SANnav Management Portal 2.1.0

Brocade SANnav Management Portal Release Notes

Version 1.4 (Digest Edition)

Table of Contents

Chapter 1: Release Contents 5
1.1 Brocade SANnav Management Portal 2.1 Release Overview 5
1.2 New Hardware Platforms Supported in SANnav 2.1 5
1.3 New Blades Supported in SANnav 2.1 5
1.4 New SANnav Management Portal Server Platform Support and Infrastructure 6
1.4.1 New OVA Support 6
1.4.2 New OS Support 6
1.5 Summary of New Software Features 6
1.5.1 Flow Management 6
1.5.2 Northbound Streaming 7
1.5.3 REST API 7
1.5.4 Templates, Dashboards and Reports 7
1.5.4.1 Templates 8
1.5.4.2 Health Summary Dashboard 8
1.5.4.3 Network Port Traffic Conditions Dashboard 8
1.5.4.4 New Dashboard Widgets 8
1.5.4.5 New Reports and Report Widgets 8
1.5.4.6 New Filters on Reports 9
1.5.5 Topology 9
1.5.6 Inventory, Storage Enclosure Mapping, End Device Mapping and CLI Scripting 10
1.5.6.1 Inventory 10
1.5.6.2 Storage Enclosure Mapping 10
1.5.6.3 End Device Type Mapping 10
1.5.6.4 CLI Scripting 11
1.5.7 Investigation View Enhancements 11
1.5.8 Event Management 11
1.5.9 Event Actions Policies 12
1.5.10 Zoning Management 12
1.5.11 Configuration Policy Management 12
1.5.12 Fabric OS Version Management 13
1.5.13 Discovery 13
1.5.14 Extension Tunnels Management 13
1.5.15 FICON Enhancements 14
1.5.16 Fabric OS EEOS (Extended End Of Support) 14
1.5.17 Miscellaneous Enhancements 14
1.6 Unsupported Features 15
1.7 Deprecated Features 15
1.8 Supported SAN Switches 16

Chapter 2: Brocade SANnav Management Portal Deployment 17
2.1 Server Requirements 17
2.1.1 Server Requirements Details 17
2.2 Client Requirements 18
2.3 Software Upgrade and Downgrade 18

Chapter 3: Licensing 19

Chapter 4: Scalability 20
4.1 SANnav Management Portal Scalability 20

Chapter 5: Important Notes 22

Chapter 6: Security Vulnerability Fixes 26

Chapter 7: Defects 27
7.1 Known Issues in SANnav Management Portal v2.1.0 27
7.2 Defects closed with code change in SANnav Management Portal v2.1.0 30
7.3 Defects closed without code change in SANnav Management Portal v2.1.0 32

Chapter 8: Contacting Technical Support for your Brocade® Product 34

Chapter 9: Revision History 35

Chapter 1: Release Contents

1.1 Brocade SANnav Management Portal 2.1 Release Overview

SANnav 2.1.0 is a major new release of Brocade's two Fibre Channel SAN management software products, **Brocade SANnav Management Portal** and **Brocade SANnav Global View**. SANnav Management Portal 2.1.0 supports the introduction of Brocade's new Gen 7 platforms with Fabric OS 9.0.0, and adds new features and capabilities that make managing Brocade SAN environments easier than ever before.

This chapter highlights many of the new features, support, capabilities, and changes in the SANnav Management Portal 2.1.0 release. Please 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** 2.1.0 release.

1.2 New Hardware Platforms Supported in SANnav 2.1

Note: These new hardware platforms require FOS 9.0 or later releases

Product Name	Device Name
Brocade G720	Gen 7 56-port Switch
Brocade X7-4	Gen 7 4-slot Director
Brocade X7-8	Gen 7 8-slot Director
Brocade G620 (switch Type 183)	Gen 6 (32Gb/s) 64-port Switch
Brocade G630 (switch Type 184)	Gen 6 (32Gb/s) 128-port Switch

1.3 New Blades Supported in SANnav 2.1

Note: These new blades require FOS 9.0 and later releases

Blade	Description	Compatible devices
Brocade FC32-X7-48	Gen 6 48-port blade for X7	Brocade X7 Director
Brocade FC64-48	Gen 7 48-port blade	Brocade X7 Director
Brocade CR64-4	Gen 7 core routing blade for X7-4	Brocade X7-4 Director
Brocade CR64-8	Gen 7 core routing blade for X7-8	Brocade X7-8 Director
Brocade CPX7	Gen 7 control processor blade for X7	Brocade X7 Director

1.4 New SANnav Management Portal Server Platform Support and Infrastructure

1.4.1 New OVA Support

- SANnav 2.1 introduces new support for Open Virtual Appliance (OVA) deployment. Starting with SANnav 2.1, customers can deploy SANnav Management Portal Base or Enterprise Editions as a virtual appliance (OVA file).
- The OVA file can be downloaded from the Broadcom Customer Support Portal (CSP) and is about ~25 GB in size.
- The OVA file packages a CentOS Operating System (OS) version 8.0 and requires ESXi hypervisor version 6.7 in order to be extracted.
    - If ESXi 6.5 is required, contact Broadcom Support. The OVA appliance can be extracted and installed with ESXi 6.5 using OVF Tool; however, the procedure and steps are different from what is documented for ESXi 6.7.
- OVA is only available for SANnav Management Portal and not for SANnav Global View.

