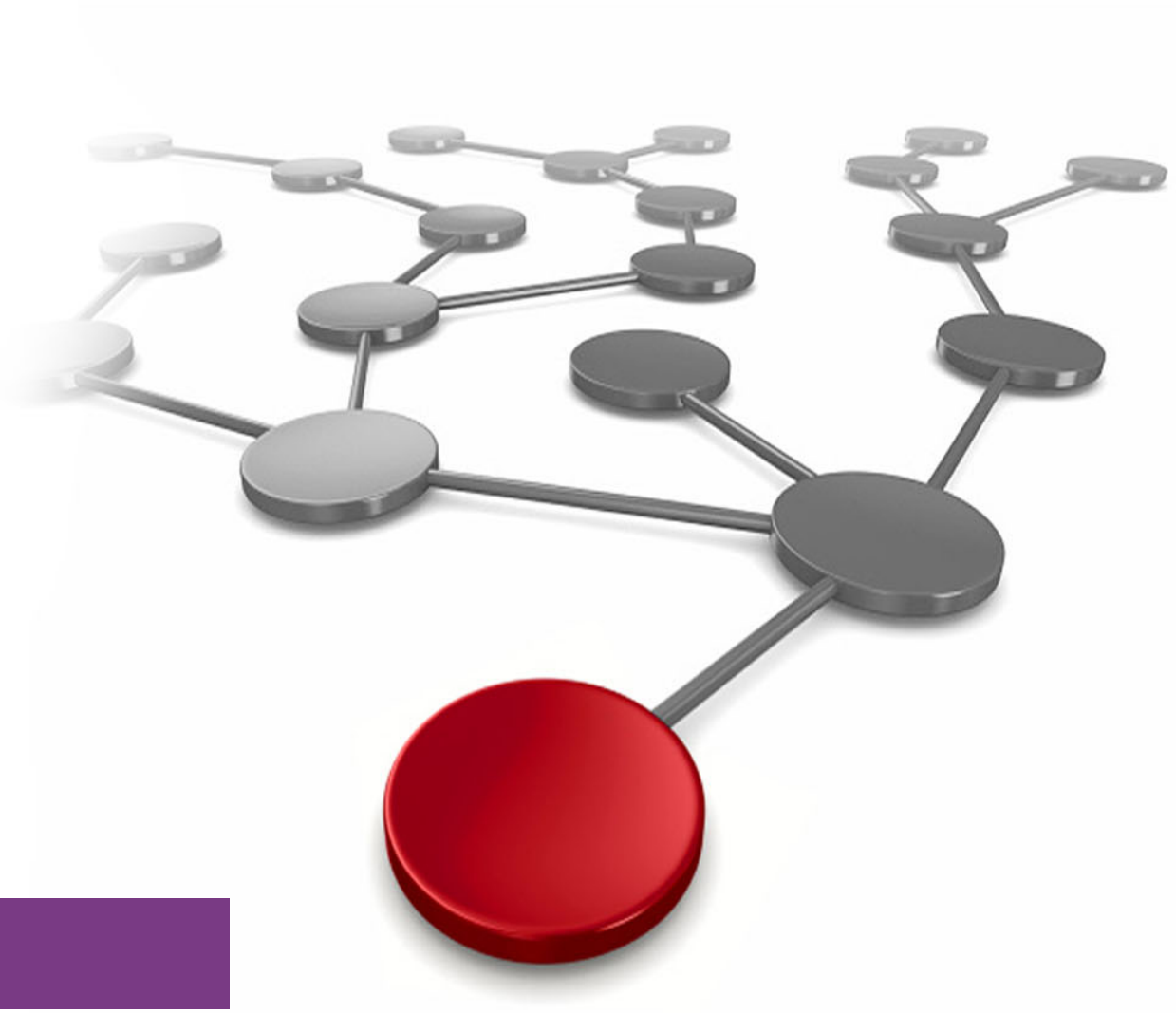
Redbooks
ibm.com/redbooks

IBM SANnav Management Portal v2.2.X Implementation Guide

Vasfi Gucer
Kai Jehnen
Piotr Kurkowski
Hartmut Lonzer
Dirk Preinl
Thomas Scheld
Simeon Tsonev



Storage

IBM

Redbooks

IBM Redbooks

IBM SANnav Management Portal v2.2.X Implementation Guide

January 2023

SG24-8534-00

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

First Edition (January 2023)

This edition applies to IBM SANnav Management Portal v2.2.

Contents

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

C3®	IBM FlashSystem®	Redbooks (logo)  ®
FICON®	IBM Spectrum®	Storwize®
IBM®	Redbooks®	

The following terms are trademarks of other companies:

ITIL is a Registered Trade Mark of AXELOS Limited.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

VMware, VMware vCenter Server, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Other company, product, or service names may be trademarks or service marks of others.

Preface

IBM® SANnav Management Portal and IBM SANnav Global View empower IT administrators to be more efficient and productive by providing comprehensive visibility into the SAN environment. These tools transform information about SAN behavior and performance into actionable insights, allowing administrators to quickly identify, isolate, and correct problems before they impact the business. In addition, SANnav Management Portal and SANnav Global View accelerate administrative tasks by simplifying workflows and automating redundant steps, making it easier for organizations to realize their goal of an autonomous SAN.

This IBM Redbooks® publication introduces IBM SANnav Management Portal and SANnav Global View, and covers the installation, customization, operation, and troubleshooting of the IBM SANnav Management Portal.

This book is targeted at IT and network administrators.

Authors

This book was produced by a team of specialists from around the world.

Vasfi Gucer is the Storage Team Lead of the IBM Redbooks Team. He has more than 25 years of experience in the areas of systems management, networking hardware, and software. He writes extensively and teaches IBM classes worldwide about IBM products. His focus has been primarily on storage, cloud computing, and cloud storage technologies for the last 15 years. Vasfi is an IBM Certified Senior IT Specialist, Project Management Professional (PMP), IT Infrastructure Library (ITIL) V2 Manager, and ITIL V3 Expert.

Kai Jehnen is the Europe, Middle East, and Africa (EMEA) lead for SAN remote technical support at the EMEA Storage Competence Center (ESCC) in Frankfurt, Germany. In this role, he leads a team of technical experts in EMEA who support IBM clients through both break/fix support and billable services. In his 15+ years at IBM, he worked in various roles in storage remote support and gained skills for various IBM storage products.

Piotr Kurkowski is a subject matter expert (SME) for IBM Spectrum® Virtualize and SAN. He has worked for the last 12 years for EMEA as Storage and SAN support. He has 26 years of experience working as a system administrator, field engineer, and remote technical support who supports many IBM hardware and software products. Piotr has been working at IBM in various technical and team lead positions for 25 years.

Hartmut Lonzer is the IBM FlashSystem® Territory Account Manager for Deutschland (Germany), Austria, and Confœderatio Helvetica (Switzerland) (DACH). In addition, he covers the SAN portfolio as Offering Manager for DACH. Before this position, he was OEM Alliance Manager for Lenovo in IBM Germany. His working location is at the IBM German headquarter in Ehningen. His main focus is on the IBM FlashSystem family and the IBM SAN Volume Controller. His experience with IBM SAN Volume Controller and IBM FlashSystem products goes back to the beginning of these products. Hartmut has been with IBM in various technical and sales roles for 44 years.

Dirk Preinl is a SME for IBM Storage and SAN technical support. He holds a degree in Information Technologies from the University of Applied Sciences Friedberg in Germany, and has more than 25 years of experience in IT. He works for IBM Systems to provide support and guidance for IBM SAN Volume Controller, IBM Storwize®, and IBM FlashSystem for customers in EMEA. Dirk has more than 20 years of experience with IT infrastructures, and has worked directly and indirectly for systems integrators and consultancy companies and storage, networking, and infrastructure hardware and software vendors. In his positions with these companies, he acquired in-depth technical knowledge of storage, Fibre Channel, high availability, backup, and disaster recovery (DR) technologies.

Thomas Scheld is a Senior Systems Engineer Storage Networking for Brocade and Broadcom. His responsibilities include consulting for customers in pre-sales engagements. Thomas works throughout the engagement lifecycle by identifying, designing, planning, and implementing complex storage area networking solutions. In addition, Thomas is responsible for providing knowledge transfer through workshops and technical presentations.

Simeon Tsonev is a SME for IBM SAN switch products. He has been with IBM for 6 years. He started as a support agent for mid-range storage before focusing on SAN and IBM FlashSystem products. In addition to his support role, he has prepared and held lectures on Fibre Channel protocol (FCP), SAN hardware, and software products over the years for IBM.

Thanks to the following people for their contributions to this project:

Wade Wallace
Senior Editor, IBM Redbooks

The team would like to thank to the following people from **Broadcom Inc** for their contributions to this project:

Brian Larsen, Salim Galou, Tim Werts

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, IBM Redbooks
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Introducing IBM SANnav Management Suite

This chapter describes all the system and server requirements that you must meet before you plan the IBM SANnav Management suite installation. The system and server requirements for the deployment of SANav Management Portal and IBM SANnav Global View are described.

This chapter includes the following topics:

- Introduction
- SANnav Management Portal
- SANnav Global View
- IBM SANnav Management Suite v2.2 release overview
- IBM SANnav Management Portal v2.2 release overview
- IBM SANnav Global View v2.2 release overview

1.1 Introduction

IT organizations are facing an ever-increasing volume, variety, and velocity of data, yet users still expect data centers to deliver maximum performance, business intelligence, and operational efficiency. As organizations race to modernize the data center to support innovation and digital transformation, these demands are driving storage networks to evolve even faster to accommodate new applications. Therefore, SAN administrators need ways to simplify management, visualization, and analysis of their SAN performance and overall operational health. Many organizations lack these capabilities due to the growing complexity of their IT environments and the lack of easy-to-use SAN management tools.

IBM SANnav Management Portal and IBM SANnav Global View empower IT by simplifying processes and delivering the correct information at the correct time. IBM SANnav Management Portal processes and transforms billions of metrics about SAN behavior and performance into actionable insights, allowing administrators to quickly identify, isolate, and correct problems even before they start impacting the business. In addition, IBM SANnav Management Portal and IBM SANnav Global View eliminate the tedious and repetitive tasks of managing, monitoring, and alerting on issues that affect the SAN. These products accelerate administrative tasks by applying a single action across multiple SAN switches by using bulk actions.

Note: In this chapter, IBM SANnav Management Portal or IBM SANnav Global View might also be referred to as SANnav Management Portal or SANnav Global View.

1.2 SANnav Management Portal

SANnav Management Portal is a next-generation SAN management application that uses a browser-based GUI without needing a Java-based thick client. SANnav Management Portal focuses on streamlining common workflows, such as configuration, zoning, deployment, troubleshooting, and reporting. With SANnav Management Portal, the administrator's frequent tasks of configuring SAN switches or provisioning new devices to fabrics are no longer a matter of sending hundreds of individual command-line interface (CLI) commands to multiple switches. Instead, configuration policy management and zoning management allow SAN administrators to quickly and consistently configure hundreds of switches and devices in matters of seconds in a non-error-prone fashion. SANnav Management Portal also increases operational efficiencies by enabling enhanced monitoring capabilities to provide faster troubleshooting and simplify frequent and common configuration use cases.

SANnav Management Portal allows management of one or more SAN fabrics that are in the same or different geographical locations, and it supports a maximum of 15,000 physical SAN ports. For environments that are larger than 15,000 ports, you can deploy multiple SANnav Management Portal instances. SANnav Management Portal does not replace Brocade WebTools or the Fabric OS (FOS) CLI.

For more information, see SANnav Management Portal and SANnav Global View.

1.2.1 Scaling without compromising performance

Most organizations are overwhelmed by the enormous volume of storage data that they must process daily. Even well-managed IT organizations struggle to keep up with the demand for storage. IBM SANnav Management Portal enables linear scaling of business services without compromising performance so that organizations can easily scale their management to meet the requirements of new servers and storage that is deployed. With the enormous growth, organizations also must reduce the manual process of correlating millions of data points to extract useful information for the business. To increase efficiency, enterprises need tools that collect, aggregate, distribute, and serve the correct data at the correct time.
SANnav Management Portal delivers actionable intelligence in a consumable and uniquely optimized manner for up to 25 different users concurrently. This actionable intelligence can be collected and processed by streaming from FOS switches and a state-of-the-art software infrastructure for SANnav Management Portal 25 different users and REST sessions (combined) concurrently.

1.2.2 Reducing administrative tasks by automating processes

Even the most experienced storage administrator can get overwhelmed by the operational steps that are required to deploy and manage new resources, fabric zoning, inventory, reports, and security settings, and extract intelligence from it all. SANnav Management Portal focuses on automating as many processes as possible to free operational cycles so administrators can focus on tasks. With configuration policy management, it accelerates the commissioning or replacing of switches, hosts, and storage arrays. It also has features that automatically identify inconsistencies with zoning databases in multiple SAN fabrics, security-related features, and many other features.

1.3 SANnav Global View

Whether an organization has data center locations across the globe or a single, multi-tenant data center, it is important for administrators to understand the health of the entire SAN. With SANnav Global View, administrators can quickly visualize the health, performance, and inventory of multiple SANnav Management Portal instances by using a simple, intelligent dashboard. In addition, administrators can easily navigate from SANnav Global View down to the local environment that is managed by SANnav Management Portal to investigate points of interest. Important events across all local environments are propagated at a global level for instant visibility in the alerts box. Using powerful search capabilities within SANnav Global View, administrators can seamlessly navigate across instances and drill down into any individual SANnav Management Portal instance for more details.

SANnav Global View aggregates the configuration policy drifts that are detected by each SANnav Management Portal instance in a dashboard summary widget. With a few clicks, SANnav Global View can enforce a customer’s “golden” configuration policy across all instances of SANnav Management Portal that it manages. Then, when drifts are detected by each SANnav Management Portal instance, they are aggregated into the main SANnav Global View Summary dashboard, which eliminates the need for the SAN administrator to monitor each local instance.

Brocade Fibre Channel hardware includes integrated network sensors that gather millions of real-time metrics that SANnav Management Portal uses to identify, monitor, and analyze the overall health and performance of the SAN. This data is contextualized into dashboards that can be used to quickly detect and isolate problems. At a glance, administrators have actionable intelligence on the overall health of their fabric, switches, servers, and storage, which they can view in the form of summary health score circles. The summary health score circles help administrators quickly identify areas that require further investigation. Administrators can drill down from each dashboard into investigation mode to further examine any relevant data for performance optimization or troubleshooting.

1.4 IBM SANnav Management Suite v2.2 release overview

SANnav is the next generation SAN management application suite for IBM b-type SAN environments. SANnav allows you to efficiently manage your SAN infrastructure through various easy-to-use functions.

SANnav implements a highly scalable client/server architecture for SAN management. With a modern browser-based UI, SANnav eliminates the need for a Java-based thick client.

The user interface of SANnav is based on real-world use cases and user workflows, and provides a highly intuitive user experience.

SANnav also uses a micro-services-based architecture that is based on Docker container technology so that it can scale the management needs of small and large SAN environments. Those environments can change over time. This scalable architecture also allows SANnav to support new functions in the future without causing degradation to the performance of the application.

To address the management needs of large-scale SAN environments or those environments that are distributed by function or location, SANnav supports a hierarchical management model. In this model, a higher-level “global” application (SANnav Global View) provides comprehensive visibility, summarization, and seamless navigation across multiple instances of the SANnav Management Portal application.

The following SANnav product offerings are available:

- IBM SANnav Management Portal
- IBM SANnav Global View

1.4.1 New hardware platforms that are supported in IBM SANnav v2.2

SANnav v2.2.0 is a major new release of the IBM b-type Fibre Channel SAN management software products IBM SANnav Management Portal and IBM SANnav Global View. SANnav Management Portal v2.2.x supports the introduction of IBM b-type Gen 7 platforms with FOS 9.X, and adds features and capabilities that make managing IBM b-type Gen 7 SAN environments easier than ever before.

Supported hardware and software

SANnav Management Portal v2.2.x supports the Brocade FOS software versions and hardware platforms that are listed in this section.

FOS software support for the following releases:

- FOS 9.0 or later
- FOS 8.0 or later
- FOS 7.4 or later

Table 1-1 through Table 1-8 on page 6 show the supported switches and directors.

Table 1-1 IBM Gen 7 (64G) fixed-port switches

IBM name	IBM machine type and model (MTM)	Brocade MTM
IBM System Networking SAN128B-7	8969-P96/R96	Brocade G730 switch
IBM System Networking SAN64B-7	8960-P64/R64	Brocade G720 switch

Table 1-2 IBM Gen 7 (64G) directors

IBM name	IBM MTM	Brocade MTM
IBM System Networking SAN512B-7	8961-F78	Brocade X7-8 director
IBM System Networking SAN256B-7	8961-F74	Brocade X7-4 director

Table 1-3 IBM Gen 6 (32G) fixed-port switches

IBM name	IBM MTM	Brocade MTM
IBM System Networking SAN128B-6	8960-F97/N97 8960-F96/N96	Brocade G630 v2 Brocade G630 v1
IBM System Networking SAN64B-6	8960-F65/N65 8960-F64/N64	Brocade G620 v2 Brocade G620 v1
IBM System Networking SAN24B-6	8969-F24 8960-F24	Brocade G610
IBM System Networking SAN18B-6	8960-R18	Brocade 7810

Table 1-4 IBM Gen 6 (32G) directors

IBM name	IBM MTM	Brocade MTM
IBM System Networking SAN512B-6	8961-F08	Brocade X6-8 director
IBM System Networking SAN256B-6	8961-F04	Brocade X6-4 director

Table 1-5 IBM Gen 5 (16G) fixed-port switches

IBM name	IBM MTM	Brocade MTM
IBM System Networking SAN96B-5	2498-F96 2498-N96	Brocade 6520 switch
IBM System Networking SAN48B-5	2498-F48	Brocade 6510 switch
IBM System Networking SAN24B-5	2498-F24 2498-X24	Brocade 6505 switch

Table 1-6 IBM Gen 5 (16G) directors

IBM name	IBM MTM	Brocade MTM
IBM System Storage SAN768B-2 Backbone	2499-816	Brocade DCX 8510-8 Backbone
IBM System Storage SAN384B-2 Backbone	2499-416	Brocade DCX 8510-4 Backbone

Table 1-7 IBM Gen 4 (8G) fixed-port switches

IBM name	IBM MTM	Brocade MTM
IBM SAN06B-R Extension switch	2498-R06	Brocade 7800 switch
IBM SAN24B-4 switch	2498-B24	Brocade 300 switch

Table 1-8 IBM Gen 4 (8G) directors (not supported in IBM SANnav v2.2.1)

IBM name	IBM MTM	Brocade MTM
IBM System Storage SAN768B Backbone	2499-384	Brocade DCX Backbone
IBM System Storage SAN384B Backbone	2499-192	Brocade DCX 4S Backbone

Switches that support data streaming

SANnav uses Kafka to provide real-time data streaming from switches that are running FOS 8.2.1a or later. Data streaming provides for the collection of high-frequency performance statistics, Fibre Channel over IP (FCIP) performance and error statistics, and flow statistics and violations.

The following Gen 7 platforms support data streaming:

- IBM SAN64B-7 and IBM SAN128B-7 switches
- IBM SAN256B-7 and SAN512B-7 directors

The following IBM b-type Gen 6 platforms support data streaming:

- IBM SAN24B-6, SAN64B-6, and SAN128B-6 switches
- IBM SAN18B-6 switch
- IBM SAN256B-6 and SAN512B-6 directors

1.5 IBM SANnav Management Portal v2.2 release overview

SANnav Management Portal allows the management of one or more SAN fabrics that are in the same or different geographical locations. It also supports managing a maximum of 15,000 physical SAN ports.

For environments that are larger than 15,000 ports, you can deploy multiple SANnav Management Portal instances, which can be managed by SANnav Global View. Use SANnav Management Portal to monitor and manage fabrics, switches, switch ports, and other elements of your SAN.

Dashboards provide summary status and performance information from which you can drill down to get detailed views. By using filters and tags, you can sort and search your inventory to find the information that you want.

A highly flexible reporting infrastructure allows you to generate custom graphical or tabular reports. SANnav Management Portal does not replace Brocade WebTools or the FOS CLI.

1.5.1 Browser requirements

The latest versions of the following web browsers are supported for a SANnav Management Portal v2.2.0 client:

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

Note: If you access the client from Remote Desktop, the user interface might degrade performance. Starting Brocade WebTools 9.0.0 and later from a SANnav client is supported on Chrome (on Windows, Linux, and MacOS), Firefox (on Windows and Linux), or Edge (on Windows). Starting Brocade WebTools versions earlier than 9.0.0 is supported on Firefox only.

1.5.2 IBM SANnav Management Portal server platform support and infrastructure

IBM SANnav Management Portal v2.2.0 can be deployed on a single bare-metal host or virtual machine (VM) or on a cluster of bare-metal servers or VMs. The tables that are included in this section provide more information about server requirements.

For more information about installing SANnav Management Portal on a VM, see SANnav Management Portal and SANnav Global View.

1.5.3 Server requirements

Table 1-9 shows the VM or bare-metal installation requirements.

Table 1-9 VM or bare-metal installation

Product and edition	Maximum switch ports or instances under mangement	Operating system	Host type	vCPU	Memory	Hard disk
SANnav Management Portal Base Edition (Manages switches only, not directors.)	600 ports	Red Hat Enterprise Linux (RHEL) 7.9, 8.4, 8.5, and 8.6 Community Enterprise Operating System (CentOS) 7.9 only	Bare-metal/ESXi ESXi/HyperV VM OVA (CentOS 7.9)	16 cores	48 GB	600 GB
SANnav Management Portal Enterprise Edition (Required to manage directors.)	Up to 3000 ports	RHEL 7.9, 8.4, 8.5, and 8.6 CentOS 7.9 only	Bare-metal/ESXi ESXi/HyperV VM OVA (CentOS 7.9)	16 cores	48 GB	600 GB
	3000 - 15,000 ports	RHEL 7.9, 8.4, 8.5, and 8.6 CentOS 7.9 only	Bare-metal/ESXi ESXi/HyperV VM OVA (CentOS 7.9)	24 cores	96 GB	12 TB
SANnav Global View	Up to 20 SANnav Management Portal instances	RHEL 7.9, 8.4, 8.5, and 8.6 CentOS 7.9 only	Bare metal/ESXi ESXi/HyperV VM	16 cores	92 GB	450 GB

Table 1-10 and Table 1-11 shows the ordering information for SANnav products.

