) will be migrated.

- It is mandatory to add a filter when generating any Time Series reports; otherwise, the generated report will be empty. The UI does not enforce a filter to be applied.

- 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.

- 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. As long as 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.

- 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.

- Cockpit web console for Linux cannot co-exist with SANnav Management Portal.

- SANnav uses 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. Failure to do so will result in the SANnav server not starting properly.

- When performing SANnav migration from previous releases to SANnav 2.1.1 with IPv4 installation, the following internal ports need to be available before migration for SANnav to use otherwise the SANnav 2.1.1 server will not start properly.

Ports needed for SANnav 2.1.1 (migration from 2.0.0, 2.1.0x, IPv4)	80, 8081, 443, 19092, 19093, 19094, 2377, 7946

- SANnav 2.1.1 added a new port 18082 for Avro schema registry secure mode, please make sure this port is open in the Firewall so that SANnav can communicate with the switch.

- **Firewalld Backend Configuration:**

  When Centos/RHEL 8.x 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

a. Stop the firewalld using the command **systemctl stop firewalld**
b. Edit the firewalld configuration using the command **vi /etc/firewalld/firewalld.conf** and change the FirewallBackend=**nftables** to FirewallBackend=**iptables**
c. Start the firewalld using the command **systemctl start firewalld**
d. Reload the firewalld using the command **firewall-cmd --reload**

- When installing SANnav Management Portal 2.1.1 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:

  1. Stop the SANnav Management Portal server using the script **stop-sannav.sh** present in `<install_home>/bin` folder
  2. Stop the Docker using the command **systemctl stop docker**
  3. Follow the firewalld configuration procedure as per the *Firewalld Backend Configuration* important note (**Note:** This step is not applicable for Centos/RHEL 7.x versions)
  4. Start the Docker using the command **systemctl start docker**
  5. Start the SANnav Management Portal 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 in order to re-insert all the missing firewall rules

  ```
  systemctl restart sannaviptablesetup.service
  ```

- 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.

- Brocade G620 platforms running Fabric OS v8.2.2x incorrectly show Faulty_Blade, WWN_Down, HA_Sync as supported measures in the CHASSIS Group. Due to this, after importing a MAPS policy from these switch models, subsequent deletion of custom policy operations will fail. If this happens, import the MAPS policy from another switch present in the fabric and use CLI to delete custom policy.

- In the Configuration Policy feature, there is an issue while syncing data from the switch to the SANnav database in certain conditions for some of the switch configuration data. When this happens some of the functionalities such as drift detection, pushing the policy to the switch and importing configuration from the switch may not work as expected. This has been observed in the following use cases:

  1. Failure of completing the Switch configuration backup after Fabric Discovery
  2. When the user changes the switch configuration parameters such as FTP, Banner etc. using CLI

  The user needs to perform a manual backup of the configuration to resolve this issue.

- SANnav Management Portal 2.1.1 does not support the short URL name for accessing the client (for example, `https://sannav/`). The fully qualified domain name (FQDN) or an IP address must be used instead (for example, `https://sannav.sjc.sqalabs.sjc.com/).`

- Users will not be able to login to SANnav Management Portal if IPv6 is disabled at the OS kernel level. The workaround is to either enable IPv6 in the server at the OS kernel or modify SANnav configuration files.

  Enable IPv6 at the OS Kernel:

  1. Uninstall SANnav Management Portal.

2. Edit the grub file using the command “`vi /etc/default/grub`”.

   ----- SAMPLE Content -------
   ```
   GRUB_TIMEOUT=5
   GRUB_DEFAULT=saved
   GRUB_DISABLE_SUBMENU=true
   GRUB_TERMINAL_OUTPUT="console"
   GRUB_CMDLINE_LINUX="ipv6.disable=1 crashkernel=auto rhgb quiet"
   GRUB_DISABLE_RECOVERY="true"
   ```
   ----

3. Change the value for "`ipv6.disable`" to "0".
   ```
   GRUB_CMDLINE_LINUX="ipv6.disable=0 crashkernel=auto rhgb quiet"
   ```