1.4.2 New OS Support

SANnav 2.1 Management Portal introduces support of new versions of RHEL and CentOS:

- RHEL 8.0 and 8.1
- CentOS 8.0 and 8.1

1.5 Summary of New Software Features

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

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

1.5.1 Flow Management

Starting with SANnav 2.1.0, Flow Management provides flow monitoring and management capabilities for Gen 6 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 along with their related details.
- Investigate flows to view historical and real-time performance statistics in graphical form.
- Generate Time Series and Top N Reports
- Manage collections (aggregated and non-aggregated) with custom rule sets.

- View violated events triggered for flows as well as aggregated collections.
- Investigate collections to view historical statistics at collection level.
- Easily navigate from Collection Investigation View to member Flow Investigation View.
- View various reports on Flows and Flow Collections.

1.5.2 Northbound Streaming

Northbound Streaming is a new SANnav 2.1 feature that allows customers to write Kafka consumers in order to consume the port performance and flow telemetry data that SANnav broadcasts on a secure channel.

- A maximum of one Northbound server is supported (secure using certificate)
- The Northbound Server Kafka requirements are the same as that of SANnav:
  - Kafka Version - 2.2.1
  - Confluent Platform Version for Schema Registry & Zookeeper - 5.2.2
- REST APIs to register/remove/get consumer, enable/disable streams
- Stream of following metrics (aka Stream Types)
  - 1 - FCPORT – FC Port metrics,
  - 2 - ETH/GIGE PORT - ETH Port and GigE Ports metrics
  - 3 - EXTENSION - Extension Tunnel and Circuit metrics
  - 4 - SWITCH - Switch performance metrics
  - 5 - FLOW - Flow Metrics (AMP and Gen 6 Flows, IO Violation Metrics)

Note: Some of the object names used in the Kafka streams are subject to change in upcoming releases. Brocade will make every effort to provide backward compatibility for these names so that users' implementations with SANnav 2.1 remain compatible with upcoming releases. However, at some point in time, Brocade may deprecate the previous schemas. This deprecation of schemas will be announced in applicable version's release notes.

Refer to the *Brocade SANnav Management Portal REST API and Northbound Streaming Reference Manual*.

1.5.3 REST API

The following new REST APIs are available with SANnav 2.1.0.

- Listing Events (with a newer version of Filters)
- Health Summary for Fabrics, Switches, Hosts and Storage

1.5.4 Templates, Dashboards and Reports

This section highlights the new features or enhancements related to SANnav Management Portal dashboards and reports including associated widgets and templates.

1.5.4.1 Templates

New features added for templates in this release are:

- Sharing of templates for dashboards and reports among users (RBAC controlled)
- Support bulk import/export for templates and generated **reports**

1.5.4.2 Health Summary Dashboard

Customization of two Health Score Computation factors are introduced in this release:

- Fabric -->Link Down Count: allows to deduct points from Fabric Health when the Link Down Count is exceeded by a specified value.
- Host & Storage --> Fan In Ratio: allows to deduct points from Host Health when the Fan In Ratio is exceed by a specified value.

An option called **Run Computation** is added to allow for Health Score recalculation.

1.5.4.3 Network Port Traffic Conditions Dashboard

The Network Port Traffic Conditions (NPTC) Dashboard has been fully redesigned in SANnav 2.1. It contains:

- Time Series widget showing Congested Ports and an associated table ranked by weighted average score
- Time Series widget showing Oversubscribed Ports and an associated table ranked by weighted average score
    - Note that this widget is available only for switches running Fabric OS 9.0.
- Quarantined Ports widget

There are also operations to investigate congested, oversubscribed or quarantined ports. Appropriate port metrics are selected when investigating from here.

1.5.4.4 New Dashboard Widgets

In SANnav 2.1, 2 new widgets are added:

- Port Health violations Widget with details of distribution of Port Health Violations (Top 10)
- FPI Violations Widget to show details of Violations (same categories as Investigation)

The OORV widget is enhanced to add OORV for Flows (Gen 6 and AMP Flows):

- IO Latency
- IO Performance
- IO SCSI (AMP only)
- Flow Collection Aggregation

1.5.4.5 New Reports and Report Widgets

The following new reports for flows, collections, zoning, and idle device ports are introduced in SANnav 2.1:

- Time Series Reports
    - Flows
    - Flow Collection (Aggregated)
    - Flow Violation (AMP only)