Table 1-10 Ordering information for SANnav products (1of 2)

SANnav Management Portal		
License	**Supported ports**	**Duration**
Trial (Enterprise Edition with no license)	15,000	30-day trial period
Base Edition (Manages switches only, not directors)	600	BR SKUs are offered 1-year to 7-year durations in increments of 1 year. All OEM SKU durations continue to be 1, 3, or 5 years.
Enterprise Edition (Required to manage directors.)	15,000	BR SKUs are offered 1-year to 7-year durations in increments of 1 year. All OEM SKU durations continue to be 1, 3, or 5 years.

Table 1-11 Ordering information for SANnav products (2 of 2)

SANnav Global View		
License	**Supported ports**	**Duration**
Trial (no license)	20 SANnav Management Portal instances	30-day trial period
SANnav Global View license	20 SANnav Management Portal instances	BR SKUs are offered 1-year to 7-year durations in increments of 1 year. All OEM SKU durations continue to be 1, 3, or 5 years.

1.6 IBM SANnav Global View v2.2 release overview

Brocade SANnav Global View v2.2.0 is a major software release that was introduced to support FOS 9.1.x and provide new or major feature enhancements on SANnav Global View v2.2.x.

This section highlights the new features, support, capabilities, and changes in SANnav Global View v2.2.0.

1.6.1 What is new in IBM SANnav Global View v2.2.0

SANnav Global View v2.2.0 provides new features and feature enhancements that aim at simplifying and automating common and frequent use cases.

Highlights of the SANnav v2.2 release include the following items:

- Eliminate tedious and repetitive tasks to manage, monitor, and alert on issues impacting the SAN.
- Gain immediate understanding of the health, performance, and points of interest across the SAN.

- Accelerate the deployment of new switches, hosts, and targets with SANnav configuration policy management.
- Continue to provide security features and enhancements in all areas.

Specifically, new features or feature enhancements are provided in each of the following areas:

- Server platform installation, migration, and deployment
- Server platform installation, and OS support
- Infrastructure and security
- SANnav licensing
- Configuration policy
- Managing portals and portal discovery
- Inventory
- Dashboard and reports
- SANnav backup
- SANnav support data collection
- Usability enhancements

1.6.2 SANnav Global View Server platform support, OS support, and infrastructure

This section covers SANnav Global View Server platform support, OS support, and infrastructure.

SANnav Global View OS support (VM and bare metal)

SANnav Global View v2.2.0 officially supports the versions of RHEL and CentOS that are shown in Table 1-12.

Table 1-12 Server requirements: SANnav Global View

Maximum SANnav Management Portal instances supported	Operating system	Host type	Minimum vCPU	Minimum number of vCPU sockets	Memory	Hard disk
20	RHEL 7.9, 8.4, 8.5, 8.6 CentOS 7.9 only	Bare-metal/ VMware ESXi/7.0 VM	16 cores at 200 MHz	2	32 GB	450 GB

Note: In SANnav Global View v2.2.0, the installation script allows users to install SANnav Global View on RHEL 7.8 or 8.1, or 8.3. The installation script displays a warning message indicating that the SANnav Global View installation will proceed on an untested and unqualified OS version. Explicit customer acceptance is required for the SANnav Global View installation to proceed.

Note: Using IBM SANnav on an earlier or later release level of RHEL or CentOS other than the ones that are qualified for IBM SANnav v2.2.0 (CentOS 7.9, and RHEL 8.2 and 8.4) is explicitly not qualified or tested by Brocade. This scenario might be supported by Brocade unless an issue is found to be caused by using a different RHEL or CentOS version. IBM SANnav issues that occur when using an unqualified version of RHEL or CentOS will be addressed at Brocade's discretion.

For IBM SANnav Global View v2.2.0 release, compatibility with RHEL 8.5 was not tested at the time of writing. Therefore, RHEL 8.5 and later support for IBM SANnav Global View v2.2.x is subject to this rule and depend on whether compatibility issues between IBM SANnav v2.2.x and the RHEL versions are found.

Note: For both CentOS and RHEL (all versions), the following setting must be set in the OS on which SANnav Global View server is installed:

```
Language = English and Locale = US
```

Other languages and locales are not supported.

Client requirements

The latest versions of the following web browsers are supported for the SANnav Global View v2.2.0 client:

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

SANnav Global View v2.2.0 and FIPS-140 enabled OS

SANnav Global View v2.2.0 is supported on FIPS-140-enabled RHEL or CentOS (all deployment models, bare-metal, and VM):

- FIPS-140 mode may be enabled before installing SANnav.
- For the exact command to enable FIPS mode, see the RHEL/CentOS specific OS version.

Note: SANnav is *not* FIPS-140 certified. SANnav v2.2.0 can be installed and run on an officially supported RHEL or CentOS version with FIPS-140 enabled.

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

Note: SANnav Management Portal v2.2 cannot be installed on Security Enhanced Linux (SELinux) in Enforcing or Permissive mode on either CentOS or RHEL (all versions). The only SELinux mode that is supported is Disabled.

For more information, see *Brocade SANnav Global View v2.2.0 Brocade Release Notes (Digital Edition)*.

2

Preparing the environment

To get started with SANnav, you need two things in addition to the hardware setup (server, SAN devices to monitor, and networking):

- License certificate
- SANnav software

This chapter describes how to create the license certificate and download the SANnav software by using IBM Fix Central.

This chapter includes the following topic:

- Licensing

2.1 Licensing

SANnav uses subscription-based licensing that must be renewed at the end of the subscription period. Failure to do so leads to an inability to work with SANnav. Therefore, it is crucial to obtain a new license early enough to ensure uninterrupted operation.

Note: IBM SANnav Management Portal comes with a 30-day trial period that starts at the day of installation.

2.1.1 SANnav versions

There are two different SANnav products that are available that require different licenses:

- SANnav Management Portal (Base and Enterprise version)
- IBM SANnav Global View

Depending on the environment to be managed by SANnav, the correct version must be chosen. Table 2-1 shows the differences between the versions.

Table 2-1 Differences between Base and Enterprise versions

Version	Number of ports that is managed	Device types that are managed
SANnav Management Portal Base	Maximum of 600	Fixed port switches and embedded blade switches
SANnav Management Portal Enterprise	Maximum of 15,000	Fixed port switches, embedded blade switches, and directors (4 or 8 slots)
SANnav Global View	N/A	Up to 20 SANnav Management Portal instances

2.1.2 SANnav machine types

SANnav is handled by IBM as a *pseudo-hardware* product. It has a machine type, model, and a 7-digit serial number (7xxxxxx), as shown in Table 2-2.

Table 2-2 SANnav machine types and models

IBM machine type and model	Product and subscription period
9239-B01	SANnav Management Portal Base, 1-year subscription
9240-B03	SANnav Management Portal Base, 3-year subscription
9241-B05	SANnav Management Portal Base, 5-year subscription
9239-E01	SANnav Management Portal Enterprise, 1-year subscription
9240-E03	SANnav Management Portal Enterprise, 3-year subscription
9241-E05	SANnav Management Portal Enterprise, 5-year subscription

9239-G01	SANnav Global View, 1-year subscription
9240-G03	SANnav Global View, 1-year subscription
9241-G05	SANnav Global View, 1-year subscription

This information is provided by IBM on purchase on a sticker on a paper that is titled *IBM SANnav Registration Information*.

The example that shown in Figure 2-1 is for SANnav Management Portal Base with a 5-year subscription (9241-B05).

Figure 2-1 Machine type, model, and serial number sticker

2.1.3 Creating a license certificate

The license is created from two components:

- Server unique ID (UID): Available when the software is installed (see Chapter 3, “Installing and deploying IBM SANnav Management Portal” on page 25).
- Transaction key: Provided by IBM through a letter that also contains the sticker with the machine type, model, and serial number.

Figure 2-2 shows a transaction key example.

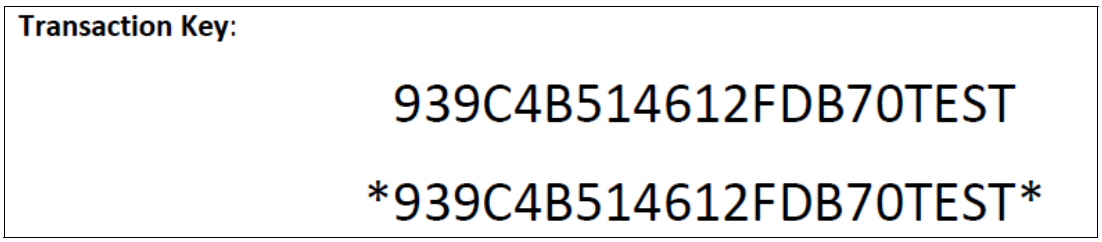


Figure 2-2 Transaction key example

Note: Do not discard the letter or the email. The information on it is needed for getting technical support or product replacement.

By using the UID or the key, the license certificate (XML file) is created on the Broadcom Licensing Portal, as shown in Figure 2-3.

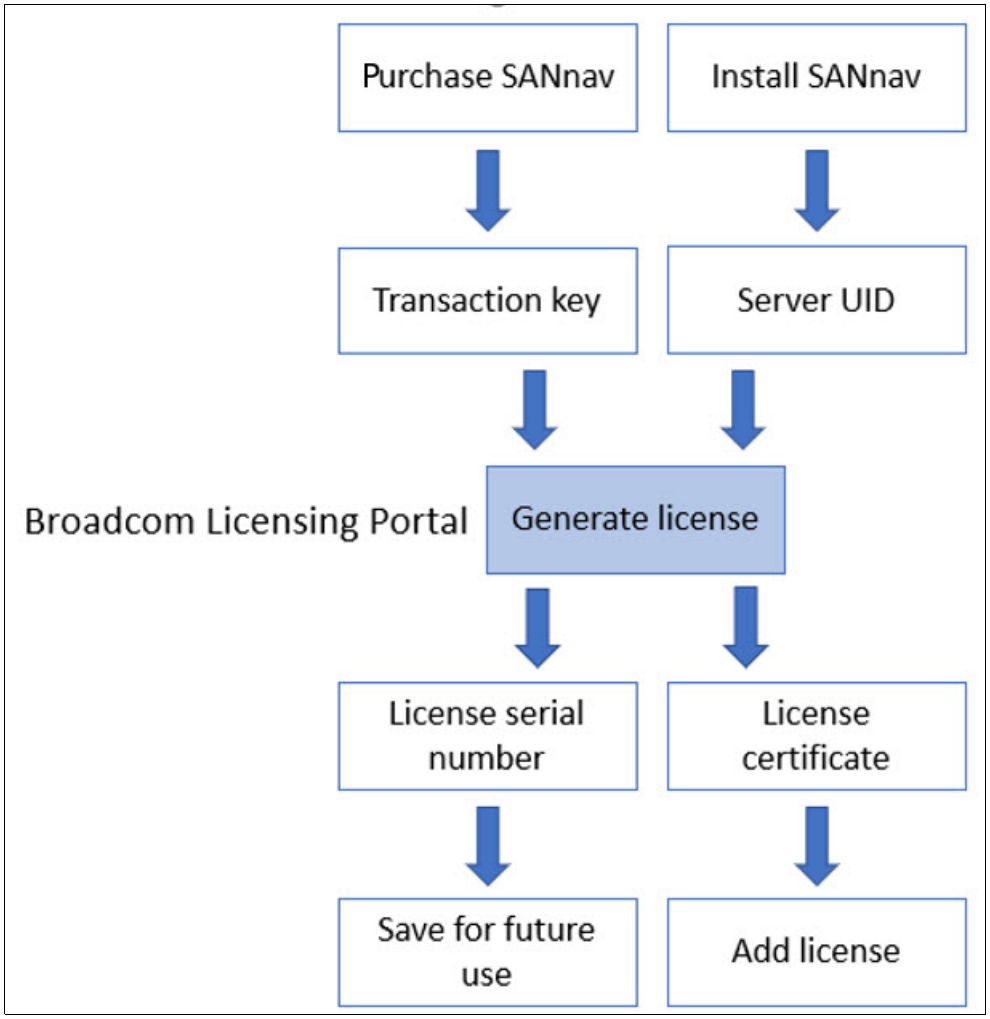


Figure 2-3 SANnav licensing flow

Note: The license serial number that is generated is required if you contact IBM Support. It also can be retrieved from the licensing window in SANnav. You will need the license key also for the support calls.

For more information about this process, see Generating a License.

For every SANnav instance, an individual license must be obtained. Cloning virtual machines (VMs) with SANnav installed is *not possible*.

2.1.4 Migrating to a different host

If you want to move a license from one host to another host (for example, moving to a different server), a process that is called *rehosting* is available. For this process, first the license must be released, and then a rehost key is generated. With this rehost key and the new server UID, you can create a license.

Note: The rehosting process allows the previous instance to continue running for 30 days to ensure that the new instance is working.

If an unplanned move is necessary (for example, permanent hardware failure of the SANnav server), you must contact support and provide them with the server UID of the new SANnav host and the license serial number that was created when initially creating the license certificate for the failed server.

For more information about rehosting, see 4.3.4, “Rehosting a license on a different server: Planned migration” on page 85) or Rehosting a License on a Different Server: Planned Migration.

2.1.5 Downloading the software

The SANnav software can be downloaded from IBM Fix Central by completing the following steps:

1. Go to IBM Fix Central.
2. Search for "SANnav" and select the version that you want to download, as shown in Figure 2-4.

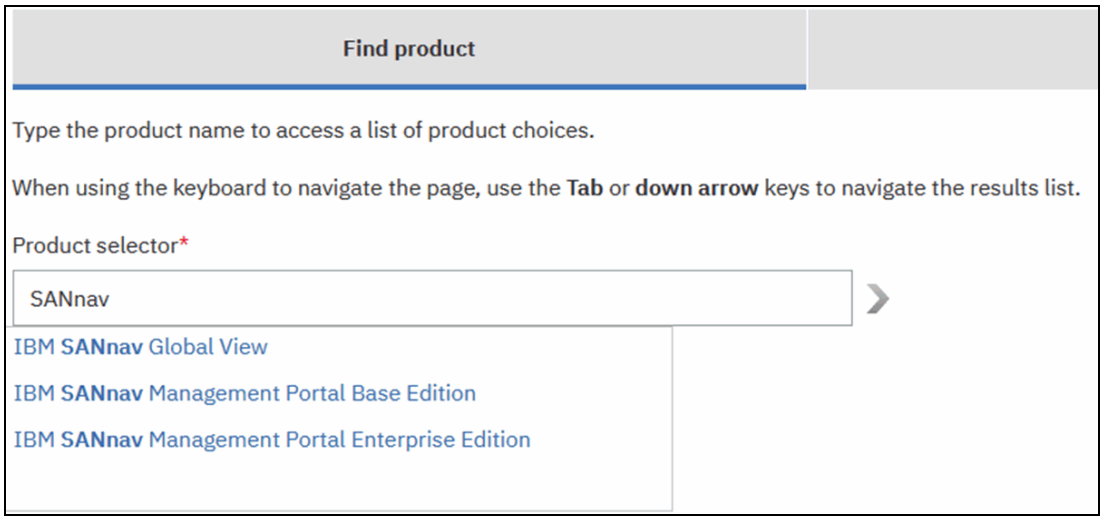


Figure 2-4 Product selection on Fix Central

3. Select the installed version (for an update) or **All** for a new installation, as shown in Figure 2-5.

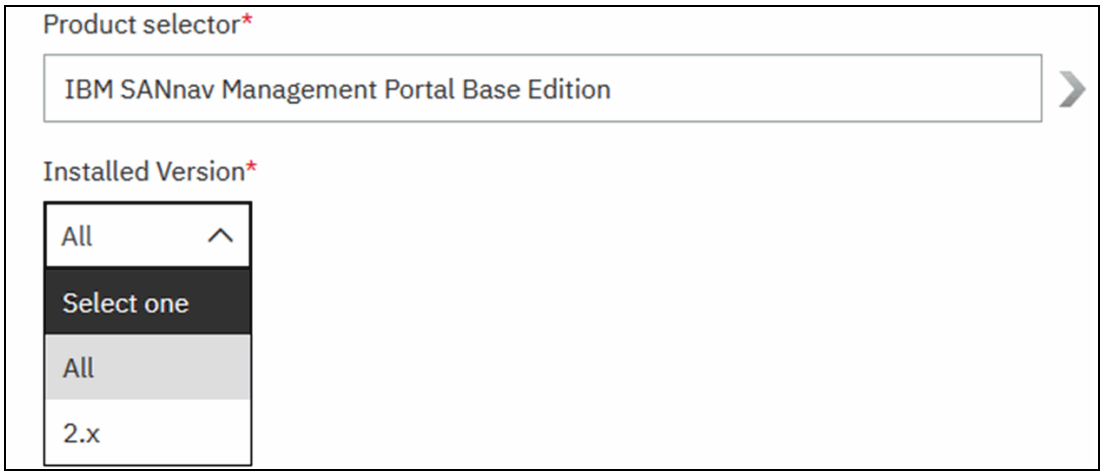


Figure 2-5 Version selection on Fix Central

4. Click **Continue**.
5. Under Select fixes, choose the **SAN Storage Networking b type** fix pack, as shown in Figure 2-6.

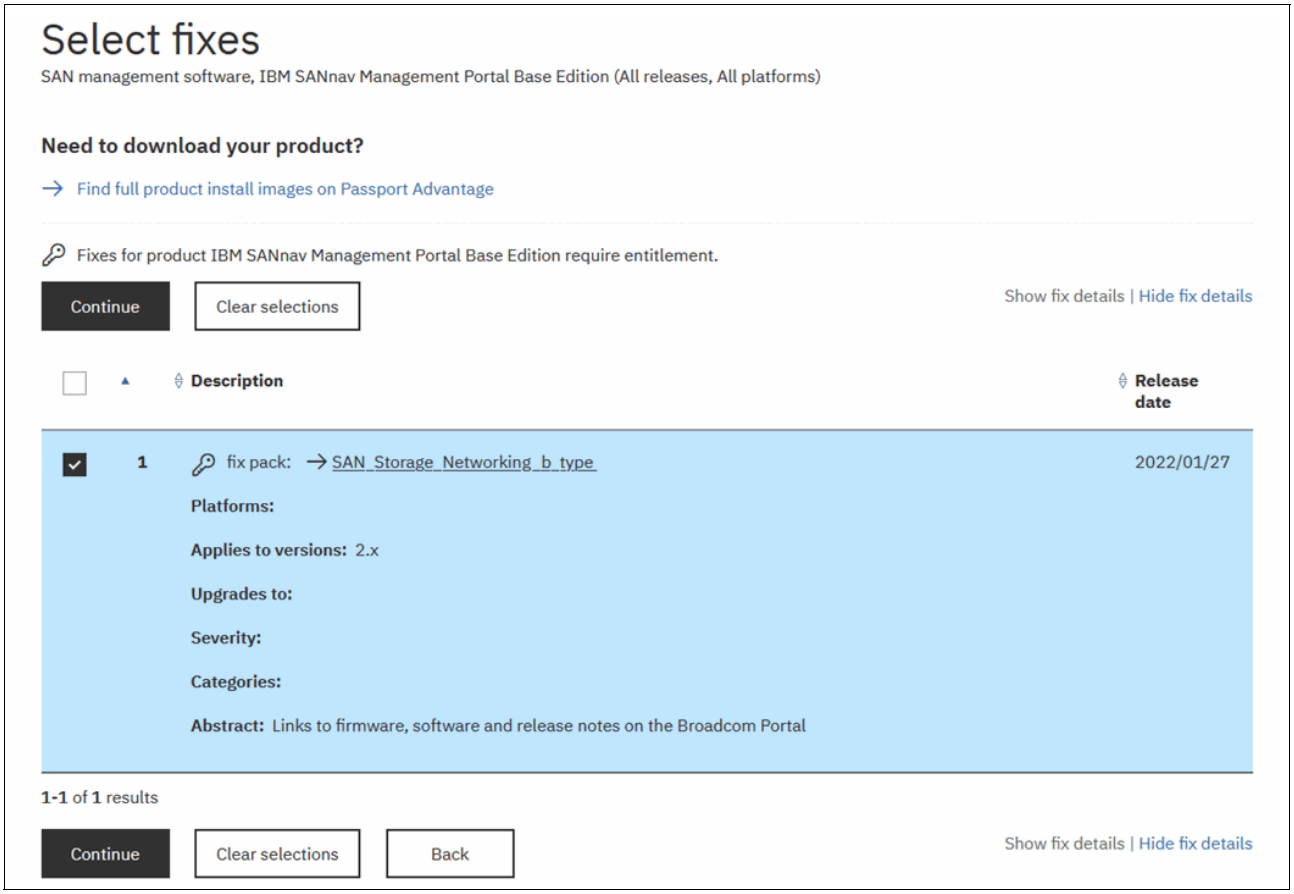


Figure 2-6 Selecting a fix pack on Fix Central

6. Click **Continue**.

7. To pass the entitlement check, enter the machine type and the serial number, as shown in Figure 2-7. (For more information, see 2.1.2, “SANnav machine types” on page 14.)