4. Apply the configuration by executing the following command.
   ```
   grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

5. Reboot the system.
   ```
   shutdown -r now
   ```

6. Reinstall SANnav Management Portal.

<u>Modify SANnav Configuration Files:</u>

1. Stop the SANnav server.
2. Edit the `nginx.conf` file.
   ```
   vi $DCM_HOME/conf/nginx/nginx.conf
   ```
3. Remove the following line:
   ```
   listen [::]:18081;
   ```
4. Save the nginx.conf file.
5. Edit the `nginx_ssl_conf_sr` file.
   ```
   vi $DCM_HOME/conf/nginx/nginx_ssl_conf_sr
   ```
6. Remove the following line:
   ```
   listen [::]:18082 ssl http2;
   ```
7. Save the nginx_ssl_conf_sr file
8. Start the SANnav server.

- When searching within a zone configuration that contains more than 50 zones, if the result of the search is a zone that is not among the first 50 entries of the zone configuration, the **Save** button is not enabled if you try to remove that zone. **Workaround:** After removing the zone, use the **Save As** option to save the zone configuration to a new one.

- If a given MAPS rule is updated in a MAPS policy and then distributed to the switches associated with the Policy, the rule is not updated on the destination switches if any of the destination switches already have a rule with the same name. **Workaround**: Save the rule with a new name when the rule is updated.

- When migrating from previous releases to SANnav 2.1.1, if a custom port is used for internal SFTP/SCP, make sure that this port is not part of the required ports list in the installation guide. If the custom port is in the required ports list, change this port to any other free port using the "change-internal-ssh-port.sh" script before starting the migration.

- Customization of the swap space to a non-default location during installation will not work. *<u>Please contact Brocade support in order to customize the swap location.</u>*

- When configuring the VM for SANnav installation, please make sure the MTU size of the network interface is set to 1500, otherwise SANnav will not receive Historical Performance data.

- During migration from a previous SANnav release to SANnav 2.1.1, the third party signed certificates of the source version will not be migrated and will be replaced with a new set of self-signed certificates in the 2.1.1 release. **Workaround**: Save the certificates before migration to 2.1.1 and execute the "`replace-server-certificates.sh`" script to re-install the third party certificates overridden during migration.

- If communication protocol is changed on any of the managed switches from HTTP to HTTPS or vice versa, SANnav re-establishes communication with the newly configured protocol on the switch. However, due to a defect the communication will not automatically be re-established by SANnav to the switch. **Workaround**: Restart the SANnav server to re-establish the communication with the switch.

Chapter 6: Security Vulnerability Fixes

This section lists the Common Vulnerabilities and Exposures (CVEs) updates included in Brocade SANnav v2.1.1.

- **CVE-2020-15377**

Webtools in Brocade SANnav versions lower than 2.1.1 allow unauthenticated users to make requests to arbitrary hosts due to a misconfiguration; this is commonly referred to as Server-Side Request Forgery (SSRF).

- **CVE-2020-15378**

The OVA version of Brocade SANnav versions lower than 2.1.1installation with IPv6 networking expose the docker container ports to the network, increasing the potential attack surface.

- **CVE-2020-15380**

Brocade SANnav versions lower than 2.1.1 log accounts credentials at the 'trace' logging level.

- **CVE-2020-15381**

Brocade SANnav versions lower than 2.1.1 contain an Improper Authentication vulnerability that allows cleartext transmission of authentication credentials of the jmx server.

- **CVE-2020-15382**

Brocade SANnav versions lower than 2.1.1 use a hard-coded administrator account with the weak password 'passw0rd' if a password is not provided for PostgreSQL at install-time.

- **CVE-2020-15384**

Brocade SANnav versions lower than 2.1.1 contain an information disclosure vulnerability. Successful exploitation of internal server information in the initial login response header.

- **CVE-2020-15385**

Brocade SANnav versions lower than 2.1.1 allow an authenticated attacker to list directories and list files without permission. As a result, users without permission can see folders and hidden files and create directories without permission.

- **CVE-2020-15387**

The host SSH server of Brocade SANnav versions lower than 2.1.1 and Brocade Fabric OS lower than Brocade Fabric OS v7.4.2h, v8.2.1c, v8.2.2, v9.0.0 utilize keys of less than 2048 bits, which may be vulnerable to man-in-the-middle attacks and/or insecure SSH communications.

- **CVE-2020-13401**

Issue in Docker Engine lower than 19.03.11: An attacker in a container with the CAP_NET_RAW capability can craft IPv6 router advertisements and consequently spoof external IPv6 hosts, obtain sensitive information, or cause a denial of service.

- **CVE-2020-11022**

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.

- **CVE-2019-20372**

NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.

- **CVE-2017-14503**

libarchive 3.3.2 suffers from an out-of-bounds read within lha_read_data_none() in archive_read_support_format_lha.c when extracting a specially crafted lha archive, related to lha_crc16.

- **CVE-2009-3555**

The TLS protocol and the SSL protocol 3.0 and possibly earlier does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