- Top N Flows/Collections Reports
    - Collection Aggregation including threshold setting
    - Flow Violation including threshold setting and IT/ITL Filter (AMP only)
    - SCSI Errors including threshold setting (AMP only)
- Top N Storage Reports
    - Data Rate including time series and threshold setting (AMP only)
    - Port Exchange Completion Time including time series and threshold setting (AMP only)
    - Port First Response Time including time series and threshold setting (AMP only)
    - Port IOPS including time series and threshold setting (AMP only)
    - Port Pending IOs including time series and threshold setting (AMP only)
- Top N Host Reports
    - Pending IOS including time series and threshold setting (AMP only)
    - Port Read Over Subscription including time series and threshold setting (AMP only)
- New Zoning Report
    - Zone Summary Table
        - Provides details of all zone databases, including configurations, zones, aliases and members
    - Unzoned/Unaliased Device Table
        - Identifies Devices not Zoned or not aliased
- Idle Device Report –Device ports with combined (Tx+Rx) Utilization % <= 1%

1.5.4.6 New Filters on Reports

New filters are introduced in Time Series Reports:

- Filter by Average or Max: Ports will be filtered based on the average value of the metric in the given time scope.
- Filter by # of Occurrences: Ports will be filtered based on the range for the metric and the number of occurrences specified by the user.
- Filter by Sum: Applicable only for Error widgets, for example, Port Errors. Ports will be filtered based on the sum value of the metric in the given time scope.

1.5.5 Topology

Following are the new Topology features added in SANnav 2.1:

- Showing details related to health score
- Save Topology contexts
- FCoE LAG support in topology links
- Split AG representation to show connectivity to different fabrics
- Link utilization enhancements
    - Turn on/off utilization indication for links

1.5.6 Inventory, Storage Enclosure Mapping, End Device Mapping and CLI Scripting

1.5.6.1 Inventory

The following new features are introduced:

- Export CSV from Inventory
- All Import/Export in same location
  - Due to this, the "*SANnav → Inventory Name and Mapping Management"* SANnav 2.0 UI menu is removed
- QSFP Enhancements
  - Show QSFP number in port inventory
  - Allow Port Decom from one port for the entire QSFP (a warning message will be shown)
  - Run D-Port (Diagnostics) on QSFP Ports (select any)
- Move Maintenance Mode indication to Chassis inventory view (was in Switch before)
- Move CPU, Memory, and Up Time to Chassis inventory view (was in Switch before)
- Enhanced chassis report: Exporting a chassis report will have a new .csv structure
- Support for Extension Tunnel scheduled data collection of 5-second granular data
- Support stopping scheduled high granular data collection (Ports, Tunnels)

1.5.6.2 Storage Enclosure Mapping

- SANnav will determine the mapping of Storage Ports to Storage Enclosures automatically based on one of the following:
  - FDMI (Fabric Device Management Interface) information if supported by the Storage Vendor. It is highly recommended to turn on FDMI on storage devices from vendors/models that support it.
  - Storage Port information in Name Server (based on Node Symbolic Name)
- Where possible, storage ports are automatically mapped to storage enclosures
  - The storage objects will be created automatically in SANnav and the storage ports will be automatically associated to the storage based on heuristics of the port node symbolic names.
  - Node symbolic name is not consistent across storage vendors and may fail for some storage vendors and models.
- It is recommended that users turn on FDMI on all hosts to enable the automatic mapping of host ports to host enclosures.
- Whenever the mapping appears to be incorrect, users can update enclosure mapping manually as before.

1.5.6.3 End Device Type Mapping

- Policy-driven method to deterministically identify the logged-in device type (Host or Storage)
- GUI for updating Vendor OUI Mapping
- Supports custom policy for device type mapping

- Regex-based device type mapping when OUI mapping fails

1.5.6.4 CLI Scripting

The CLI scripting tool is meant to be used to isolated cases and is not meant as a comprehensive CLI scripting tool with if-then-else statements and user interactivity.

- Provides capability to send CLI commands to switches managed in SANnav.
- Run non-interactive commands and report output.
- Not an interactive tool - Used primarily for quick troubleshooting when there is no direct connectivity to the switch from the client machine.
- Results of CLI commands are in the **Output** tab.

1.5.7 Investigation View Enhancements

The following enhancements have been made to the Investigation View:

- Show violations in Investigation View along with telemetry data
- Show port properties in Investigation View
- Increase MxN investigation to **4x4**
- **Show Related Ports** in Investigation View (new option menu replacing **All Ports** option menu)
- Ability to investigate from host/storage enclosures directly (will select all connected F-Ports)

1.5.8 Event Management

- New Event and Violations filters:
    - Event Filter: New Event filter to allow filtering of events By:
        - Categories
        - Event Columns
        - Values
    - MAPS Violations Filter: New Violations filter to allow filtering of MAPS Violations by:
        - Category
        - Rules/measures
        - Threshold values
- Adding *Port Type* and *Measure* as additional columns in the MAPS Events Violations view.
- From MAPS Violations page
    - Allow investigation of port telemetry data from MAPS event
    - Investigate view takes user to the source port with violated measure and time scope around the preselected occurrence time (+ or – 30mn)

  - View Switch Details
  - View Fabric Details
- **Note**: Event filters created with SANnav 2.0 will not be migrated in SANnav 2.1. They will have to be recreated. All other filters (Inventory filters) will be migrated.