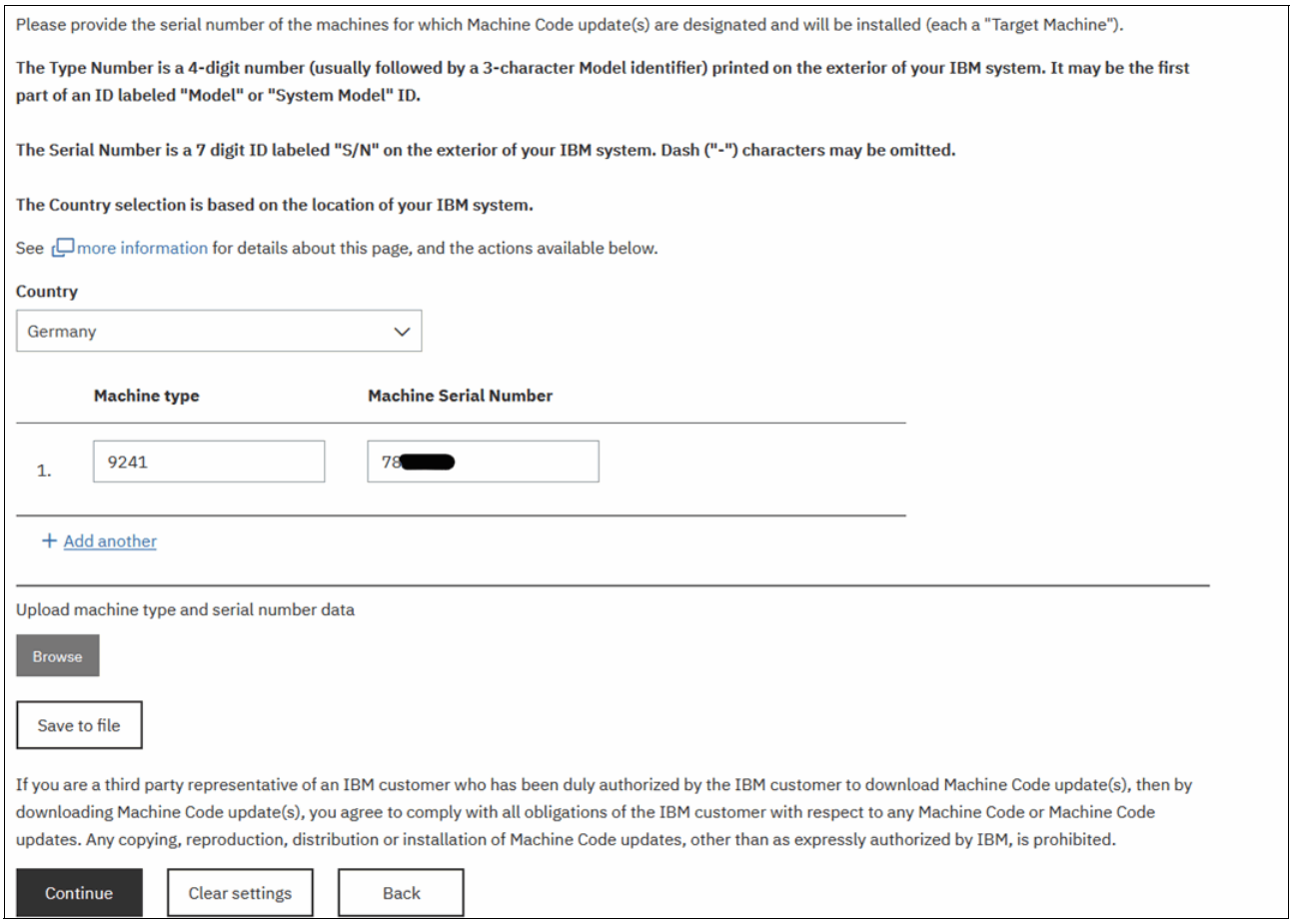


Figure 2-7 Entitlement check on Fix Central

8. Click **Continue**.

   Figure 2-8 shows a customized link to the Broadcom software portal.

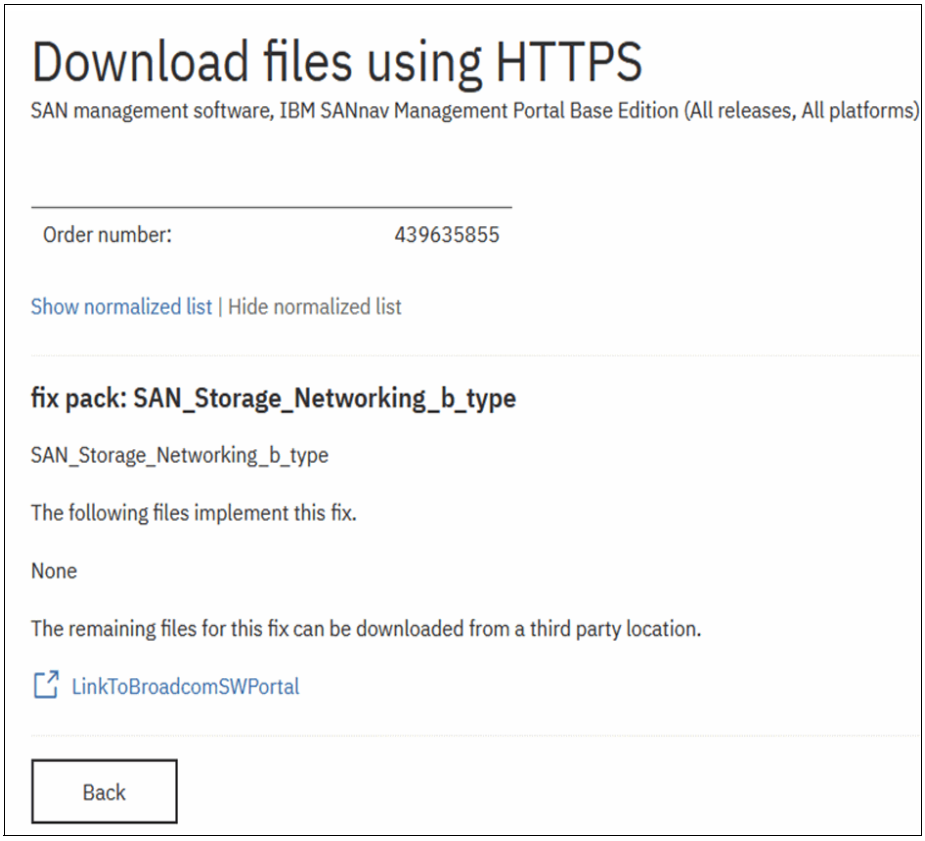


Figure 2-8 Link to Broadcom Software Portal

9. Click the link to go to the Broadcom Software Portal. Click **Continue** on the window that informs you that you are leaving the IBM website.
10. On the Broadcom Assist Portal window, enter your email address and complete the captcha, as shown in Figure 2-9.

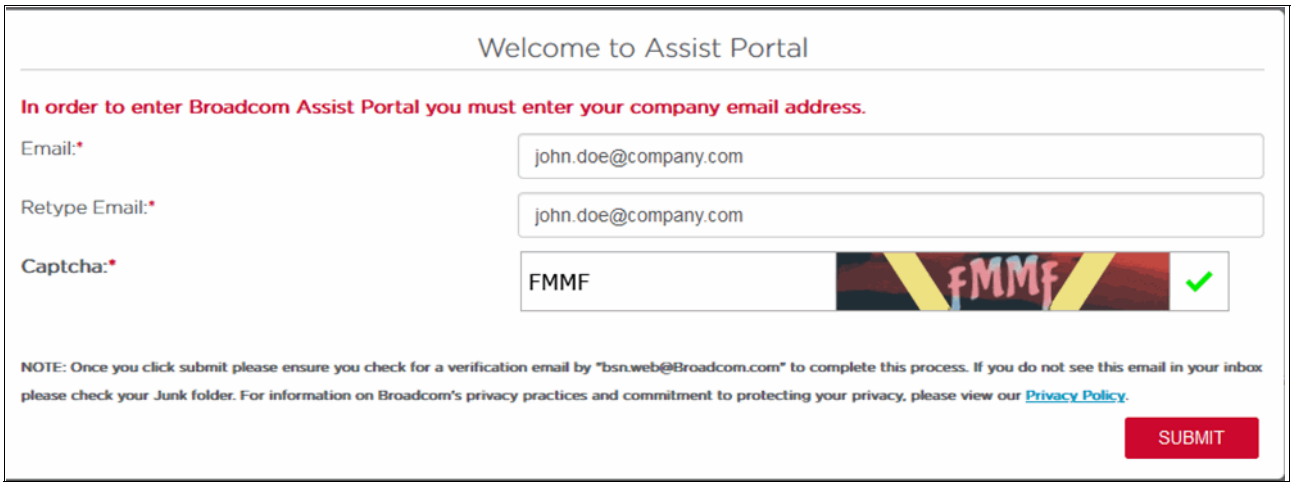


Figure 2-9 Broadcom Assist Portal window

11. Click **Submit**.
12. A verification code is sent to your email address, as shown in Figure 2-10.

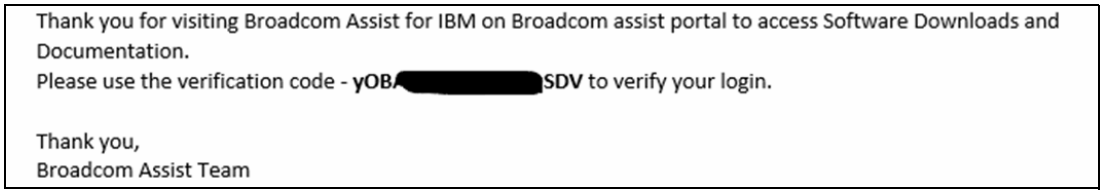


Figure 2-10 Broadcom verification code email

13. Enter the verification code and complete the captcha on the Broadcom Assist Portal, as shown in Figure 2-11.

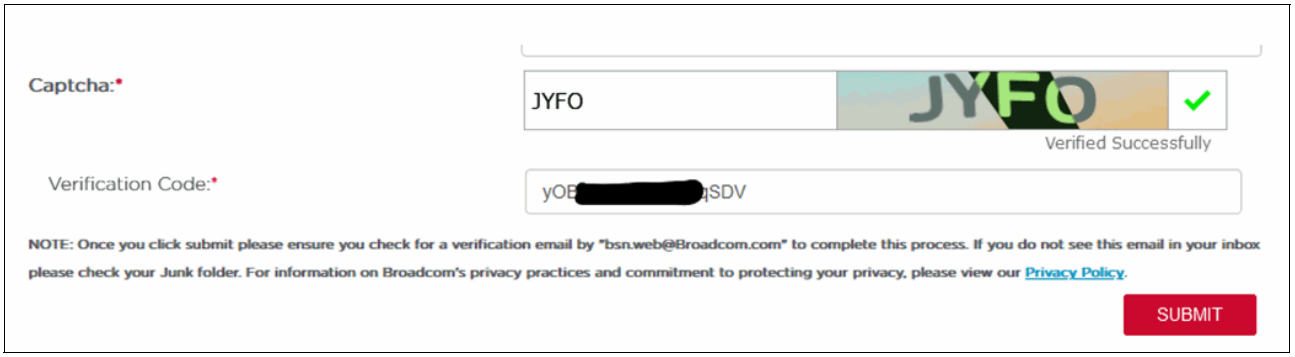


Figure 2-11 Entering Broadcom verification code and captcha

14. On the next window, select the files that you want to download, as shown in Figure 2-12.

> **Note:** You do not need to enter a serial number because the entitlement verification was done on IBM Fix Central.

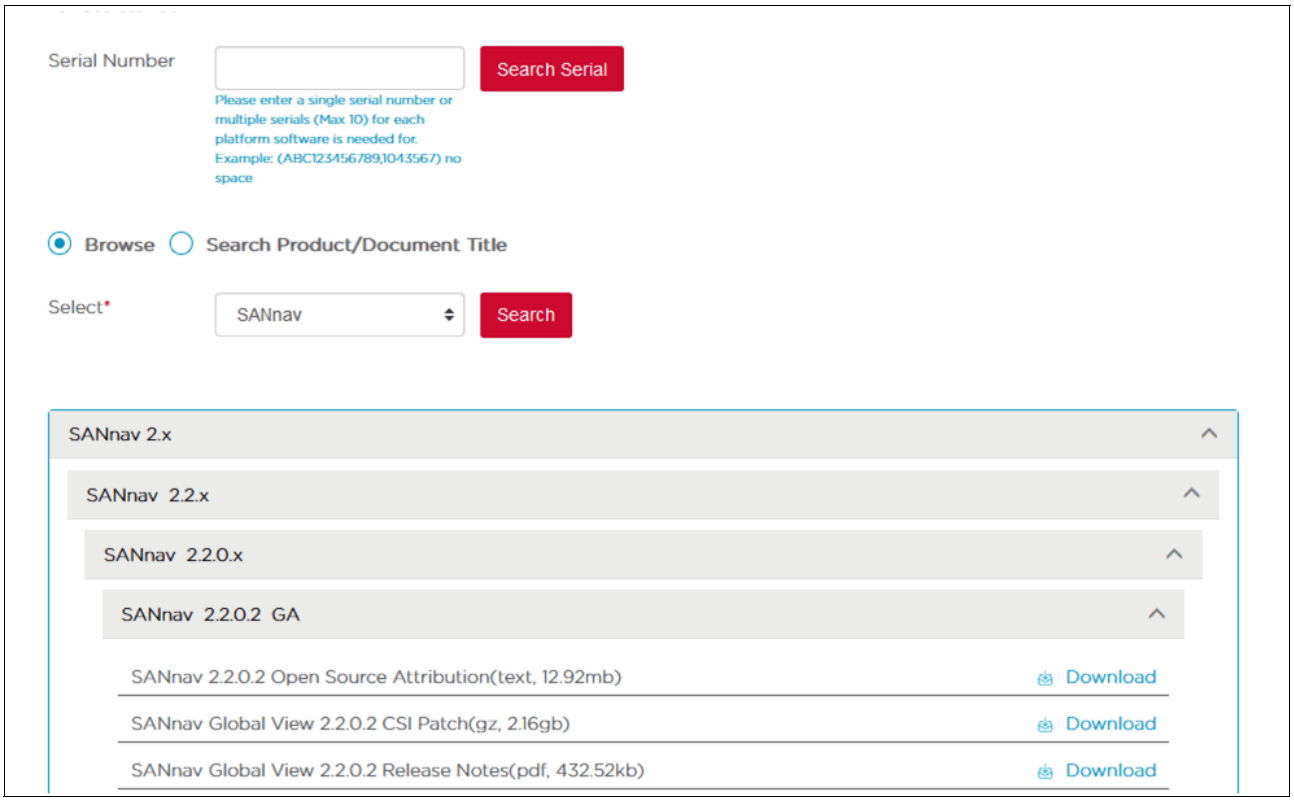


Figure 2-12 Selecting files to download

15. Read and accept the end-user license agreement (EULA) and click **I accept**, as shown in Figure 2-13 on page 23.

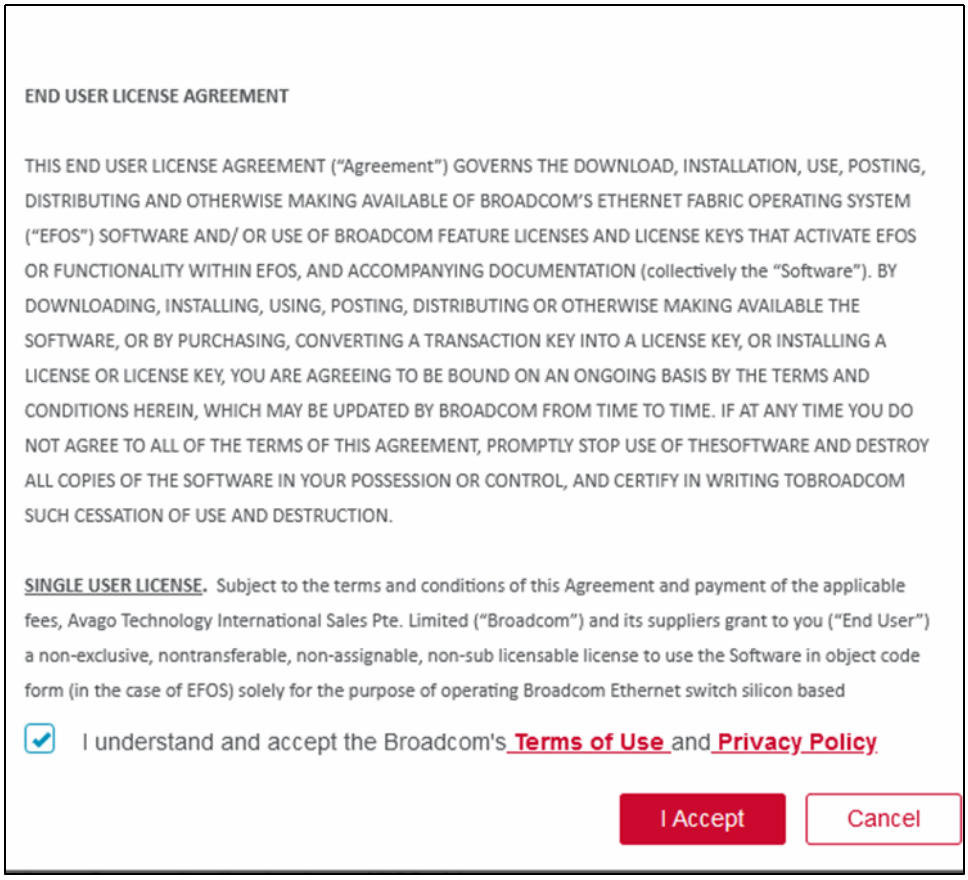


Figure 2-13 End-user license agreement

16. Download your files and save them for the installation.

3

Installing and deploying IBM SANnav Management Portal

This chapter describes how to install IBM SANnav Management Portal v2.2.x in your SAN environment. It provides the necessary adaptations for the different operating systems and installation platforms. This chapter also describes the requirements and settings that are necessary to adapt SANnav to your SAN and network environment.

This chapter includes the following topics:

- Options for platform and operating system installation
- Installation requirements
- Linux operating system installation and preparation
- SANnav installation process
- SANnav deployment as an Open Virtual Appliance
- Firewall configuration and used ports
- SANnav Management Console and scripts
- SANnav and operating system upgrade
- Removing SANnav from the server

3.1 Options for platform and operating system installation

The following options are available for the installation:

- Installing on a bare-metal server (x86_64 architecture) with Red Hat Enterprise Linux (RHEL) or Community Enterprise Operating System (CentOS).
- Installing as a virtual machine (VM) that is based on VMware and Microsoft HyperV. No hypervisor other than VMware ESXi and Microsoft HyperV is supported.
- Deploying an Open Virtual Appliance (OVA) that is based on VMware. The SANnav appliance uses CentOS 7.9 and is supported only by a VMware infrastructure.

The supported operating systems and host types are shown in Table 3-1.

Table 3-1 Host type and operating system requirements

Product/edition	Maximum switch ports/instances under management	Operating system	Host type
SANnav Management Portal Base Edition (Manages switches only, not directors.)	600 ports	RHEL 7.9, 8.4, 8.5, and 8.6 CentOS 7.9 only	Bare-metal/ESXi ESXi/HyperV VM OVA (CentOS 7.9)
SANnav Management Portal Enterprise Edition (Required to manage directors.)	Up to 3000 ports	RHEL 7.9, 8.4, 8.5, and 8.6 CentOS 7.9 only	Bare-metal/ESXi ESXi/HyperV VM OVA (CentOS 7.9)
	3000 - 15,000 ports	RHEL 7.9, 8.4, 8.5, and 8.6 CentOS 7.9 only	Bare-metal/ESXi ESXi/HyperV VM OVA (CentOS 7.9)
SANnav Global View	3000 - 15,000 ports	RHEL 7.9, 8.4, 8.5, and 8.6 CentOS 7.9 only	Bare-metal/ESXi ESXi/HyperV VM

Note: CentOS and Red Hat announced that support for CentOS Linux 8, as a rebuild of RHEL 8, ended December 2021. CentOS 7.9 continues to be supported until end of service in on 15 June, 2024. The SANnav virtual appliance is based on CentOS 7.9.

3.2 Installation requirements

Depending on the size of the SAN environment to be managed and the license type, an appropriate host must be used or a VM must be prepared.

The installation requirements in Table 3-2 are valid for bare-metal and VM installations.

Table 3-2 Installation requirements

Installation requirement	**Up to 3,000 SAN ports License type: Base or Enterprise**	**Up to 15,000 ports License type: Enterprise**
Platform	x86/64-bit architecture	
Operating system	Red Hat Enterprise Linux (RHEL) 7.9, 8.4, 8.5, or 8.6 CentOS 7.9	
CPU cores	16	24
CPU sockets	2	2
Memory	48 GB	96 GB
Available space (minimum)	600 GB	1.2 TB

Note: At the time of writing, only the operating systems that are mentioned in Table 3-2 on page 27 were released. For more information about updates and changes, see *SANnav Management Portal v2.2.0 Release Notes (Digest Edition)*.

The required storage space depends on the number of SAN ports that you want to manage, as shown in Table 3-3, which refers to the space that is required for SANnav (some additional space is needed for the operating system itself). Depending on the type of installation and whether you use a GUI, you might need an extra 25 - 50 GB.

Table 3-3 Disk space requirements

Requirement	**Up to 3000 SAN ports License type: Base or Enterprise**	**Up to 15000 ports License type Enterprise**
SANnav installation directory `<sannav_home>` (available space)	450 GB	1050 GB
Docker Installation directory `<docker_home>` (available space)	120 GB	120 GB

Note: Before starting the installation procedure, you must copy the installation package to the SANnav installation directory, which reduces the amount of space that is available in the installation directory. Therefore, you must have more space (about 15 GB) than the space that is available.

3.2.1 Installation requirements for a bare-metal server

The SANnav Management Portal should run on a server that is intended only for this purpose. No other applications, even if they belong to the SANnav Management Suite, may be installed. SANnav uses Docker as a containerization platform and various Ethernet ports, and network address translation, for communication between the individual components. As a best practice, do not install unnecessary software to ensure that the SANnav server functions properly.