Chapter 7: Defects

7.1 Known Issues in SANnav Management Portal v2.1.1

Defect ID	Description
SANN-125628	Inventory and Reports show the same switch multiple times when filter is applied.
SANN-125751	MAPS policy deletion fails.
SANN-125806	Pushing Universal MAPS policy to switches fails.
SANN-125811	Trap and Syslog forwarding doesn't honor filters in some cases.
SANN-125869	Investigate view sometimes shows no data to display on changing time-scope from preselected time-scope to last 30 days
SANN-126352	No data to display shown sometimes for network metric in the VM investigation view.
SANN-126549	Pushing FTP configuration fails.
SANN-126558	Updated FTP parameters not seen when importing the configuration from Switch.
SANN-126566	Widget in user defined Dashboard not loading in template view.
SANN-126629	User changed syslog port number in configuration block is not reflected immediately.
SANN-126652	SANnav iptables rules are removed.
SANN-126666	Selecting multiple flows using shift key does not work.
SANN-126675	Fabric name displays as blank in investigation view for Fabric Performance Impact violation.
SANN-126676	FID is displayed as blank in investigate view for Fabric Performance Impact violation.
SANN-126699	"Monitored switch count" shows less switches than the actual switches present in fabric.
SANN-126719	Configuration restore operation not completed.
SANN-126747	Search does not produce correct result.
SANN-126750	Member change column shows "New changes" in Fabrics even though there are no changes in Fabric.
SANN-126865	Intermittently switch supportsave generation fails for few switches.
SANN-126900	Informs are not received after the initial discovery.
SANN-126908	Auto registration for informs fails.

SANN-126957	Missing data points in historical investigation view.

7.2 Defects closed with code change in SANnav Management Portal v2.1.1

Defect ID	Description
SANN-122628	User observes an error popup dialog over a popup dialog while applying license changes
SANN-122677	FOS Update dialog lists some switches that do not need EULA acceptance in the EULA agreement prompt.
SANN-122782	Editing a zone and saving it could take up to 5 mins.
SANN-122806	Zone list in edit zone configuration page is empty
SANN-122813	User will see Fan-in ratio rule box checked even though it was disabled in 2.0
SANN-123029	Event log is filled with messages showing Syslog and SNMP Trap Registration every few minutes.
SANN-123593	'Update-events-purge-settings.sh' script does not work.
SANN-123642	Unable to perform MAPS Policy operations (Edit/Create/Distribute/Import).
SANN-123703	Accessing SANnav server using FQDN/DNS Name fails to login to the server.
SANN-123765	When filtering for "Degraded" hosts under the Inventory tab, some "Healthy" hosts show in result.
SANN-123981	FTP configuration is not setting password on the switches.
SANN-123987	Events view is not showing data beyond few days.
SANN-124252	Unable to discover the fabrics.
SANN-124614	SANnav 2.1 does not display any Event Action Policies.
SANN-124817	Zone config compare between effective and defined configuration shows incorrect data.
SANN-124977	User will not be able to login SANnav
SANN-125260	Error when attempting to set up email and the Event Management pages do not work in the UI.
SANN-125378	Events management operations do not work.
SANN-125967	SANnav is not receiving SNMP informs.
SANN-126680	SNMP username not accepting "-"
SANN-126753	The switch is listed on the non-FICON management page.

7.3 Defects closed without code change in SANnav Management Portal v2.1.1

Defect ID	**Description**
SANN-123233	Hostname sorting is not working in the Hosts widget of Health Summary.

Chapter 8: Contacting Technical Support for your Brocade® Product

For product support information and the latest information on contacting the Technical Assistance Center, go to https://www.broadcom.com/support/fibre-channel-networking/. If you have purchased Brocade® product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7.

Online	Telephone
For nonurgent issues, the preferred method is to log in to myBroadcom at https://www.broadcom.com/mybroadcom. (You must initially register to gain access to the Customer Support Portal.) Once there, select **Customer Support Portal** > **Support Portal**. You will now be able to navigate to the following sites: • **Knowledge Search**: Clicking the top-right magnifying glass brings up a search bar. • **Case Management**: The legacy MyBrocade case management tool (MyCases) has been replaced with the Fibre Channel Networking case management tool. • **DocSafe**: You can download software and documentation. • **Other Resources**: Licensing Portal (top), SAN Health (top and bottom), Communities (top), Education (top).	Required for Severity 1 (critical) issues: Please call Fibre Channel Networking Global Support at one of the numbers listed at https://www.broadcom.com/support/fibre-channel-networking/.

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.

Document Feedback

Quality is our first concern. We have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission or if you think that a topic needs further development, we want to hear from you. Send your feedback to documentation.pdl@broadcom.com. Provide the publication title, publication number, topic heading, page number, and as much detail as possible.

Chapter 9: Revision History

Version	Summary of changes	Publication date
1.0	Initial version of the document	12/18/2020
1.1	Updated important notes	3/8/2021
1.2	Added Security Updates and updated important notes	6/14/2021

BROCADE
A Broadcom Company