1.5.9 Event Actions Policies

- A new default, system wide, Event Action Policy called “Auto_Upload_SupportSave” is created. This policy performs an automatic upload of Supportsave upon receiving any FFDC events. It is disabled by default.
- Note: Capture Support Save policies created in SANnav 1.1.x or 2.0 will not be migrated to SANnav 2.1.

1.5.10 Zoning Management

Following are new features added in Zone Management:

- Zone alias enhancements
  - Show devices that have been added to the fabric
- Fabric-wide lock implementation in Fabric OS 9.0 presents an error message to the user when a conflict occurs
- Reverse lookup of zone alias
  - Support ability to navigate from zone alias to zones and to zone configurations
- **Note**: Before migrating SANnav to v2.1.0, or restarting the SANnav server, it is recommended that all fabrics be monitored. If a fabric is unmonitored during one of these two operations and monitored back after migration or server restart, zoning operations will fail. The workaround is to restart the SANnav server.

1.5.11 Configuration Policy Management

Following are new features added in Configuration Policy Management:

- New Universal MAPS Policy
  - Single policy of all possible rules that can be applied to all switches for all Fabric OS versions
  - SANnav will selectively push only applicable rules to switches based on Fabric OS version

    Note: there is no monitoring of drifts for Universal Policy in SANnav 2.1.
- MAPS Configuration Drift Detection
  - Support MAPS Policy as Config block for drift detection (*not applicable to Universal MAPS Policy)*
- MAPS FPI Configuration Rules
  - Support FPI threshold customization using Policy Config (Fabric OS 9.0)
- New Oversubscription support
  - Support new “Oversubscribed” and ”Oversubscription Clear” rules (Fabric OS 9.0)
- Support Impaired or Disable (default) options as part of Port Decommission Configuration Action (Fabric OS 9.0)
- Drift monitoring for Disruptive Configuration settings (10 total properties on Chassis, Fabric, Switch, Zone and F-Port objects)
- Basic Configuration blocks for FTP configuration (Auto Enabled)
- Drift monitoring for Extension Tunnels and Circuits Configuration

- Configuration Drift Widget redesigned to show number of switches in drift (also for SANnav Global View)

1.5.12 Fabric OS Version Management

Recent releases of Fabric OS have requirements for the user to acknowledge and accept the EULA prior to allowing new FOS versions to be loaded on a switch. SANnav 2.1 has added support to let users perform this EULA acceptance directly in the SANnav UI.

The process for managing Fabric OS versions from SANnav has not changed in its functionality. However, there is a new enforcement of EULA licenses in Fabric OS that has been introduced, which will require user acceptance prior to download from SANnav. Below are the details of the new behaviour.

- **FOS EULA Aware Definition:** A Fabric OS version of firmware that has knowledge of the FOS EULA acceptance feature.

  - FOS 8.2.1d and above
  - FOS 8.2.2a and above
  - FOS 9.0 and above

  All other versions are referred to as FOS Non EULA Aware versions.

Please note the following scenarios:

- Scenario 1: Firmware upgrade from a **non-EULA aware** Fabric OS version to **a EULA aware** Fabric OS version below 9.0 will continue to work as it is currently without needing the user to accept the EULA.

- Scenario 2: Upgrade/Downgrade from **EULA aware** Fabric OS version 8.2.x to a **non-EULA** aware version. In this case, by default, SANnav users will be prompted to accept the EULA.

- Scenario 3: Upgrade from a **EULA aware** version to another **EULA aware** version. In this case, by default, SANnav users will be prompted to accept EULA.

- Scenario 4: Upgrade from a **non-EULA aware** version to **FOS 9.x**. This upgrade will have to be done from the CLI and will fail in SANnav. In order to do this upgrade, you must upgrade to Fabric OS 8.2.1d or Fabric OS 8.2.2a first before attempting upgrade to Fabric OS 9.0.

  Note: SANnav Management Portal 2.0.x does not support firmware migration from FOS v8.2.1d and later, and 8.2.2a and later to any Fabric OS version. For these scenarios, use the CLI or WebTools to do the firmware migration or upgrade to SANnav 2.1.

1.5.13 Discovery

The following new features are introduced in SANnav Discovery:

- Support for IPv6 discovery.
- Bulk edit of multiple fabrics.
- Prevent ‘root’ account being used for fabric discovery.
- Deleting a fabric will also delete all associated historical data, logs, and other related information.

1.5.14 Extension Tunnels Management

- Single-sided tunnel and circuit configuration

- Schedule tunnel/circuit telemetry data streaming at 5-second intervals for 3 days.