3.2.2 Installation requirements for a virtual environment

SANnav v2.2.1 supports VMware 7.0 and Microsoft HyperV 2019. You can create a VM and install one of the supported operating systems (RHEL or CentOS) that are listed in Table 3-2 on page 27. Create a VM that meets at least the minimum requirements for the number of CPUs or sockets, memory, and disk space.

Figure 3-1 shows an example of a possible configuration for up to 3,000 SAN ports. Adjust the configuration according to your requirements. You can use several virtual drives and add network connections.

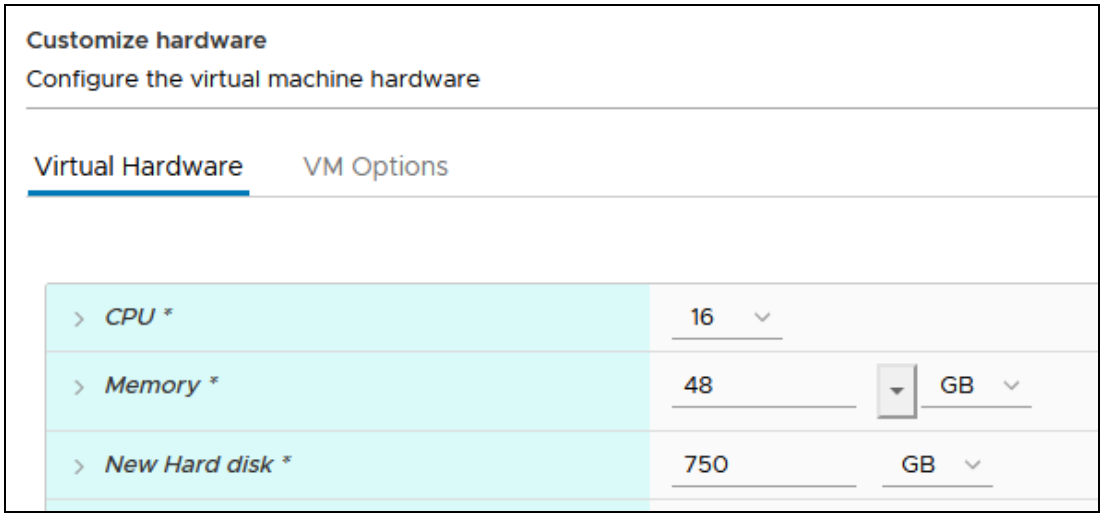


Figure 3-1 Customizing hardware

If you use a virtual environment, as a best practice, reserve the virtual memory to exclusively allocate the required amount of physical memory on the ESXi hypervisor. Edit the settings of the VM as shown in Figure 3-2 on page 29 and select **Reserve all guest memory**.

Do not install hypervisor virtualization tools, such as VMware software tools and Microsoft Hyper V tools that are used, to shut down the server. The SANnav server installation and management requirements are more complex than for a conventional, standard server. The usage of external tools for managing the VM is not supported and can impair the function of the SANnav server. Use the tools and scripts that are provided by the SANnav installation to manage the SANnav VM for tasks such as starting, stopping, updating, upgrading, backing up, restoring, and other similar management tasks. For more information, see the scripts and explanations in 3.7, “SANnav Management Console and scripts” on page 57.

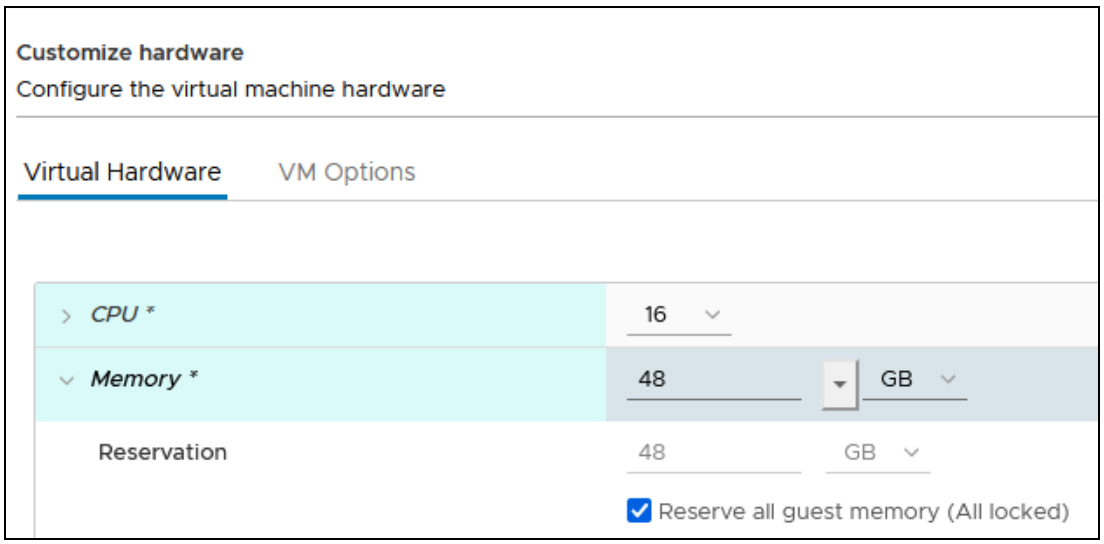


Figure 3-2 Permanent memory reservation for the virtual machine

3.3 Linux operating system installation and preparation

For a successful SANnav installation, you must follow certain guidelines and settings, which are explained in the following sections.

If you create Linux installations in your company or organization by using automated processes or if you clone existing virtual servers, you must adapt them to the requirements for the SANnav installation and add virtual disks or partitions if necessary.

3.3.1 Linux installation steps

This section describes the basic procedures of the Linux installation. Essentially, the steps for preparing a hardware server or a VM are the same. Provide a system that meets the requirements and install a supported operating system. If you are not familiar with Linux installation, see the information pages of the distribution publishers Red Hat or CentOS for a detailed description.

Your company or organization might have guidelines for the installation of Linux systems that you should follow. If they are not included in these specifications, separate the operating system and applications and create one or more dedicated partitions for the installation of the SANnav software.

After you start the installation by inserting a DVD or connecting to an image in your virtual environment, follow the Linux installation menu (Figure 3-3) and observe the following points.

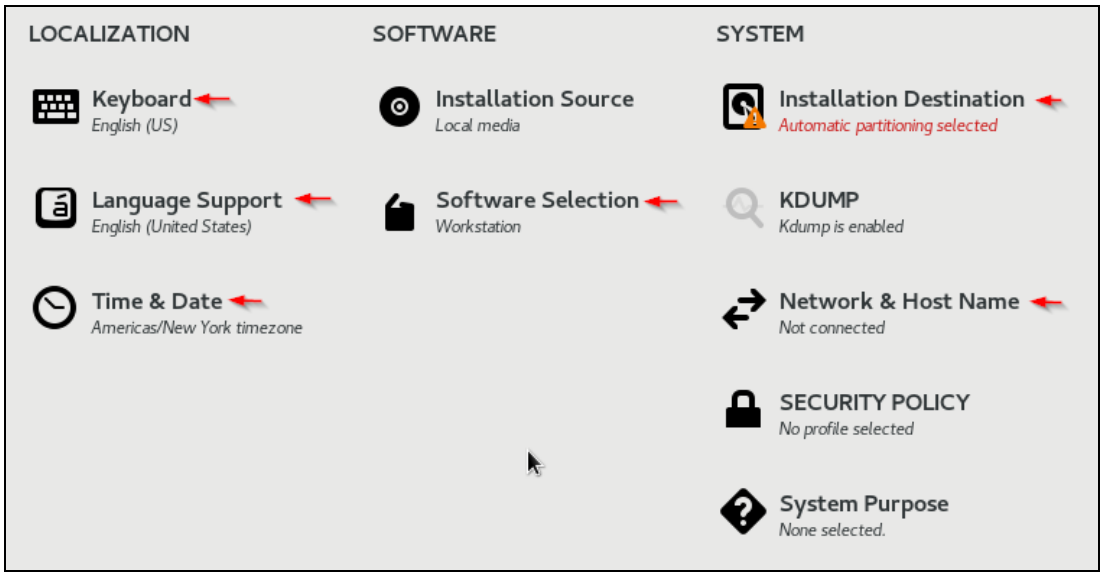


Figure 3-3 Linux RHEL or CentOS installation main window

- The language support must be English, and the locale must be US (`Language=English, Locale=US`). Other settings can lead to problems in the installation process.
- The SANnav installation script uses many commonly available Linux commands. If any of the commands that are used in the script are not available on the SANnav server, the SANnav installation fails. The Red Hat and CentOS minimal installation might not have all the required packages, so you might need to add the missing packages manually. If you want to avoid installing individual packages and modules, build Red Hat as “Server” or “Server with GUI”, which reduces the number of extra packages that is required to a minimum and simplifies the installation. For **Software Selection**, use Server Type `Server`.
- For Installation Destination, *do not use automatic partitioning, but instead use customized partitioning*. Select I**nstallation Destination** → **Storage Configuration Custom** → **DONE** → **Manual partitioning**. When you get the message “You haven’t created any mount points for Linux”, select **Click here to create them automatically**. Adjust the partitions and mount points according to your needs and create one or more partitions for the SANnav installation.
- As explained in 3.4, “SANnav installation process” on page 36, Docker uses an installation directory (optionally a partition) for the SANnav software and a directory for the Docker containerization platform. The directory names can be chosen arbitrarily, but must not contain any spaces. The default directory for Docker is `/var/lib/docker`, but can be changed during the installation. When installing SANnav, the partition where the Docker installation directory is created must have at least the available space that is specified in Table 3-3 on page 27.
- The SANNav installation directory (`<sannav_home>`) can be created manually in an existing partition or you can create a dedicated partition during the Linux installation. Also, for the SANnav installation directory, the associated partition must at least meet the specifications in Table 3-3 on page 27, plus more storage capacity (about 20 GB) for the installation file.
- The image in Figure 3-4 on page 31 shows an example of a SANnav installation for up to 3000 ports by using a 500 GB partition for the `<sannav_home>` directory and a 130 GB `/var/lib` partition for the Docker installations directory `<home_docker>`.

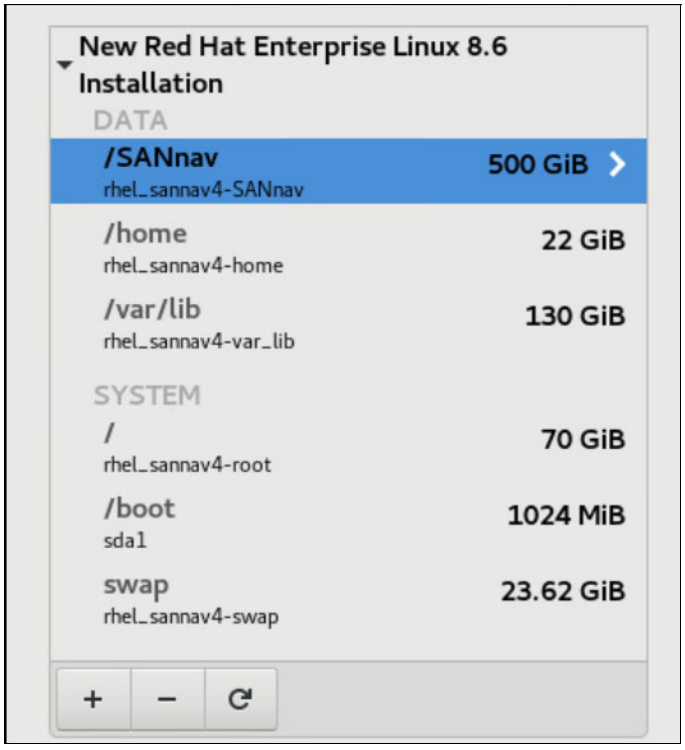


Figure 3-4 Linux partitions

- Finally, make the appropriate settings for the time, date, and network settings before starting the installation.

3.3.2 Prerequisite steps before starting the SANnav installation

In the following section, we look at the software packages and services that SANnav relies on and that must be installed before you install the SANnav software.

If you selected the installation type `Server` during the installation of CentOS or RHEL, most of the packages already are installed, but there are several packages and settings that must be configured manually.

Table 3-4 shows the software packages that are required for the installation. You can use the **`yum`** command to get a list of all installed packages:

```
yum list installed
```

Table 3-4 Commands and packages that are needed for installation

Command or service	RHEL or CentOS package
`lsof`	List open files: `lsof.x86_64`
`nslookup / bind-utils`	Name server lookup: `bind-utils.x86_64`
`rngd-service`	Random number generator: `rng-tools.x86_64`
`chrony / ntp`	Network Time Protocol (NTP): `chrony.x86_64`

Command or service	RHEL or CentOS package
iptables	IP address filter packet rules: iptables.x86_64
zip/unzip	File compression: unzip.x86_64

lsof and nslookup

Ensure that the **lsof** and **nslookup** packages are installed on CentOS and RHEL. If one of the packages is not installed, run the following commands to install them.

```
yum install lsof
yum install bind-utils
```

Random number generator: rngd service

rngd stand for the random number generator daemon. The server must have **rngd** installed and activated because SANnav relies on secure random numbers. You can use the **systemctl status rngd.service** command to check whether **rngd** is installed and running. If it is not installed, install the rng-tools package or start the service by running the following commands:

```
yum install rng-tools
systemctl start rngd.service
systemctl enable rngd.service
```

Synchronizing the server time with Network Time Protocol

For flow management, synchronize your clocks by using NTP for all switches and the SANnav server. SANnav uses the time synchronization of the underlying operating system. RHEL 8 use **chrony**, and CentOS 7.9 can use **ntpd** or **chronyd**. Check that the settings for time synchronization are correct or change them if necessary.

Setting the correct time zone

If the time zone is set to “n/a”, the SANnav database installation fails.

Check the current time zone of the server by running the following command:

```
timedatectl
```

If necessary, look up and set the correct server time zone by using the following commands:

```
timedatectl list-timezones
timedatectl set-timezone <time zone>
```

Installing a decompression tool on CentOS 7.9

Installing patches requires the usage of compression and decompression utilities. In RHEL8, the unzip package is part of the “standard” installation package, but on CentOS 7.9, it might need to be installed manually.

If you use the SANnav virtual appliance or if you do not have the CentOS installation media, you can download the packages from CentOS repositories.

Download or copy the following packages to a directory on the server:

```
unzip-6.0-21.el7.x86_64.rpm
zip-3.0-11.el7.x86_64.rpm
```

Use rpm to install the packages by running the following commands:

```
rpm -ivh unzip-6.0-21.el7.x86_64.rpm
rpm -ivh zip-3.0-11.el7.x86_64.rpm
```

Hostname resolution and IP address configuration

Set up a proper configuration for the server hostname (fully qualified domain name (FQDN)) on your local Domain Name Server (DNS) server. Check that forward and reverse lookup is working properly.

- Ensure that the **`hostname -i`** command resolves to a valid IP address.
- Ensure that the **`nslookup`** command is successful and resolves the hostname and IP address of the physical server or VM:

  `nslookup <hostname.domain>, nslookup <ip-address>`

- The **`ipcalc`** command is used to validate the server IP address. You can use the **`ipcalc <server-ip-address>`** command. If the **`ipcalc`** command cannot be found, install the `ipcalc` package by running the following command:

  `yum install ipcalc`

- To verify that the value for MTU size is at least 1500, use the **`ifconfig`** command.

Uninstalling Docker if it is installed

The SANnav software architecture is based on Docker container technology. With this technology, SANnav can easily adapt to the needs of small, medium, and large SAN environments, especially when they grow over time.

With the SANnav installation, a dedicated Docker environment is installed on the server and only this installation can be used. If you installed Docker during the Linux setup or if you use an existing Linux server that already has Docker installed, you must remove Docker before starting the installation.

By default, Docker uses an IP address range of 192.168.255.240/28 (192.168.255.240 - 192.168.255.255). If this IP range overlaps with a range in your network, it can be changed during installation.

Disabling Security Enhanced Linux

SANnav Management Portal v2.2.1 is *not* supported on Security Enhanced Linux (SELinux) in Enforcing or Permissive mode on either CentOS or RHEL (all versions). The only SELinux mode that is supported is `Disabled`. The installation script stops and exits if the SELinux mode is enabled. It does not matter whether the mode is set to “Enforcing” or “Permissive”. Activating SELinux after successful SANnav installation might prevent SANnav from working correctly, so this mode is not supported.

To check the current SELinux status, use the **`getenforce`** command:

```
# getenforce
Disabled
```

If the SELinux mode is not `Disabled`, then change the `SELINUX` value to `SELINUX=disabled` in the `/etc/selinux/config` file. To activate the new mode, restart Linux.

Iptables

Docker requires **iptables** to create Network Address Translation (NAT) rules for the Docker internal network. Without the **iptables** package, the Docker service cannot start and the installation fails.

You can check whether **iptables** is installed by running the following **yum** command:

```
yum list installed | grep -i iptables
```

Iptables and **iptables-services** are two different services. When **iptables-services** is enabled, it works like a firewall, where the default rule blocks all ports. If **iptables-services** is installed and running, you must manually open the required ports for clients and switches on the server.

SANnav does not need **iptables-services**, so as a best practice, disable and stop **iptables-services** to avoid any issues with mis-configured rules.

Configuring the firewalld back end in RHEL 8

In Linux, *firewalld* is the controller for **nftables** and **iptables**, and it is used to implement persistent network traffic rules. RHEL and CentOS have firewalld installed by default. You can check the status of the firewall with the command **firewall-cmd --state** or **systemctl status firewalld**. When the firewall is active (running) and you want to use it, you must adjust the back-end mode.

In RHEL 8.4, 8.6, and later, the default settings for firewalld use **nftables** instead of **iptables**. Docker does not support **nftables**, so you must change the settings for firewalld to **iptables**. (CentOS 7.9 uses **iptables** by default, so no changes are necessary.)

To change the settings for **iptables** in RHEL 8, complete the following steps:

1. Get the active zone details by running the following command:

   ```
   firewall-cmd --list-all
   ```

   Look up the zone name of the active zone, for example, `public (active)`.

2. Disable the masquerade option by running the following command:

   ```
   firewall-cmd --zone=<ActiveZoneName> --remove-masquerade --permanent
   ```

   Use the zone that is listed as `active` from the command in step 1 for the `<Active ZoneName>`.

3. Stop the firewalld (firewall daemon) by running the following command:

   ```
   systemctl stop firewalld
   ```

4. Edit the firewalld configuration file `/etc/firewalld/firewalld.conf`.

   Open the file with an editor (for example, vi) by running the following command:

   ```
   vi /etc/firewalld/firewalld.conf
   ```

   Search for the `FirewallBackend` setting. Change the setting from `FirewallBackend=nftables` to `FirewallBackend=iptables`.

   Figure 3-5 on page 35 shows this section in the file `firewalld.conf`.

```
# FirewallBackend
# Selects the firewall backend implementation.
# Choices are:
#       - nftables (default)
#       - iptables (iptables, ip6tables, ebtables and ipset)
FirewallBackend=iptables
```

Figure 3-5 FirewallBackend settings

5. Start firewalld by running the following command:

   ```
   systemctl start firewalld
   ```

6. Reload firewalld to activate the changed settings by running the following command:

   ```
   firewall-cmd --reload
   ```

Customizing the Linux Secure Shell port if SAN Fabric OS is earlier than Version 8.2.2

By default, port 22 is used for Secure Shell (SSH) communication on Linux and CentOS for Linux host management access.

SANnav has a built-in SSH server that is used for the internal firmware repository and Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP) services. By default, port 22 is used for the internal SSH, but SANnav allows you to customize the internal SSH server port during installation.

If you use SAN switches in your environment that are running Fabric OS (FOS) versions that are earlier than Version 8.2.2, then port 22 must be used for the access to SANnav; otherwise, an external FTP, SCP, or SFTP server is needed (providing the service on port 22) for switch supportsave and firmware download functions.

To eliminate the overlap with the Linux SSH service and use port 22, adjust the Linux SSH configuration. The following example shows how to use port 6022 (You can use any other available port instead of port 22).

1. Edit the `sshd_config` file as follows:

   ```
   vi /etc/ssh/sshd_config
   ```

   a. Locate the following line:

      ```
      #Port 22
      ```

   b. Uncomment the line and change the port number to another, unused port, such as 6022:

      ```
      Port 6022
      ```

   Whatever port that you select must be available and allowed through the firewall. A best practice is to use the **`netstat`** command to check whether the port is in use:

   ```
   netstat -plnt
   ```

2. Restart the SSHD by running the following command:

   ```
   systemctl restart sshd
   ```

   The current SSH session remains logged in, but any new sessions must now use the new port. In this example, the port is `6022`.

3. Add the new port to the firewalld configuration if the internal firewall is in use by running the following commands:

```
firewall-cmd --zone=public --add-port=6022/tcp --permanent
firewall-cmd --reload
firewall-cmd --list-all
```

3.3.3 SANnav installation file

To install SANnav Management Portal on the server, complete the actions in the following subsections.

Creating the SANnav directory

If you did not create a separate partition for the SANnav installation during the Linux installation, create a directory in the partition of your choice. The name of the directory must not contain any spaces or the installation fails.

Downloading and transferring the software to the server or virtual machine

Download the SANNav Management Portal software as described in 2.1.5, “Downloading the software” on page 17. Transfer the `.tar` file that contains the installer and software (for example, `Portal_<version>-distribution.tar.gz`) to the correct directory (`<sannav_home>`).

Before unpacking `Portal_<version>-distribution.tar.gz`, make sure that the file permissions for the unpacked files are set correctly. Make sure that the **`umask`** setting for the root user is `0022`, which corresponds to the Linux standard. Use the command **`umask`** to check the current setting. If the current **`umask`** is not `0022`, change it.

```
umask 0022
```

Extract `Portal_<version>-distribution.tar.gz` to extract the file to the current directory by running the following command:

```
tar -xvzf Portal_<version>-distribution.tar.gz
```

It might take a few minutes until the file is unpacked to a directory with a name like `Portal_<version>_bldxx`. This directory is referred to as `<install_home>` in 3.4, “SANnav installation process” on page 36.