1.5.15 FICON Enhancements

- Launch WebTools from FICON Configuration page (Fabric OS 9.0 and above only)
- FICON Inventory enhancement: The following columns are added to Host Port and Storage Port inventory tables and reports:
  - FC Address
  - Type
  - Model
  - Manufacturer
  - Sequence #
  - RNID Tag

1.5.16 Fabric OS EEOS (Extended End Of Support)

SANnav handles EOS HW platforms/models according to the official Brocade Policy on End Of Support Hardware platforms, see Brocade EOS Official Website

- SANnav 2.0 Behavior
  - When an EOS switch is discovered as a seed switch, discovery will fail with the popup message “This fabric cannot be discovered. Switch Model: {Model Name} is no longer supported.”
  - If the seed switch is not an EOS switch and if there are 1 or more switches in the fabric that have reached the EOS date, then fabric discovery will succeed and indicate “Switch <SwitchName> Unmonitored: End of Support” for all switches that have reached EOS in that fabric.
  - Switches that are unmonitored because the EOS date has already been reached will not be able to be monitored again.
  - Dates for EOS are defined in a SANnav configuration file (not editable).
- New SANnav 2.1 behavior
  - Customers may purchase an Extended End Of Support (EEOS) license for switches that are already EOS and install it on the switch (FOS 8.2.2b or higher is required).
  - If an EEOS license is installed on any switch that supports the EEOS feature (FOS 8.2.2b or higher), SANnav will retrieve the new extension date and apply it to reflect the extended EOS date for those switches (that is, for those customers that have purchased an EEOS license).
  - After the EEOS is installed, if the switch is in the unmonitored state, the user will have to explicitly monitor it from the SANnav **Discovery** page.

1.5.17 Miscellaneous Enhancements

- Software ID Tagging: An XML file (ISO/IEC 19770-2 compliant) for each SANnav Management Portal and SANnav Global View.
  - The file contains XML tags to briefly describe the content of the software, such as the product name, product edition, product version, and publisher
- White Listing of Client Access to SANnav server
  - By default, any IPv4 client address can connect to the SANnav server
  - Comma-separated list of IPv4 addresses/mask specify which clients can connect to the SANnav server (Management Portal and Global View)

- HTTP (Port 80) Redirection to HTTPS (Port 443)
  - In earlier releases of SANnav, HTTP port (80) was automatically redirected to HTTPS port (443) for ease of use and simplicity
  - Due to security concerns, an option will be provided to the SANnav Administrator to allow or disallow redirection of HTTP to HTTPS automatically
- SANnav Management Console Scripts: SANnav now provides a new wrapper script to customize all post-installation activities
  - man page type documentation for all SANnav scripts
  - All scripts will accept a "--help" parameter, which will detail the usage of the script.
- Feature Data Collection: Analyze SANnav usage in order to determine which features are frequently/rarely used by SANnav users.

1.6 Unsupported Features

- SANnav Management Portal Server Multi-Node deployment is no longer supported on SANnav 2.1 Management Portal.

1.7 Deprecated Features

The following features or support have been deprecated in this release and will be removed in the next release:

- SANnav → Event Management → Trap Configuration menu

1.8 Supported SAN Switches

- SANnav Management Portal 2.1.0 supports management of any Brocade Fibre Channel switch operating with Fabric OS v7.4.0 or later.
- SANnav 2.1 supports all previous versions of Fabric OS supported in SANnav 2.0 (FOS 7.4 up to FOS 8.2.2x) and adds support for FOS 9.0 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 can be deployed either on a single bare-metal host or virtual machine (VM) or on a cluster of bare-metal servers/VMs. The following tables provide details of server requirements

2.1.1 Server Requirements Details

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)	Red Hat Enterprise Linux 7.7, 8.0, 8.1 CentOS 7.7, 8.0, 8.1	Bare metal/ VMware ESXi VM	16 cores, 2000 MHz	2	48 GB	600 GB
15000 (Enterprise)	Red Hat Enterprise Linux 7.7, 8.0, 8.1 CentOS 7.7, 8.0, 8.1	Bare metal/ VMware ESXi VM	24 cores, 2000 MHz	2	96 GB	1.2 TB

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

Notes:

- On the **hard disk**, a **minimum of 120 GB** must be allocated for the **docker files** directory.
- 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.
- RHEL and CentOS 7.5 and 7.6 are no longer supported in SANnav Management Portal 2.1.

2.2 Client Requirements

The latest versions of the following web browsers are supported for SANnav client:

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

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

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

Launching of Web Tools from a SANnav 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

Upgrade from Brocade SANnav Management Portal versions 1.1.1/1.1.1a, 2.0 to Brocade SANnav Management Portal 2.1.0 is supported. Refer to the “Installation and Migration” section of the User Guide.