3.4 SANnav installation process

The SANnav application installation is script-based. You must run the scripts **`install-sannav.sh`** that is provided in the `bin` folder of your `<install_home>` directory, for example:

```
/SANnav-home/Portal_2.2.0_bld374/bin
```

All the scripts for the SANnav installation must be run in the bash shell.

Run the installation script from the `bin` directory as follows:

```
./install-sannav.sh
```

When the script starts, it runs some preinstallation checks to check whether the requirements for disk space, CPU, memory, and IP address and hostname resolution are met. If any test fails, the installation exits with an error message. If there is an error, you must eliminate the reported issues before you can make another installation attempt. If the installation fails after the preinstallation check, during the software installation or SANnav server start, you must uninstall the SANnav application, restart the server, and run the installation script again.

The entire installation process, with the necessary parameters, settings, and notes, is shown in Table 3-5. Some of installation parameters cannot be changed after installation. If you need to change one or more of these parameters after installation finishes, you must uninstall and then reinstall the SANnav software.

Table 3-5 Installation tasks

Step	Installation task	Changeable after installation?
1.	BROCADE COMMUNICATIONS SYSTEMS LLC END USER SOFTWARE LICENSE AGREEMENT FOR Brocade SANnav Management Portal and IBM SANnav Global View IMPORTANT: READ THIS CAREFULLY BEFORE INSTALLING, USING OR ELECTRONICALLY ACCESSING THIS PROPRIETARY PRODUCT! ... Do you agree with these terms and conditions? (Yes / No): [No]	N/A
2.	In order to install SANnav Management Portal services, the address <server-ip-address> will be used. Is this the correct and valid IP address? (Y / y / N / n): [Y/y]	N
3.	SANnav Management Portal needs to use an IP address range for its container services. The default range pool is set to "192.168.255.240/28" (that is, 192.168.255.240 to 192.168.255.255). NOTE: Now is the only time you can change this default HTTPS port. It CANNOT be modified after you proceed with the default setting. You will need to uninstall and reinstall SANnav in order to change it later. Does this IP address range need to be modified? (Y / y / N / n):	N
4.	The default home directory for installing SANnav Management Portal services is: /var/lib/docker. NOTE: A minimum of 120 GB disk space is required. NOTE: Now is the only time you can change this default HTTPS port. It CANNOT be modified after you proceed with the default setting. You will need to uninstall and reinstall SANnav in order to change it later. Does this default location (/var/lib/docker) need to be modified? (Y / y / N / n):	N
5.	Installing SANnav Management Portal platform. This may take a few minutes. Successfully installed SANnav Management Portal platform. Press Enter to proceed with server installation.	N/A

Step	Installation task	Changeable after installation?
6.	Configure automatic redirection of SANnav Management Portal clients from HTTP to HTTPS: 0 For automatic redirection of SANnav Management Portal clients from HTTP to HTTPS. 1 For no automatic redirection of SANnav Management Portal client from HTTP to HTTPS.	Y
7.	To configure HTTP or HTTPS connections between SANnav Management Portal and SAN switches, select one of the following options: 0 For HTTP 1 For HTTPS (SAN switches must be configured for HTTPS connection) 2 For HTTPS first then HTTP (if HTTPS fails)	Y
8.	To configure the method by which SANnav Management Portal launches WebTools, select one of the following options: 0 To always require login when launching WebTools 1 To launch Web Tools with Single Sign On (SSO) using the managed SAN switch credentials 2 To launch Web Tools with SSO using the SANnav Management Portal user's credentials	Y
9.	Select the preferred IP address for client to SANnav Management Portal server communication, or press Enter to proceed with option (Any). 0 : Any 1 : <server-ip-address>	Y
10. 10.	To run the SANnav SSH server on port 22, press Enter to proceed or enter another port number (1- 65535). Note: If port other than 22 is selected, you cannot use the internal SSH server for downloading firmware to switches and chassis that are running a firmware version lower than 8.2.2	Y
11.	The default HTTPS port number for SANnav Management Portal is: 443. NOTE: Now is the only time you can change this default HTTPS port. It CANNOT be modified after you proceed with the default setting. You will need to uninstall and reinstall SANnav in order to change it later. Does this default HTTPS port (443) need to be modified? (Y / y / N / n):	N
12.	The default SNMP Traps port number for SANnav Management Portal is: 162. NOTE: Now is the only time you can change this default SNMP Traps port. It CANNOT be modified after you proceed with the default setting. You will need to uninstall and reinstall SANnav in order to change it later. Does this default SNMP Traps port (162) need to be modified? (Y / y / N / n):	N

Step	Installation task	Changeable after installation?
13.	The default Syslog port number for SANnav Management Portal is: 514. NOTE: Now is the only time you can change this default Syslog port. It CANNOT be modified after you proceed with the default setting. You will need to uninstall and reinstall SANnav in order to change it later. NOTE: If Syslog port is customized, SANnav Management Portal will not receive syslog messages from switches running FOS version less than v8.2.2d. Does this default Syslog port (514) need to be modified? (Y / y / N / n):	N
14.	The default Secure Syslog port number for SANnav Management Portal is: 6514. NOTE: Now is the only time you can change this default Secure Syslog port. It CANNOT be modified after you proceed with the default setting. You will need to uninstall and reinstall SANnav in order to change it later. NOTE: If Secure Syslog port is customized, SANnav Management Portal will not receive secure syslog messages from switches running FOS version less than v8.2.2d. Does this default Secure Syslog port (6514) need to be modified? (Y / y / N / n):	N
15.	Enter database password: Password must be between 8 to 64 alphanumeric characters. Spaces are not allowed. Allowed special characters are ! # $ * ()	Y
16.	Enter SFTP/SCP password: Password must be between 8 to 64 alphanumeric characters. Spaces are not allowed. Allowed special characters are ! # $ * ( )	Y
17.	Enter the SANnav Management Portal security password. This password will be used to protect private keys, keystores and truststores used by different services: Note: In order to change the SANnav Management Portal security password after installation you will need to uninstall and reinstall SANnav Management Portal. Password must be between 8 to 64 alphanumeric characters. Spaces are not allowed. Allowed special characters are ! # $ * ( ).	N
18.	Enable SANnav Management Portal license automatic renewal? (Note that Internet connectivity for the SANnav Management Portal server is required for this feature to work.) (Y / y / N / n): [Y/y]	Y
19.	In order to improve the user experience of SANnav product features in the future, SANnav server will collect usage data. Allow this data to be sent to Broadcom? (Y / y / N / n): [Y/y]	N/A

Step	Installation task	Changeable after installation?
20.	Loading SANnav Management Portal services from File System. This might take a few minutes. SANnav Management Portal services loaded successfully. Created symlink /etc/systemd/system/multi-user.target.wants/sannaviptablesetup.service · /usr/lib/systemd/system/sannaviptablesetup.service. SANnav Management Portal server has been installed successfully. SANnav Management Portal server startup may take up to 15 minutes. To check SANnav Management Portal server status, run **/<install_home>/Portal_2.2.0_bld374/bin/check-sannav-status.sh.** When startup has completed, launch the client using [https://<server-ip-address>].	N/A

To change the settings for after the installation process, use the scripts that are provided with SANnav. For more information about the SANnav Management Console, see 3.7, “SANnav Management Console and scripts” on page 57.

3.5 SANnav deployment as an Open Virtual Appliance

The IBM SANnav management platform can be deployed as a virtual appliance in a VMware environment where other hypervisors are not supported.

The installation is done in two steps:

- Preparing and deploying the Open Virtual Appliance (OVA)
- Installing SANnav

Note: The terms Open Virtualization Format (OVF) and Open Virtual Appliance (OVA) are used synonymously by VMware. An OVF package is composed of metadata and files that describe a VM, plus some additional information that is needed to deploy and operate the applications in the OVF package. An Open Virtual Appliance (OVA) is an OVF package in a single compressed file archive.

3.5.1 SANnav OVA requirements

For the SANnav OVA deployment, consider the following items:

- The only supported hypervisor is VMware ESXi.
- The ESXi version must be at least Version 7.0.
- The deployment can be done only from a VMware vCenter Server (Version 7.0 or later). Direct OVA deployment without VMware vCenter is not supported.

- OVA deployment supports Base and Enterprise licenses for small configurations with fewer than 3000 ports and large configurations with up to 15,000 ports. The requirements of the OVA in terms of number of CPU memory size and hard disk drive (HDD) space are shown in Table 3-6.
- The OVA is based on CentOS 7.9. (Language and locale are US English, and may not be changed.)
- You need administrative rights to deploy the SANnav OVA in the VMware environment.

During installation, you can select a small or large configuration. The small configuration for Base and Enterprise licenses needs 48 GB of memory and support up to 3000 ports. The large configuration needs 96 GB of memory to support an Enterprise license with up to 15,000 ports.

Table 3-6 shows the SANnav virtual appliance requirements.

Table 3-6 SANnav virtual appliance requirements

VMware requirements	**Small configuration Base and Enterprise license with up to 3,000 ports**	**Large configuration Enterprise license with up to 15,000 ports**
VMware environment	► VMware ESXi 7.0 host ► vCenter Server 7.0	► VMware ESXi 7.0 host ► vCenter Server 7.0
CPU cores	16	24
CPU sockets	2	2
Memory (RAM)	48 GB	96 GB
Drive space that is needed	630 GB	1.3 TB

Note: The SANnav virtual appliance comes with a predefined file system and disk partitions. Two partitions are created during installation: One for the operating system and swap, and another one for the SANnav installation and Docker.

3.5.2 Installing the SANnav virtual appliance

To install the SANnav Management Portal appliance by using vCenter, complete the following steps:

1. Download the SANnav OVA package from IBM Fix Central, as described in 2.1.5, “Downloading the software” on page 17.
2. Log on to the vCenter manager (vSphere client) and select the cluster in where you want to deploy the OVA. From the **Actions** menu, select **Deploy OVF Template**, as shown in Figure 3-6.

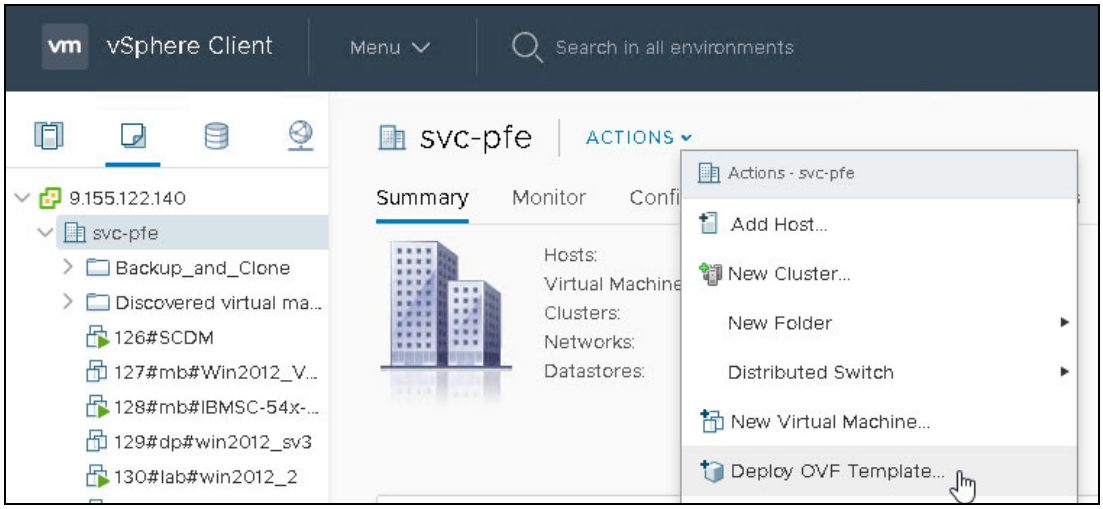


Figure 3-6 Deploy OVF Template menu

3. Select an OVF template. The deployment OVF Template user interface guides you through the installation steps, starting with **Select an OVF template**, as shown in Figure 3-7. After you select **Local file**, go to the download folder and select the OVA file, as shown in Figure 3-8 on page 43 for Management Portal v2.2.0.

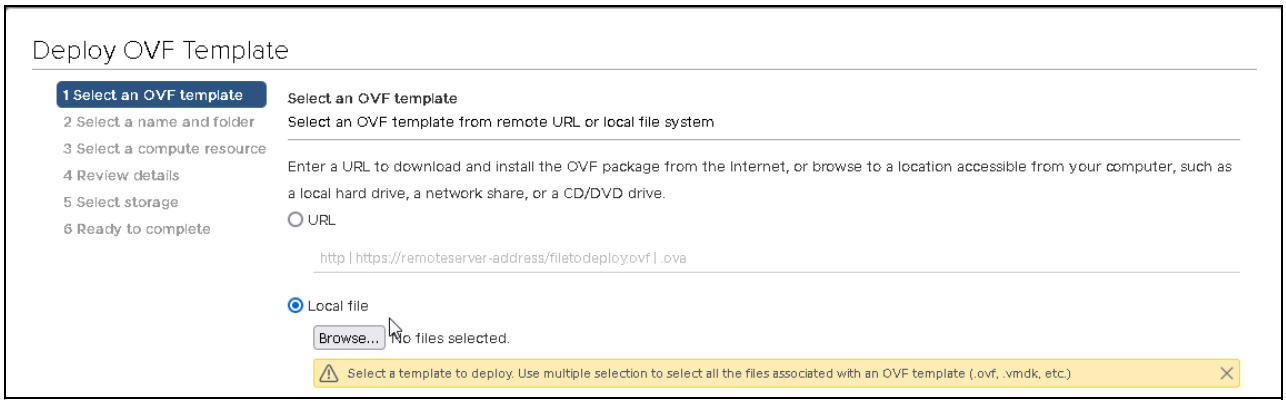


Figure 3-7 Select an OVF Template menu

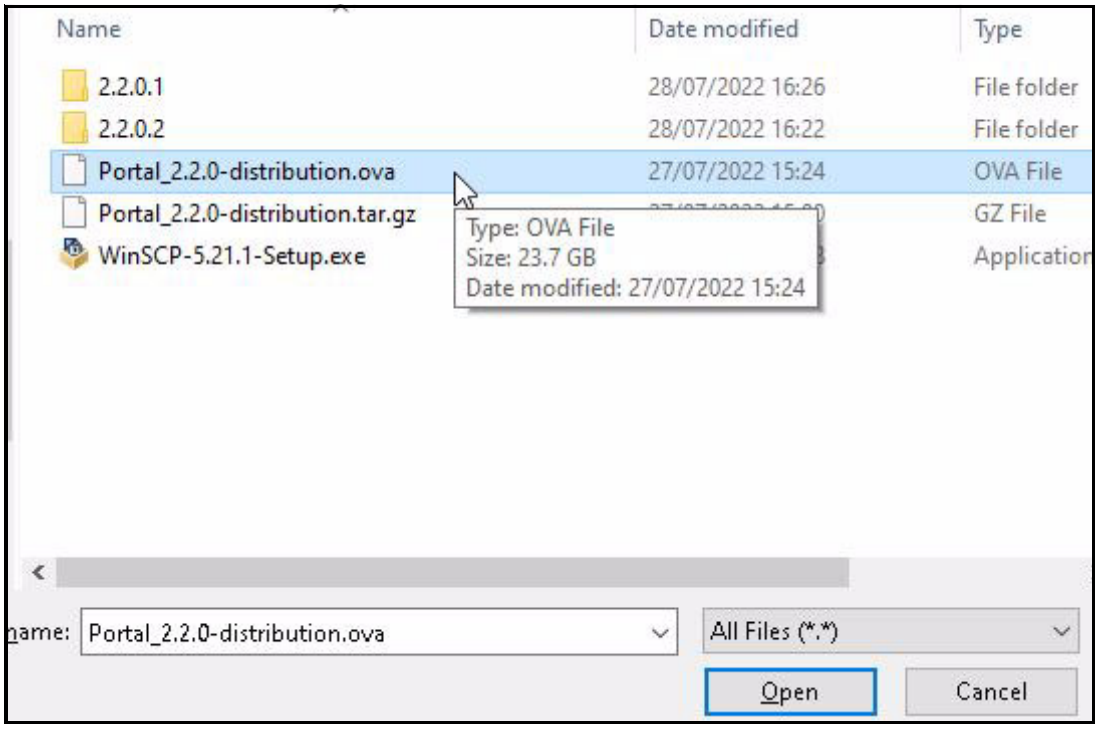


Figure 3-8 Selecting the Portal-Distribution.ova file*

Check that the correct local file is selected and click **Open** to continue.

4. Select a name and folder. In this step, you must select a name and folder from the vCenter server for the managed cluster (data center) in which you want to deploy the virtual appliance. An example is shown in Figure 3-9.

   The name that you select here is the name of the VM in your environment. The name can be changed after the installation.

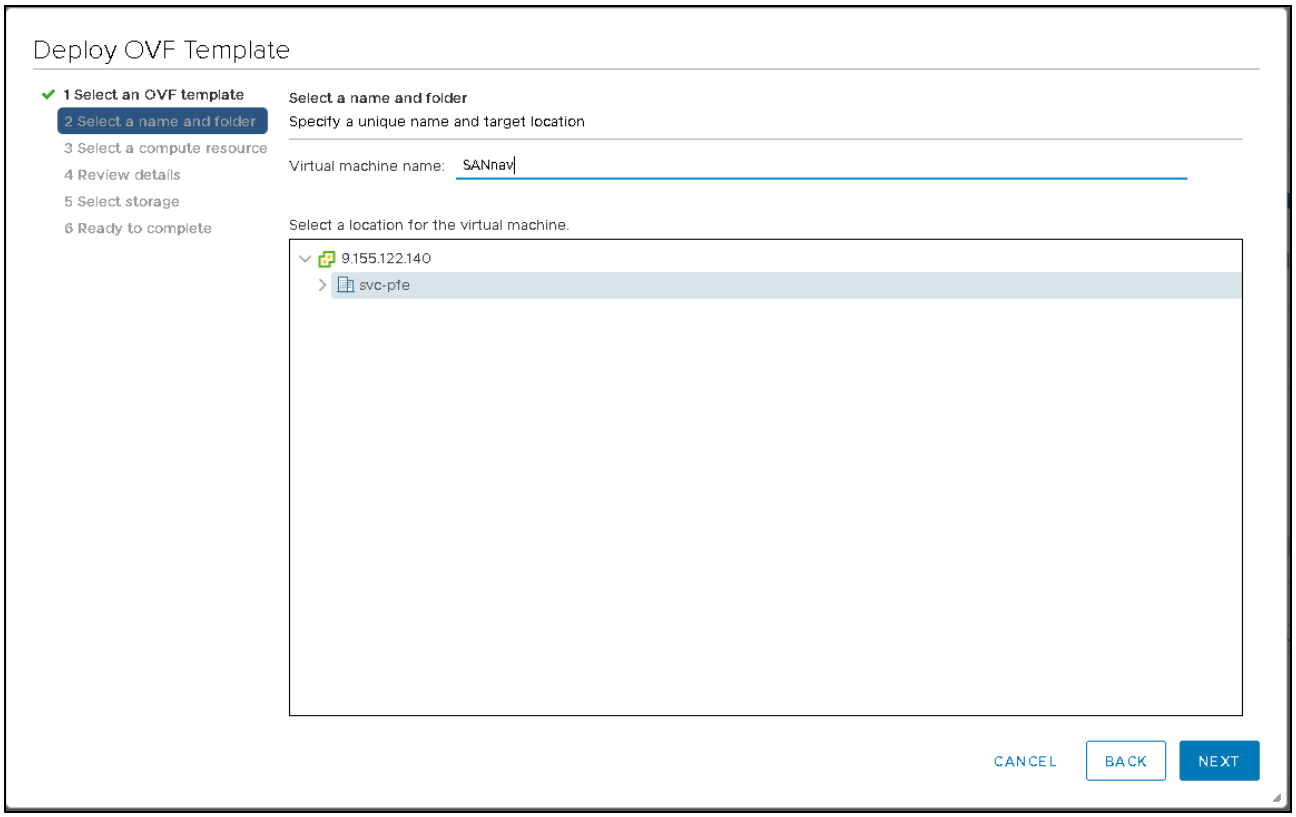


Figure 3-9 Selecting a name and folder

5. Select a compute resource (in this case, an ESXi host) for the installation. Ensure that the VMware ESXi host meets the system and server requirements for SANnav, and click **NEXT**.
6. Review the details of the OVA installation source, and click **NEXT**.

7. For the license agreements, select the **I accept all license agreements** checkbox and click **NEXT**, as shown in Figure 3-10.