Supported Migration Paths:

Current Version	New Version	Supported
SANnav 1.1.0	SANnav 2.1.0	NO
SANnav 1.1.1	SANnav 2.1.0	YES
SANnav 1.1.1a	SANnav 2.1.0	YES
SANnav 2.0.0	SANnav 2.1.0	YES
SANnav 2.0.0a	SANnav 2.1.0	YES

Chapter 3: Licensing

The Brocade SANnav Management Portal can be licensed in either a **Base** or **Enterprise** version. SANnav Management Portal **Base** enables management of up to 600 ports residing on fixed port switches or embedded blade switches, but it cannot be used to manage ports from any 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 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 ports. These ports can be on the same switch or across multiple Gen 6 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 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, 4 AMPs • Base Edition (600 ports) platform and Enterprise (3K ports) platform: 8K Flows from 4 Gen6 Chassis or 16 fixed port switches.	
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 users** per SANnav Management Portal server	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.

- When performing a firmware update on switches or collect switch supportsave using the SANnav Management Portal internal repository, users must choose the option to run the SSH server on the default port 22 during the SANnav Management Portal installation for switches running firmware less than FOS v8.2.2. If port 22 on the SANnav server is reserved, then an external FTP/SFTP/SCP server must be used for such operations (firmware update and switch support save collection).

- Users can choose any available port on the SANnav server for SCP & SFTP if all the switches are running FOS v8.2.2 and above.

- 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 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_Installation_Folder>/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 4 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 highly recommended 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 a user creates a logical fabric involving logical switches from multiple chassis, auto-discovery of the created fabric may fail. In such a scenario, the user can manually discover the fabric.

- When configuring the FTP parameters (protocol, ftp location, host, password, and so on) on the switch using Configuration Operations and Monitoring Policy, the password may not be set, and, due to that, file transfer may fail.

- 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 migrated from a previous version to 2.1, the SANnav Management Portal Client keeps the previous version layout. In this scenario, the user must refresh the browser and re-log in to the client.

- When upgrading firmware on SAN directors from earlier FOS versions to v8.2.1a or v8.2.1b, the following steps must be followed to avoid the SAN directors having HA out of sync:
    - If the switch is being monitored in SANnav, first unmonitor it, and then initiate firmware download using the CLI.
    - After the firmware upgrade is successfully completed, re-monitor the switch in SANnav.

  Recovery: Run CLI commands HAdisable & HAenable to regain HA sync.

- When the SANnav Management Portal server is restored from the SANnav Management Portal backup, high granularity performance data, FCIP performance data, and flow statistics and violations are no longer collected due to new digital certificate 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.

- When attempting to download firmware on a switch with a configuration file greater than 10 MB, the operation may timeout. Retry the operation using CLI.

- Due to a design change, the event filters created during SANnav 2.0 will not be migrated in SANnav 2.1. They will have to be recreated. All other filters (Inventory filters) will be migrated.

- It is mandatory to add a Filter when generating any Time Series Reports otherwise the report generated 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 Technical Support Data collection. It is recommended to schedule SANnav backup during application idle time.

- WebTools session depends on the session time out set on the switch irrespective of direct or proxy launch. WebTools running in proxy mode validates SANnav session before sending request to the switch to avoid any illegitimate connection. As long as WebTools is open (in proxy mode), SANnav client session will be considered as active; inactive time will be computed from the time WebTools is closed.

- Backups taken from a CLI script cannot be used for restoring the data. Users are required to always collect SANnav Backup through the SANnav client.

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

- While installing SANnav in IPv6 mode, SANnav uses the below list of ports for internal communication. Please do not use those ports while customizing the SCP/SFTP server, SNMP trap, Syslog/Secure Syslog or HTTPS communication otherwise SANnav server will not start fully.

Ports used for internal communication	6060,6061,7021,7022,7051,7052,7053,7054,7055,7056,7060,7072, 7080,7082,7087,7088,7089,7090,7096,7099,7890,7997,8021,8022, 8082,8083,8085,8200,9022,9090,9091,9101,9200 and 9443

- Docker software is pre-installed on the SANnav Management Portal server. The following IP address ranges are allocated to the Docker virtual interfaces by default:

  - 172.17.0.0/16 with Gateway 172.17.0.1
  - 172.18.0.0/16 with Gateway 172.18.0.1
  - 172.19.0.0/16 with Gateway 172.19.0.1
  - 10.11.0.0/24 with Gateway 10.11.0.1

  - In an IPv4 environment deployment (VM/baremetal or OVA installation), the IP address and gateway of the SANnav Management Portal server must not be an IP address within the ranges above.
    - **Note**: Even though the installation may be successful when choosing an IP address within the ranges above, the SANnav Management Portal server may later be unreachable. Therefore, it is mandatory to avoid doing so in order for SANnav server to start successfully.

  - **Important**: If the IP address of any switch that will be managed by SANnav Management Portal server is within the IP address ranges above, **please contact Brocade support to change the docker virtual IP interface IP address range**.

- **Firewalld Backend Configuration:**

  When Centos/RHEL 8.0 OS boots, "firewalld" backend defaults to using "nftables" instead of "iptables". The current version of Docker used by 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". Please 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 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

  1. Stop the firewalld using the command **systemctl stop firewalld**
  2. Edit the firewalld configuration using the command **vi /etc/firewalld/firewalld.conf** and change the FirewallBackend=**nftables** to FirewallBackend=**iptables**
  3. Start the firewalld using the command **systemctl start firewalld**
  4. Reload the firewalld using the command **firewall-cmd --reload**

- When installing SANnav Management Portal 2.1.0 and the firewall needs to be enabled, please ensure the "firewalld" backend 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, the Fabric and Switch discovery in SANnav Management Portal will fail (network reachability issue). However, if this happens, follow the procedure below 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

- When a SANnav *local username* (e.g., Administrator) also exists on an external authentication server configured in SANnav (e.g. LDAP/TACACS+/Radius), do not log in with that username into SANnav (e.g. Administrator)

using the credentials present on the *external* authentication server. If you do log in with the local username using the external server credentials for that user (e.g. Administrator), then the SANnav *local* username will be changed as an *external* user in SANnav. This will result in the fact that the *external* user (e.g. Administrator) will no longer be able to log in to SANnav using the *local* credentials that are configured in SANnav.

- In order to avoid this problem, please login to SANnav by using another username that exists on the external server authentication server (e.g. LDAP/TACACS+/Radius) but is not a SANnav local user.

Chapter 6: Security Vulnerability Fixes

This section lists the Common Vulnerabilities and Exposures (CVEs) that have been addressed. Each CVE is identified by the CVE ID number.

The following CVEs have been addressed in SANnav 2.1.0:

CVE ID: CVE-2019-16211 - Brocade SANnav versions before v2.1.0, contain a Plaintext Password Storage vulnerability. Database credentials are stored in plaintext in a configuration file. An unauthenticated malicious user with access to the configuration file may obtain the exposed password to gain access to the application database.

CVE ID: CVE-2019-16212 - A vulnerability in Brocade SANnav versions before v2.1.0 could allow a remote authenticated attacker to conduct an LDAP injection. The vulnerability allows a remote attacker to bypass the authentication process.

Chapter 7: Defects

7.1 Known Issues in SANnav Management Portal v2.1.0

Defect ID	Description
SANN-111969	Included/excluded port list is shown empty in ALL_PORTS System group. Also, ALL_QUARANTINED_PORTS is incorrectly allowed to be modified from SANnav.
SANN-113381	Installation fails with "Failed to Initializer Docker Swarm ... Exiting" error.
SANN-118699	Investigation view show zero values for some measures.
SANN-120191	After importing switch configuration from chassis, attribute wwnPidMode is missing from the configuration.
SANN-121451	An error is displayed when trying to save/enable tunnel with IPSec.
SANN-122352	User will have to wait for a long time to see the devices in the Add Members dialog
SANN-122357	"No data to display" message shown for brief period in Flow Investigation view.
SANN-122503	Loading saved topology takes several minutes
SANN-122600	Tags and description are not shown in zone alias page
SANN-122603	SANnav OVA installation fails with error "Error response from daemon: This node is not a swarm manager. .."
SANN-122628	User observes an error popup dialog over a popup dialog while applying license changes
SANN-122671	Unsupported switches are shown while restoring the logical fabric configuration
SANN-122677	FOS Update dialog lists some switches that do not need EULA acceptance in the EULA agreement prompt.
SANN-122681	Manual Config backup operation fails occasionally.
SANN-122689	Extension Tunnel Transmission dialog does not correctly display IPEX as being enabled on a tunnel.
SANN-122704	Blank topology page displayed for a saved device context
SANN-122741	Double quotes are shown incorrectly in the reports
SANN-122747	User will see inaccurate recommended action

SANN-122751	User will see an error during migration “Issue in Migration org.elasticsearch.client.ResponseException”.
SANN-122767	Switch type filter is not working after migration
SANN-122774	Primary fabric gets segmented
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 ration rule box checked even though it was disabled in 2.0
SANN-122819	FC address shown instead of alias name in the tool tip in Flow Investigation view
SANN-122846	Sometimes, investigate view is not launched followed for extension tunnels
SANN-122858	Hybrid storage missing in the storage report.
SANN-122860	Negative value for port index is shown in global reports
SANN-122867	Port WWN is shown in place of the zone alias in health summary dashboard
SANN-122868	User defined value for zone DB size is not migrated to 2.1
SANN-122882	Alerts widget may display only one type of alerts for some Portals.
SANN-122884	Alerts widget displays only one type of alerts for a few Portals.
SANN-122895	User can see more device ports than what was shown while saving topology
SANN-122901	User sees duplicate lines displayed in port investigation view
SANN-122908	Only the first and last entries are selected while scheduling port data collection
SANN-122909	User will see a continuous spinner while investigating single sided tunnel
SANN-122914	User will see incorrect date and time.
SANN-122942	The chart keeps loading for very long time.
SANN-122946	Scheduled switch configuration backup is not working
SANN-122947	The violations drill down popup dialog is empty
SANN-122948	Ports that are disabled or disconnected are getting listed in topology context selection.
SANN-122953	User will see drift check failed messages in events.
SANN-122957	User will not be able to perform Firmware download.