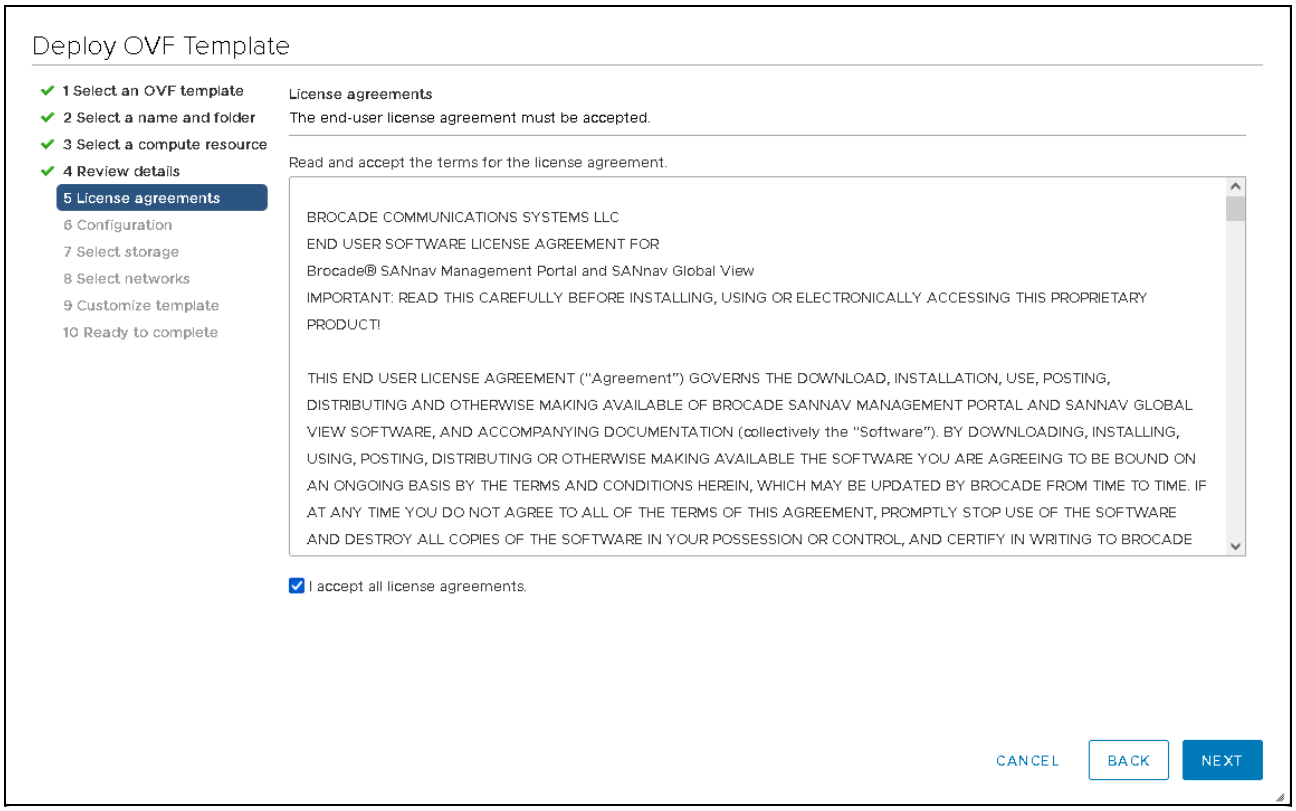


Figure 3-10 Accepting the license agreement

8. The small configuration needs 48 GB of memory, which supports the Base license (up to 600 ports) and the Enterprise license (up to 3,000 ports). The large configuration needs 96 GB of memory to support an Enterprise license and up to 15,000 ports. Select the appropriate configuration for your environment, as shown in Figure 3-11.

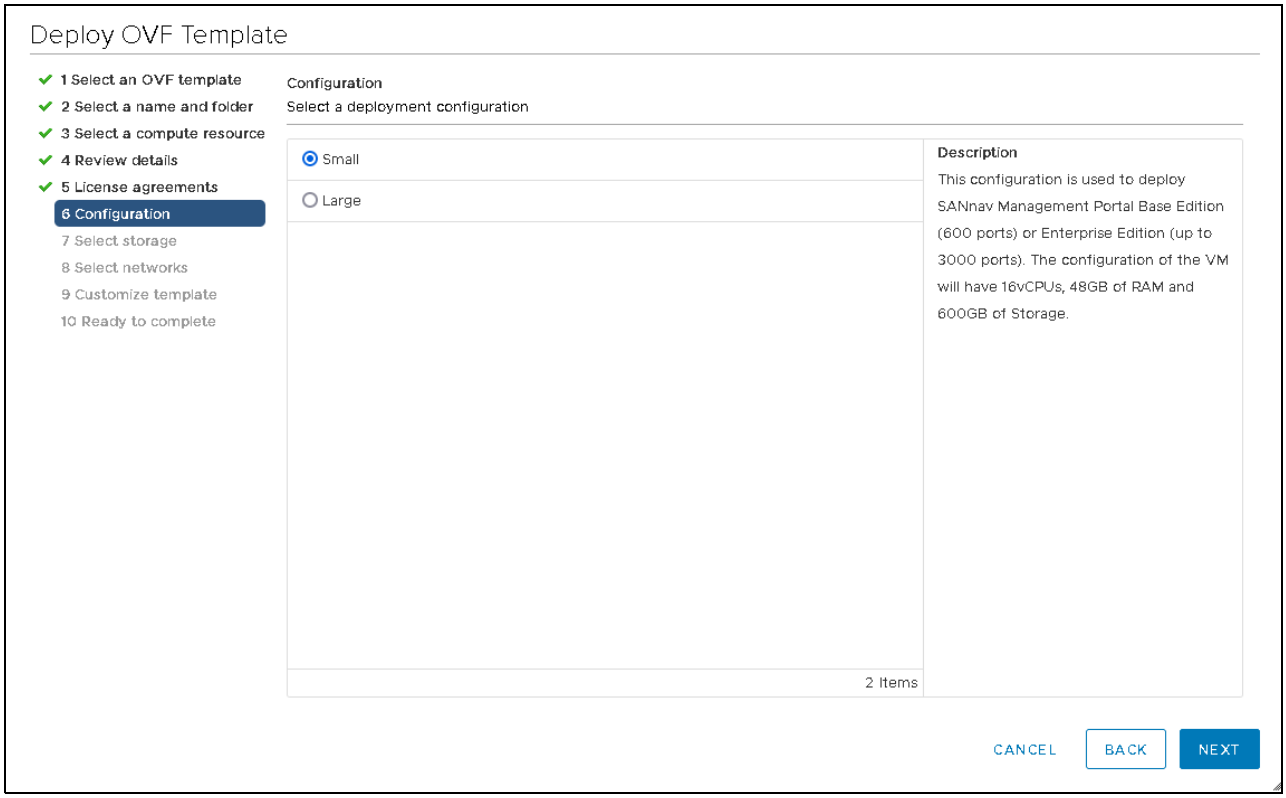


Figure 3-11 Configuration selection

9. Select the storage by selecting the virtual disk format and the data store in which you want to allocate storage space for the VMDK of the virtual appliance. The required data store depends on configuration, small or large, that was selected in step 8 on page 46. Figure 3-12 shows an example.

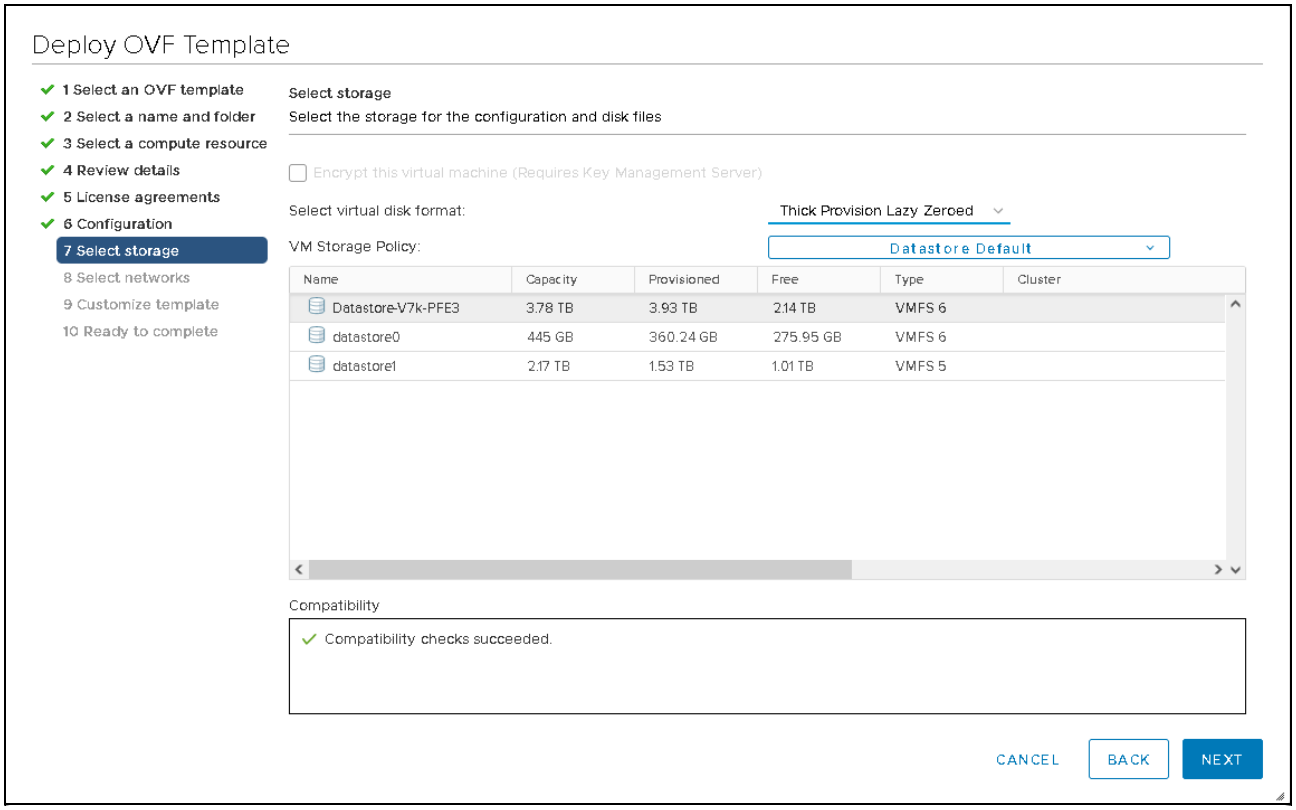


Figure 3-12 Selecting storage

In the next steps, you can adapt the OVA installation to your environment:

1. In **Select networks**, you can choose the IP protocol (IPv4 or IPv6) and virtual network that you want to attach the virtual server. For IP allocation, choose either **Static-Manual** or **DHCP**. For IP protocol, choose either **IPv4** or **IPv6**.

   Figure 3-13 shows an example for a static IPv4 address. Make the appropriate settings and click **NEXT**.

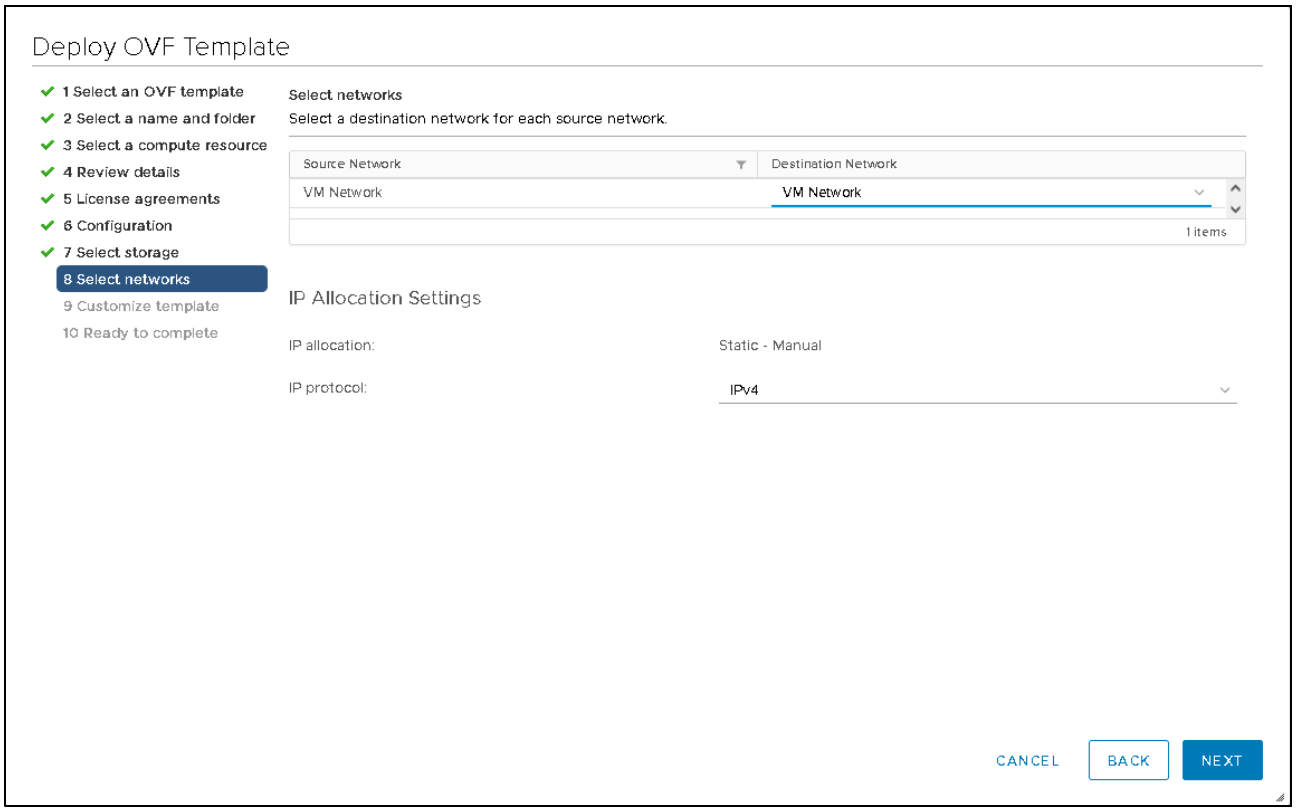


Figure 3-13 Selecting networks

2. You can customize the settings for the virtual appliance that are related to your environment. Change the hostname, network settings, DNS, and SSH port of the SANnav server, as shown in Figure 3-14 and Figure 3-15 on page 50:

   – Hostname.

     The default hostname is set to something similar to `sannav-portal-v220`. If you want to change this name, you can enter a new name or the FQDN. This hostname and FQDN must be resolved by your DNS, or the SANnav installation will fail. An example is shown in Figure 3-14.

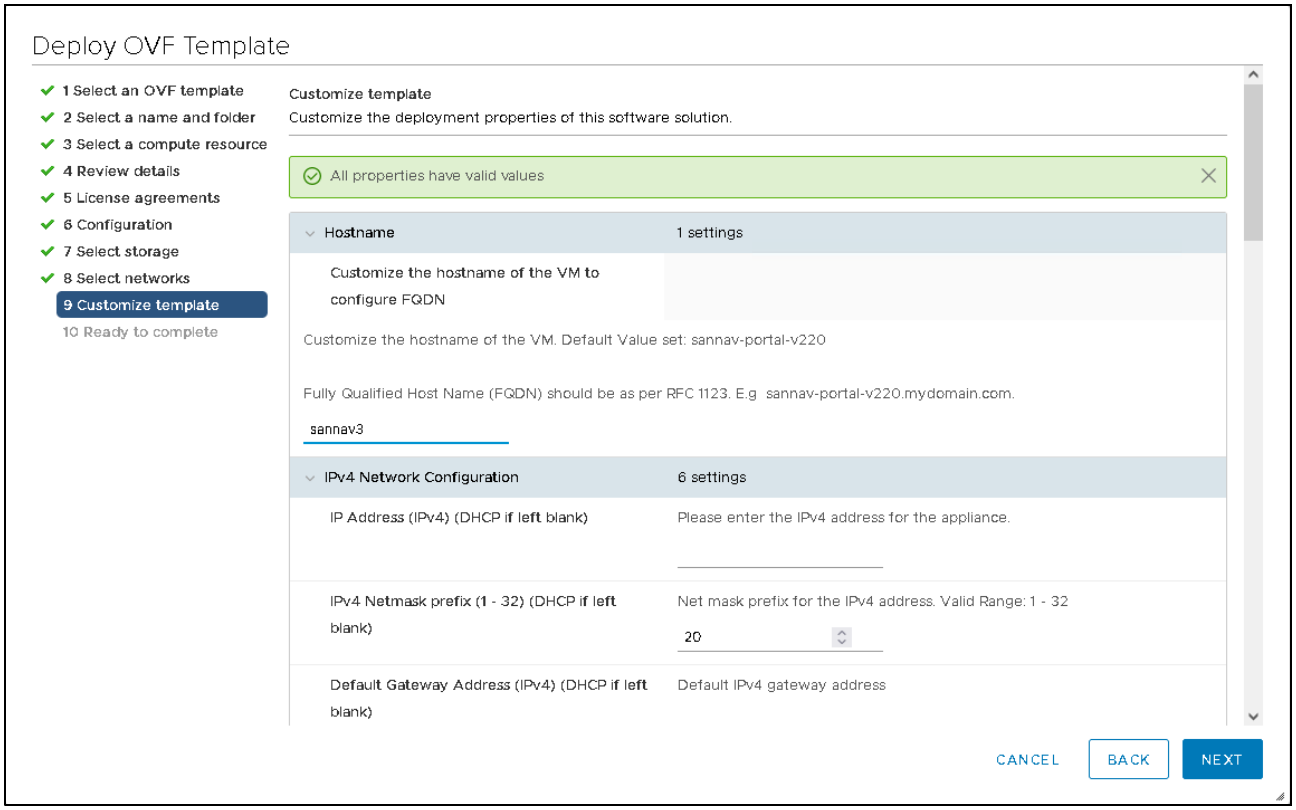


Figure 3-14 Customizing the template hostname and IPv4

– IP address for IPv4 (IPv6), netmask, and gateway.

Enter the IP address for IPv4 (or IPv6) that you want to use. If you use DHCP in your environment, leave this section blank. Set the netmask and default gateway for the virtual server according to your network environment, as shown in Figure 3-15.

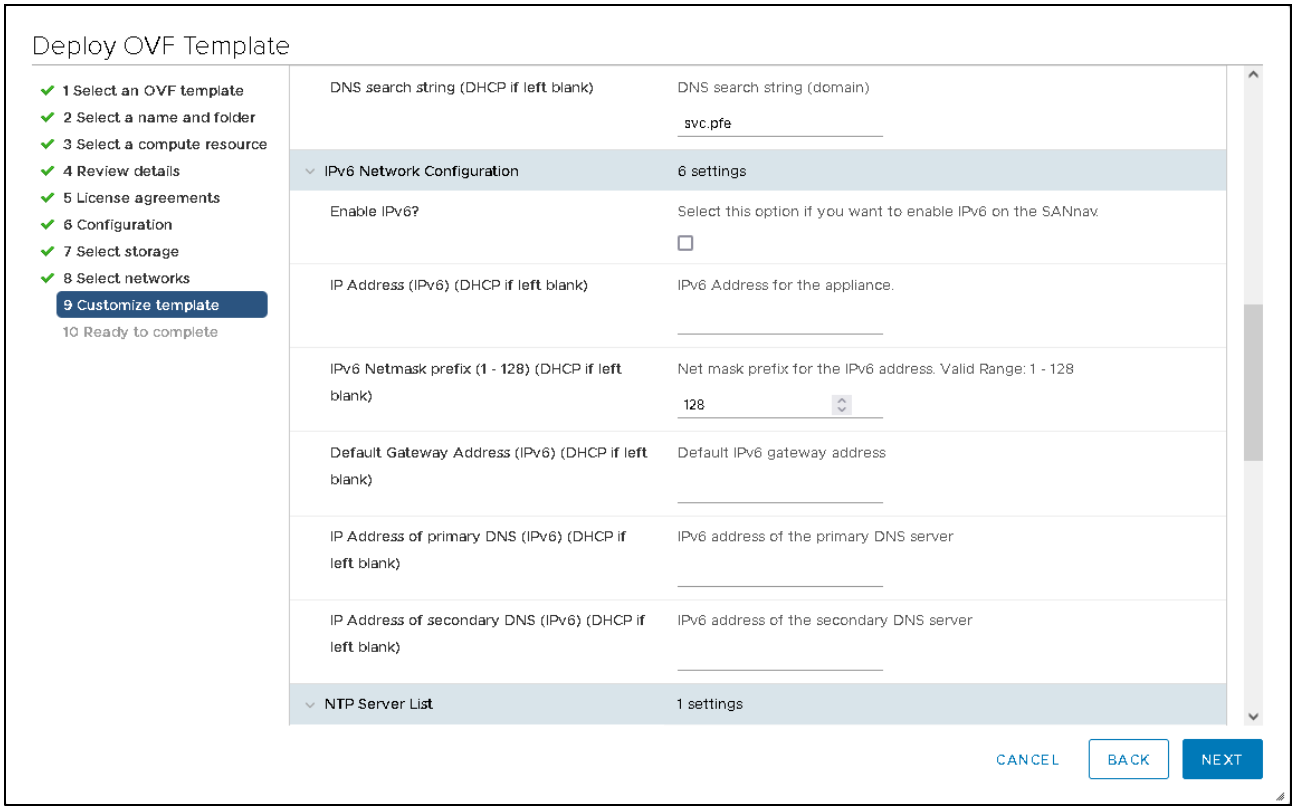


Figure 3-15 Customizing the template DNS and IPv6

– DNS.

Configure the IP address of the primary DNS server. If you use DHCP, leave this section blank. Optionally, you can specify a second DNS server and the DNS search domain. (The necessity of the DNS search domain depends on the network configuration. For a correct name resolution, specify the search domain.

– NTP Server.

To ensure correct flow management, the time of the systems in the SAN environment must be synchronized. Configure the IP address or name of an NTP server. You can configure more than one server by using a comma-separated list of NTP server IP addresses.

– SSHD Customization.

SANnav has a built-in SSH server that is used for the internal firmware repository and SCP and SFTP services. By default, port 22 is used for the Linux server SSH server management. If you use SAN switches in your environment that are running FOS versions that are earlier than Version 8.2.2, then port 22 must be used to access the SANnav, or an external FTP, SCP, or SFTP server is needed for the switch supportsave and firmware download functions. Enable the option to customize the SSHD port and enter the new port number for the Linux SSHD port, as shown in Figure 3-16.