SANN-122959	Unable to push MAPS actions to switch.
SANN-122962	Users are not notified about the changes done in the Zone.

7.2 Defects closed with code change in SANnav Management Portal v2.1.0

Defect ID	Description
SANN-104547	Unable to perform Firmware download operation using an external SFTP server.
SANN-105289	The user will see 'Network Advisor' as the source in the RAS logs displayed in Events page.
SANN-109199	Unable to create policy with IP_EXTN_Flow measure
SANN-109512	Unable to view the changes done to Quiet Time configurations on a rule in an active policy
SANN-110106	Switch CLI shows additional sub-directory with the name "tracedump/<arbitrary string>" is created inside the autoftp location.
SANN-110499	Distribute operation will fail for the MAPS policy with RoR rules
SANN-110976	SupportSave generation fails with reason "Invalid Arguments"
SANN-111193	SANnav shows firmware download status as completed though it is still in progress on the switch.
SANN-116240	'Add' button is not enabled for Filters when creating SNMP Trap forwarding Destination.
SANN-117062	Unable to receive Performance stats
SANN-117511	Incorrect results generated when user applies filter using tags.
SANN-117512	A generated report does not get listed.
SANN-117842	Newly created Logical Fabric is not automatically discovered.
SANN-118348	Configuration import fails with error "Proxy Service - Server unable to process your request".
SANN-118358	In the Health Summary dashboard, the host health score will be reduced even though hosts are zoned per peer zone best practice.
SANN-118450	Save operation fails when trying to edit a Extension Tunnel.
SANN-118614	Three minutes before the inactive duration, a message is displayed asking whether the user wants to continue the session.
SANN-118776	In Dashboard, the client goes blank when the distribution bands are deselected for the Product and Port Distribution widgets.
SANN-118843	SANnav Historical Performance Monitoring is not working.

SANN-118844	SANnav installation fails
SANN-120378	Forwarded SysLog messages contains "SPECTRE" instead of "SANnav".
SANN-120618	vCenter discovered in SANnav experiences high CPU load.
SANN-121799	Hosts showing degraded health status
SANN-122369	User stops receiving events email notifications
SANN-122575	Zone compare shows zone aliases in non-peer zones as principal zone aliases.

7.3 Defects closed without code change in SANnav Management Portal v2.1.0

Issue key	Custom field (Symptom)
SANN-121142	Unable to investigate the circuit's performance metrics
SANN-120790	Hosts showing degraded health status
SANN-120379	Zoning changes are being sent to syslog server with original fabric discovery user ID instead of the current user ID logged into SANnav.
SANN-120257	Email event notifications are not received
SANN-119979	Compare button is disabled and becomes unavailable on all zone configurations.
SANN-118826	Imported Fabric OS 8.2.2.zip is not listed in the SANnav 2.0.0
SANN-118420	Server hangs when upgrading the SANnav 1.1.1 server
SANN-117790	Incorrect message shown during multi node installation.
SANN-117755	"Add logical Switch" dialog pops up even when there is no port movement involved.
SANN-117121	When moving a port from one Logical Switch to another, SANnav reports success but the operation is actually not successful on the switch.
SANN-116426	Users will see HA out of sync during FWDL
SANN-115606	User may notice section of 60 second samples in Investigation view for port performance stats, where the value will modulate between the actual values and zero.
SANN-115482	Drift check fails showing status as 'Check Failed'.
SANN-112991	In zone config comparison dialog, user cannot see the zone names when there are membership changes.
SANN-112902	Fabric parameters are not displayed for a VF-disabled switch.
SANN-112194	When user compares a zone configuration, incorrect color representation is shown for the changes (e.g. Deleted, Inserted etc.) when viewing with "Inline" option.
SANN-111342	Incorrect warning message "Service is not available at this time" displayed during FCR configuration.
SANN-111015	Configuration drifts are shown even when there are no actual drifts
SANN-110822	Occasionally, when viewing high granularity performance data (2-second) for Rx/Tx metrics in the investigate view, users will see the values drop to zero, even though traffic was not really zero at that point in time.
SANN-110814	SupportSave collection fails stating 'Unable to connect the remote host - timed out'

SANN-110188	Configured MAPS actions will not take effect and there is no explicit indication
SANN-109246	Generated reports do not honor the sorting.
SANN-104873	Application performance is sluggish when user tries to import/view a zone config which has 5K or more zones.

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
1.4	Initial version of Digest Edition	10/23/2020