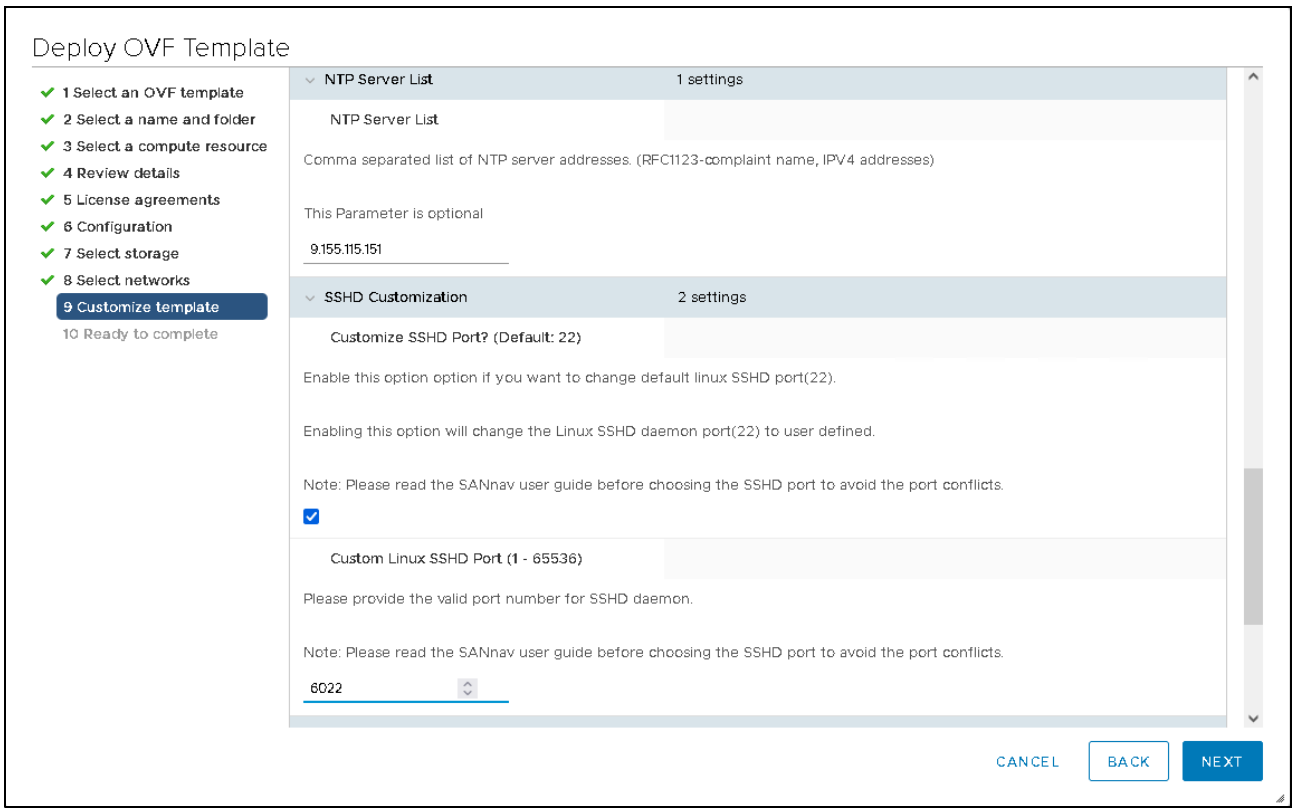


Figure 3-16 Customizing the template NTP and SSHD

– Customize the IP address range of the Docker service in SANnav.

  With the SANnav installation, a dedicated Docker environment is installed on the server, which uses (by default) an IP address range of 192.168.255.240/28, as shown in Figure 3-17. If this IP address range overlaps with an existing IP address range in your network, it must be changed.

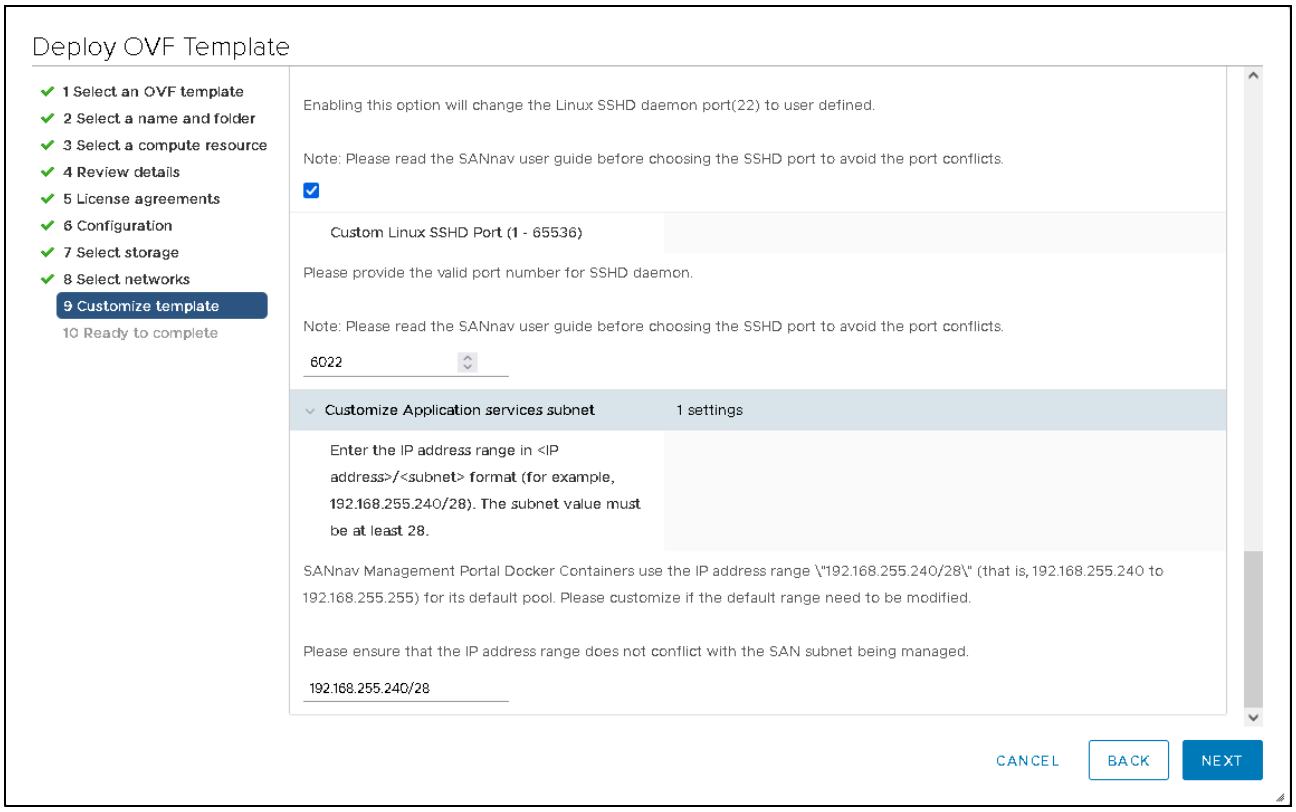


Figure 3-17 Customizing the template

3. A summary of the settings is shown in Figure 3-18 and Figure 3-19 on page 54. You can scroll through the settings and confirm by clicking **Finish** or change your settings by clicking **Back**.

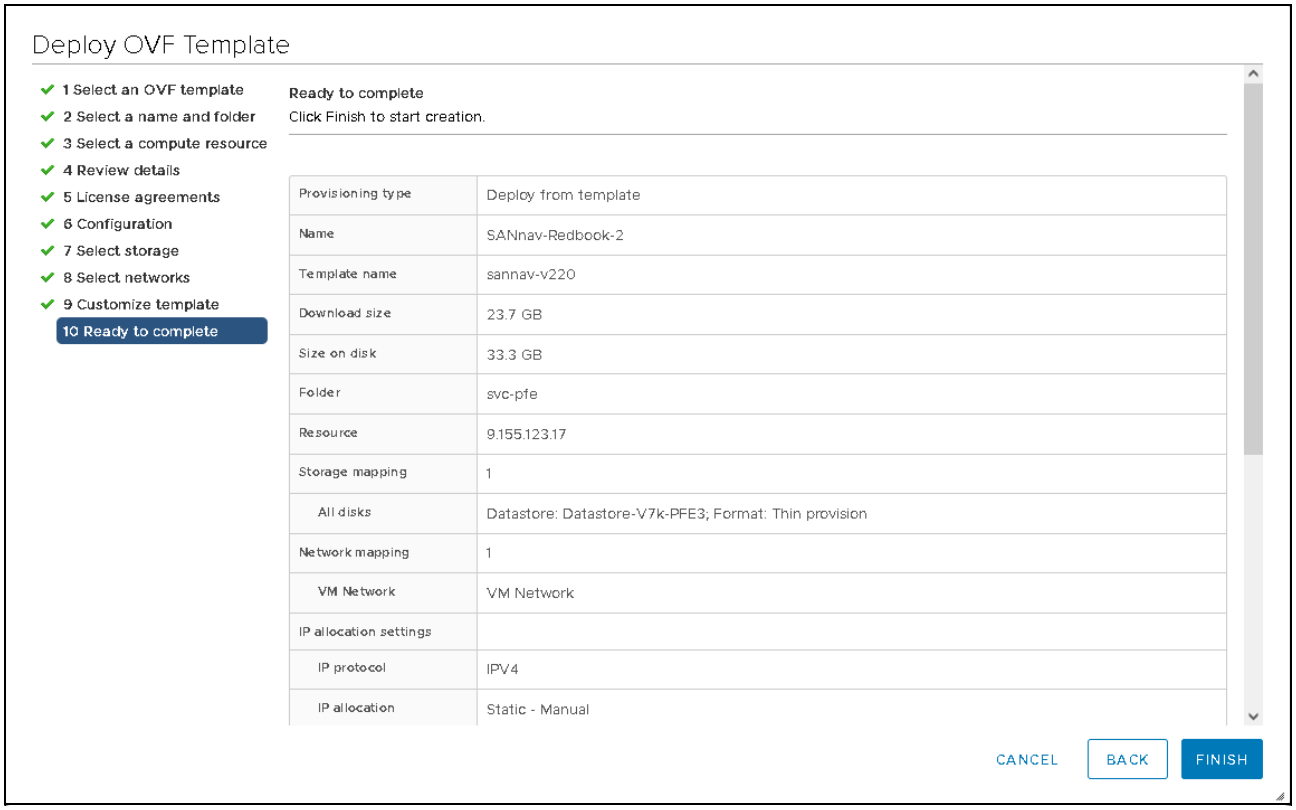


Figure 3-18 Ready to complete the deployment

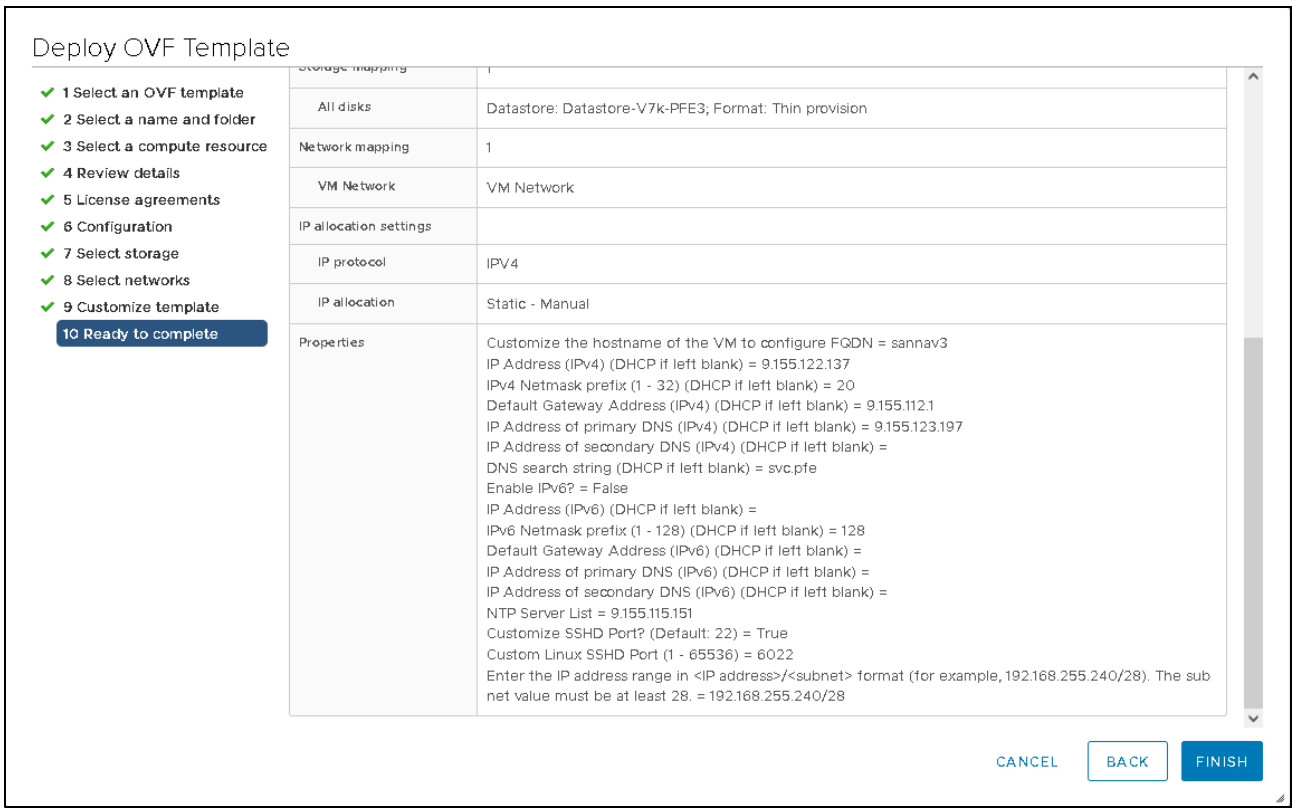


Figure 3-19 Ready to complete the deployment 2

The deployment of the OVA in the virtual environment starts. The process, which is shown in Figure 3-20, takes several minutes, depending on host performance and network bandwidth.

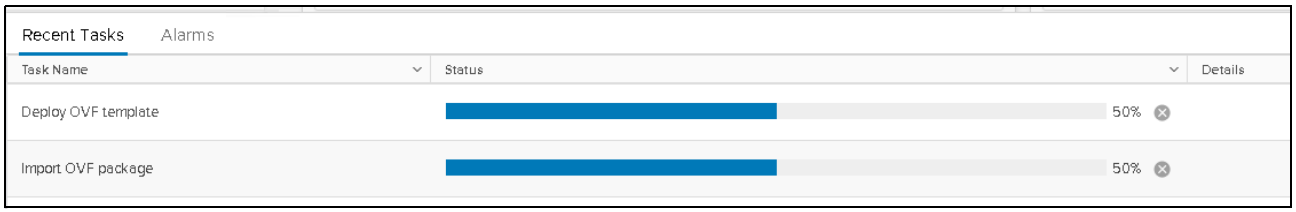


Figure 3-20 OVA deployment status in vCenter recent tasks

3.5.3 Setting up SANnav in the OVA

With the deployment, you already made the general settings for name, network, and time synchronization. The virtual disk that was created from the OVA file contains the SANnav installation software, so you do not need to transfer an installation file to the server. The initial password for the `root` user is `SANnav!@#`.

The first time that you log in to the virtual host as the root user, the SANnav installation starts automatically, as shown in Figure 3-21 on page 55.

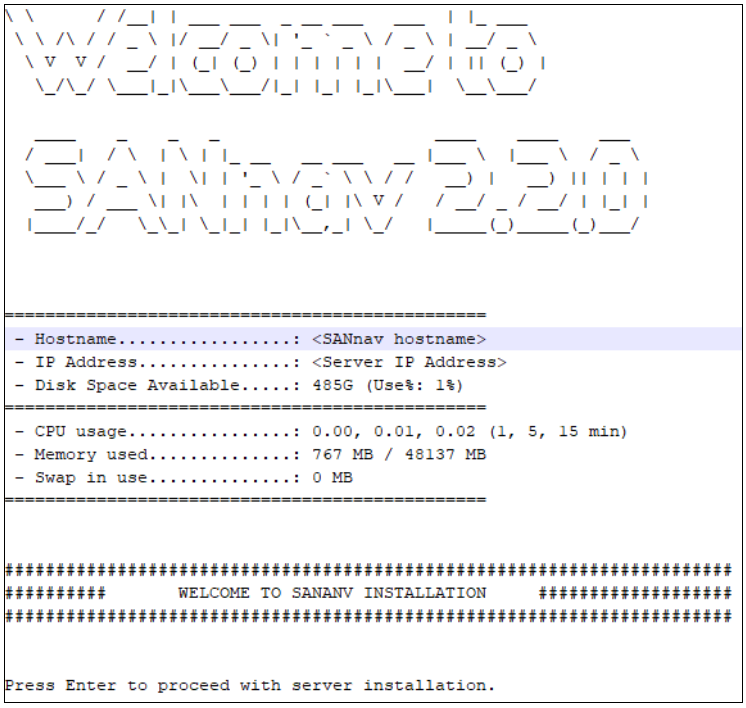


Figure 3-21 SANnav welcome panel at first login

The installation follows the steps that are described in Table 3-5 on page 37 from step 6 onwards.

Complete the installation by using the installation steps that are described in 3.4, “SANnav installation process” on page 36. When the installation completes, the SANnav services start. It takes several minutes before you can connect to the SANnav home panel through your browser to `https://<SANnav-IP-Address>`. You can check the status of the SANnav server by running the **`check-sannav-status.sh`** script, which is explained in 3.7, “SANnav Management Console and scripts” on page 57.

3.6 Firewall configuration and used ports

If your network is protected by a firewall between the SANnav client and the server or between the server and the SAN, you must open a set of ports in the firewall to allow communication. Make sure that the required ports are configured in your network firewall. For more information, see Table 3-7.

Table 3-7 Communication ports and firewall settings

Port #	Protocol (TCP or UDP)	Direction (inbound or outbound	Communication path	Description
22	TCP	Both	Client --> server Server <--> switch	SANnav internal SSH server port. If you customized the port, use the port that was specified in the installation process.
80	TCP	Both	Client --> server Server --> switch	HTTP access browser to server. HTTP access from server to switch.
161	UDP	Outbound	Server --> switch	SNMP.
162	UDP	Inbound	Switch --> server	SNMP traps.
443	TCP	Both	Client --> server Server --> switch Server --> vCenter	HTTPS access between server, switch, and client.
514	UDP	Inbound	Switch --> server	Syslog.
6514	UDP	Inbound	Switch --> server	Secure syslog.
18081	TCP	Inbound	Switch --> server	Required to enable Kafka streaming from switches to SANnav. FOS < 9.0.1.
18082	TCP	Inbound	Switch --> server	Required to enable Kafka streaming from switches to SANnav switch. FOS < 9.0.1.
19094	TCP	Inbound	Switch --> server	Secured Kafka streaming port (required for IPv4 switches).
19095	TCP	Inbound	Switch --> server	Secured Kafka streaming port (required for IPv6 switches).

By default, the relevant ports are added to the **`iptables`** configuration when the SANnav server starts. SANnav use **`iptables`** to block ports that are not required for external access, but when Linux **`firewalld`** is enabled as a local firewall on the Linux server where SANnav is installed, all ports are blocked by default.

You must adjust your firewalld configuration and open the ports that are needed for inbound communication with the server. If the ports were customized during SANnav installation, for example, the SSH port, these customized ports must be used for the firewall configuration.

SANnav uses many IP ports that are not accessed from outside the server. However, it is necessary that these ports are available on the server and not used by other applications or programs. If the ports that are listed in Table 3-8 are not available, the installation will fail.

Table 3-8 Ports internally used by SANnav

Port	Usage in SANnav
2377	Internal use for Docker
5432	Internal use for the database
6060 and 6061	Internal use for containers
7021, 7022, 7051–7057, 7080, 7087, 7089, 7090, 7097, 7611, 7711, 7890, 7946, and 7997	Internal use for containers
8021, 8022, 8080, 8081, and 8200	Internal use for containers
9090, 9091, 9094, 9097, 9100, 9101, 9300, 9443, 9611, 9711, 9763, 9887, 9888, and 9999	Internal use for containers
10800 - 10825	Internal use for containers
11211	Internal use for Apache Ignite
12181	Internal use for Kafka
38917	Internal use for containers
41185, 42239, 45687, and 46537	Internal use for containers
47100 - 47125, and 47500	Internal use for containers

3.7 SANnav Management Console and scripts

SANnav offers several scripts for server administration, verification, and customization. The scripts apply to both standard and OVA installations. They are in the `<install_home>/bin` directory. You should run these scripts only if necessary. Use the “Management Console” and the “Server Health Check” to administer the server and check its status.

SANnav Management Console

The **`sannav-management-console.sh`** script allows you to perform several actions on the SANnav server without having to run individual scripts.

Run the script **`sannav-management-console.sh`** from the `<install_home>/bin` directory to get the available options.

Select an option to run and press Enter:

```
1) Check SANnav status
2) Restart SANnav
3) Stop SANnav
4) Start SANnav
5) Show SANnav configuration
6) Show opensource code attribution
7) Update SANnav configuration
```

If it is necessary to adjust the configuration after installation, use option 5 and 7 to display and update the configuration. Changing any of the configurations stops and restarts SANnav Management Portal services.

Server Health Check

To check the health of the SANnav server, run the **check-sannav-status.sh** script. If any of the services are down, they are listed in the script output. Change to the `<install_home>/bin` directory and run the script:

```
./check-sannav-status.sh
```

Normally, you should get an output like the following one:

```
SANnav server is Healthy. All the services are currently in running state
```

If there is an error, the output contains information about the error and the services that could not be started. Have this information ready for IBM Support if you need further assistance.

Table 3-9 lists all the administrative scripts. Use them only if you are familiar with the function and purpose of the scripts or if you are asked to do so by IBM Support.

Table 3-9 SANnav provided scripts

Script	Description
sannav-management-console.sh	Allows you to perform several actions on the SANnav server.
check-sannav-status.sh	Checks the status of the SANnav server.
show-sannav-configurations.sh	Displays the SANnav port and server configurations.
change-ipv4-installation-to-ipv6.sh	Changes SANnav from an IPv4 installation to a dual-stack IPv4 and IPv6 installation.
configure-proxy.sh	Configures a proxy to connect to the internet.
manage-sannav-whitelisting.sh	Creates and manages a list of IP addresses that are allowed SANnav access. For more information, see Configuring IBM Call Home Notifications.
reconfigure-sannav-for-96GB.sh	Changes the memory configuration of the SANnav installation to 96 GB to support 15,000 ports. Before running this script, ensure that the memory capacity of the SANnav host is at least 96 GB.
replace-sannav-certificates.sh	Replaces SSL self-signed certificates with third-party signed certificates.
restart-sannav.sh	Stops the SANnav server and then restarts it.

Script	Description
sannav-firewall-checker.sh	Checks whether firewalld is enabled and whether the required ports are open (Only available since SANnav v2.2.1).
show-sannav-license-information.sh	Displays the SANnav license serial number and server unique ID (UID).
show-sannav-open-source-software.sh	Displays information about open source software that is used by SANnav.
split-file.sh	Splits a large SANnav support data collection file into smaller files for faster transmission over the network.
start-sannav.sh	Starts the SANnav server after it stops. SANnav should not be running when you run this script.
stop-sannav.sh	Stops the SANnav server.
uninstall-sannav.sh	Uninstalls the SANnav server.
update-auto-enclosure-features.sh	Enables and disables automatic host and storage enclosure creation during fabric discovery. By default, this feature is enabled.
update-events-purge-settings.sh	Changes the maximum number of days that events are retained or the maximum number of events that are stored in the database.
update-reports-purge-settings.sh	Changes the number of days after which reports are automatically deleted.
usage-data-collection.sh	Configures whether collected SANnav usage data is sent to Broadcom.

3.8 SANnav and operating system upgrade

This section describes the following topics:

- Upgrading the SANnav Management Portal installation
- Upgrading the operating system when SANnav is installed

3.8.1 Upgrading the SANnav Management Portal installation

Table 3-10 provides an overview of the possible upgrade paths from previous versions.

Table 3-10 Supported migration paths

SANnav Management Portal current version	New version	Supported / Remarks
SANnav v2.2.0x	SANnav v2.2.1	Yes. SANnav v2.2.0x to SANnav v2.2.1 OVA migration can be done inline.
SANnav 2.1.1x	SANnav v2.2.1	Yes. SANnav 2.1.1 to SANnav v2.2.1 requires full extraction and migration.

SANnav Management Portal current version	New version	Supported / Remarks
SAnav 2.1.0x	SANnav v2.2.1	No.
SAnav 2.0	SANnav v2.2.1	No.
SAnav 1.0	SANnav v2.2.1	No.

Depending on the previous version, an upgrade can be performed inline by installing the new version on the existing system or migrating the existing data to a new system. Always follow the instructions in the release notes. For more information, see the *Brocade SANnav Management Portal Installation and Upgrade Guide v2.2.x*.

Upgrading the SANnav Appliance from v2.2.0 to v2.2.x must be performed inline. The inline upgrade avoids the requirement of a duplicate VM during the upgrade phase.

If you are upgrading from SANnav v2.1.1 OVA, you cannot use this procedure. Upgrading form OVA requires extra steps regarding the license and the installation of a new SANnav Appliance to migrate data from the existing `vmdk` file. For more information, see *Brocade SANnav Management Portal Installation and Upgrade Guide v2.2.x*.

3.8.2 Upgrading the operating system when SANnav is installed

To upgrade the OS (RHEL or CentOS) on a server with SANnav, you must first stop the SANnav services; perform the upgrade; and restart the SANnav services after the upgrade finishes.

The following steps apply whether you are upgrading Red Hat Enterprise Linux (RHEL) or CentOS:

1. Go to the `<install_home>/bin` folder and run the following script:

   ```
   ./stop-sannav.sh
   ```

2. Perform the operating system upgrade by using Yellowdog Updater Modified (YUM) to upgrade to the new OS version:

   ```
   yum upgrade -y
   ```

3. Go to the `<install_home>/bin` folder and run the following script:

   ```
   ./start-sannav.sh
   ```

Note: The YUM upgrades to the latest version of the operating system. If you upgrade to an unsupported OS, its support depends on the compatibility of SANnav with that OS. The upgrade may be allowed, but requires an explicit user agreement.

3.9 Removing SANnav from the server

To remove the SANnav software application and Docker service and bring the system back to the original state, complete the following steps:

1. Go to the `<install_home>/bin` folder and run the following script:

   ```
   ./uninstall-sannav.sh
   ```

2. After the SANnav uninstall script finishes, restart the server.

4

Initial access and basic configuration

This chapter describes how to launch IBM SANnav Management Portal v2.2.x and perform the initial configuration.

This chapter includes the following topics:

- Starting the SANnav Management Portal
- Discovery
- Licensing
- SANnav Management Portal backup and restore
- User management
- Stopping and restarting SANnav

4.1 Starting the SANnav Management Portal

After the successful installation of SANnav, which was described in Chapter 2, “Preparing the environment” on page 13, check that all services are active. To do so, you can use the script **check-sannav-status.sh**:

```
[root@vm-sannav2 bin]# ./check-sannav-status.sh
SANnav server is Healthy. All the services are currently in running state
```

If you get the result that is shown here, you can be sure that all services are active. You can start SANnav configuration.

Note: If anything went wrong, uninstall SANnav or restart the services or Docker. To uninstall the SANnav and bring the background system back to the original state, complete the following steps:

1. Go to the `<install_home>/bin` folder and run the following script:

   ```
   ./uninstall-sannav.sh
   ```

2. After SANnav is uninstalled, restart the SANnav server.

To restart SANnav and Docker services, complete the following steps:

1. Stop the SANnav server with the following script:

   ```
   [root@RHEL82 bin]# ./stop-sannav.sh
   ```

2. Stop the Docker service with the following command:

   ```
   [root@RHEL82 bin]# systemctl stop docker.service
   ```

3. Start the Docker service with the following command:

   ```
   [root@RHEL82 bin]# systemctl start docker.service
   ```

4. Start the SANnav server with the following script:

   ```
   [root@RHEL82 bin]# ./start-sannav.sh
   ```

4.1.1 Browser requirements

Any laptop or machine that launches web applications can be used to launch SANnav Management Portal. For optimal performance, the system should have at least 16 GB of memory.

The following browsers can be used to access the SANnav server:

- Chrome
- Edge
- Firefox

Launching Brocade Web Tools 9.0.0 and later from a SANnav client is supported on Chrome and Firefox.

Launching Brocade Web Tools versions earlier than 9.0.0 is supported only on Firefox. For information about the supported Web Tools browsers, see the *Brocade Fabric OS Web Tools User Guide 9.0.x*.

4.1.2 Launching the SANnav Management Portal

If the output of **`script check-sannav-status.sh`** shows that all services are running, you can launch SANnav Management Portal by completing the following steps:

1. Open your browser and enter the IP address or fully qualified domain name (FQDN) of the SANnav Management Portal server. You can use HTTP or HTTPS, for example:

   `http://192.155.122.166`

   or

   `https://192.155.122.166`

   The SANnav Management Portal login window opens, as shown in Figure 4-1.

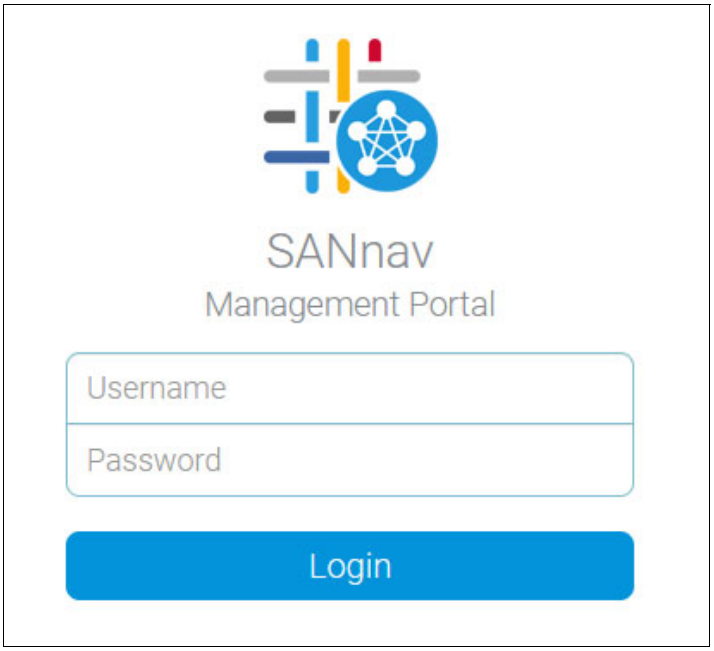


Figure 4-1 SANnav Management Portal login window

2. Enter your SANnav username and password, and click **Login**.

   For the first SANnav login, the default username is Administrator, and the default password is password.

3. The first time a new user logs in successfully, a change password warning appears. You must change your password immediately before you can access SANnav. After you change your password, you are automatically logged out, and you must log in again by using the new password. You can change your password at any time by clicking the user icon in the upper right of the window and then click **User Preferences**, as shown in Figure 4-2.

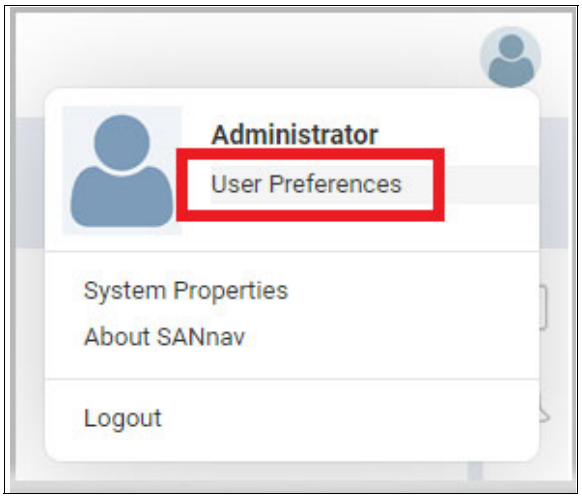


Figure 4-2 User Preferences

4. Click **Edit** next to Logging in, as shown in Figure 4-3.

Figure 4-3 Editing User Preferences

5. Click **Change** on the Logging in window, as shown in Figure 4-4.

Figure 4-4 Changing the password

6. Complete the **Change Password** fields and click **OK**, as shown in Figure 4-5 on page 65.

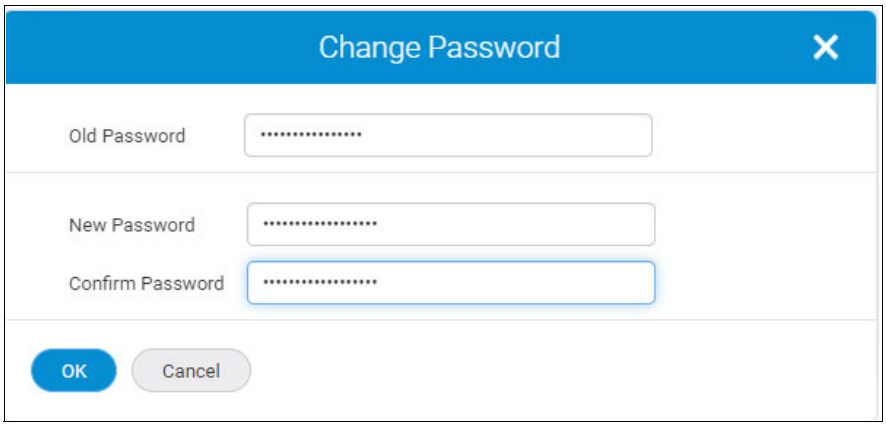


Figure 4-5 Change Password confirmation

Tip: Each time that you change your password, you are automatically logged out of SANnav.

Notes:

- Ping the SANnav server to ensure that the connection is OK.
- SANnav does not support access through a proxy server URL.
- If there is a problem with the connection to the SANnav server, check the firewall settings. HTTP/HTTPS does not work if redirection on port 80 or 443 (if you are using the default HTTPS port) is not enabled during installation.

  Verify whether the configuration is correct by using the script **`firewall-cmd --list-all`**.

  You can find more details about the firewall configuration in Chapter 3, “Installing and deploying IBM SANnav Management Portal” on page 25.

4.1.3 Overview of the user interface

SANnav launches with the default dashboard.

SANnav Management Portal allows you to manage and monitor one or more SAN fabrics in multiple locations. Figure 4-6 shows the basic layout of the SANnav user interface.

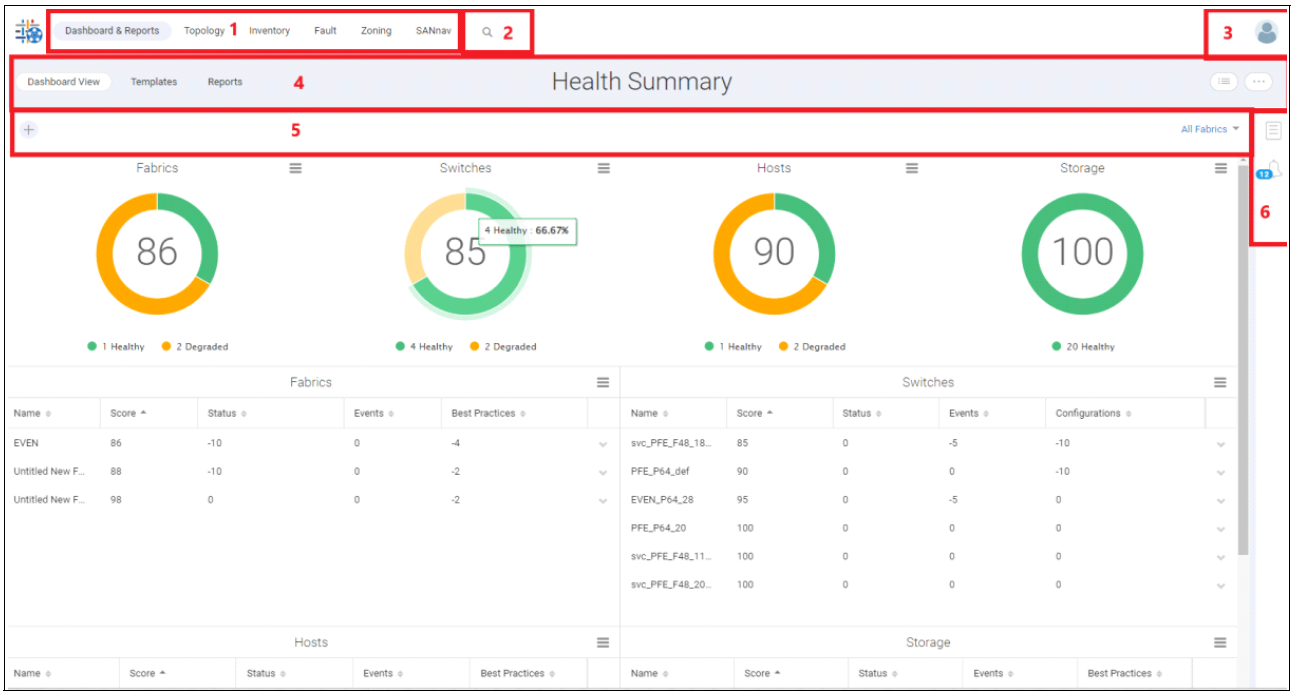


Figure 4-6 SANnav Management Portal user interface

1. Navigation bar: Contains links to feature windows. The SANnav tab displays a window where various settings and configurations can be performed.
2. Global search: Performs a global search of SANnav. Click the magnifying glass icon to select the context on which to search from a list, and enter the search term in the field, as shown in Figure 4-7 on page 67.

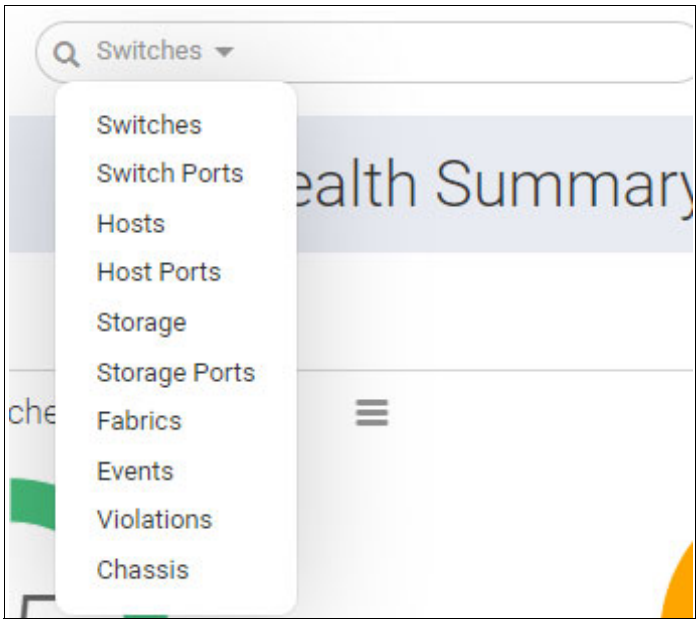


Figure 4-7 Global search

3. Profile menu: Contains links for changing user preferences, displaying the SANnav version, and logging out.
4. Subnavigation bar: Provides the window title and optional item count within parentheses. Also includes buttons and menus to take actions within the window. The subnavigation bar is the main way to navigate within a feature.
5. Filter bar: Allows you to filter the display based on columns, fabrics, and customized filters.
6. Expandable sidebar: Provides options for saving selected inventory items for investigation later and for viewing notifications.

For more information, see Chapter 5, “Main features” on page 103.

4.2 Discovery

Discovery is the process by which SANnav Management Portal contacts the devices in your SAN and adds them to the inventory list. Before you can monitor and manage a fabric, you must first discover it.

For Fibre Channel (FC)-FC routing, you must discover both the backbone fabric and the edge fabrics. The backbone fabric cannot be used to discover and manage the edge fabrics, and the edge fabrics cannot discover and manage the backbone fabric.

During fabric discovery, you provide the IP address and credentials of a switch in the fabric. This switch becomes the seed switch. You can change the seed switch after discovering the fabric. So, a *seed switch* is the switch that you use to discover the fabric.

Choose the seed switch based on the following criteria:

- Choose a switch that is running the highest firmware version in the fabric.
- Choose a Virtual Fabrics-enabled switch if the fabric has switches that are enabled for Virtual Fabrics.

- Choose a Virtual Fabrics-capable switch if no switches in the fabric are enabled for Virtual Fabrics.
- Choose a director if the fabric has both directors and fixed-port switches.

The seed switch is not the same as the principal switch. You select the seed switch when you discover the fabric. The seed switch collects all fabric-wide data, such as fabric membership, connectivity, name server information, and zoning information.

The principal switch is automatically elected when the fabric is formed. The principal switch maintains time and manages domain ID assignment for the fabric.

The seed switch and the principal switch can be the same switch.

If a switch that is running in Access Gateway mode is used as the seed switch, the switch is discovered as a stand-alone fabric. Other switches and end devices in the fabric are not discovered. To discover the entire fabric, select a switch other than the Access Gateway switch to be the seed switch.

If you are using SANnav with a Base license, a director cannot be used as a seed switch.

Note: In SANnav v2.1 and later, you cannot use root user login credentials for the seed switch. If the seed switch was discovered by using root user login credentials in an earlier version of SANnav and then SANnav migrated to Version 2.1 or later, you must reconfigure the seed switch by using other credentials.

When you discover a fabric, provide proper SNMPv3 credentials to collect performance metrics and register for SNMP traps. The SNMP configuration on SANnav Management Portal and on the switch should match for these functions to work properly.

During fabric discovery, you can select whether you want SANnav to configure SNMP by using predefined credentials or whether you want to provide SNMP credentials manually.

By default, SANnav automatically configures SNMP by using the following predefined SNMPv3 credentials:

- SNMP username:
  - For Virtual Fabrics-enabled switches: The same username as the one that was used to discover the seed switch.
  - For non-Virtual Fabrics switches: `snmpadmin1`.
- Auth protocol: `noauth`
- Priv protocol: `nopriv`

For automatic SNMP configuration, the SNMP user is added to the switch if it does not exist on the switch.

If you provide the credentials manually, the SNMP user should be on the switch. For Virtual Fabrics-enabled switches, the user must have access to all logical switches in the chassis; otherwise, collecting performance data fails.

Starting in Fabric OS (FOS) 9.0.0, the SNMPv3 configuration supports a maximum of 12 users. For Virtual Fabrics-enabled switches running FOS 9.0.0 or later, if the number of SNMPv3 users on the switch exceeds 12, which is the maximum that is allowed, then discovery proceeds without adding the SNMP user, even if the credentials are valid. An application event is issued if this situation occurs. Then, all SNMP communication fails, and SANnav cannot collect performance metrics for ports and switches.

Note: Whether you provide the credentials automatically or manually, after fabric discovery, if the SNMP profile does not exist on the switch, all SNMP communication fails, and SANnav cannot collect performance metrics for ports and switches. To fix this problem, use the command-line interface (CLI) to configure the switch and create SNMP user accounts. For more information about configuring SNMP, see the *Brocade Fabric OS Web Tools User Guide 9.0.x*.

4.2.1 Discovering a fabric

You must discover a fabric before you can monitor and manage it.

When you discover a fabric, you must provide the login credentials and IP address of the seed switch.

You can use either IPv4 or IPv6 format.

Note: The root user login credentials cannot be used to discover the seed switch.

If the seed switch is configured with both IPv4 and IPv6 addresses and you provide an IPv4 address, communication with the switches (seed switch and member switches) is over IPv4. If you provide an IPv6 address, communication with the switches is over IPv6.

When you discover a fabric, you can manually provide SNMPv3 configuration parameters, or you can allow SANnav to automatically configure SNMPv3.

To discover a fabric, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring Fabric Discovery**, as shown in Figure 4-8.

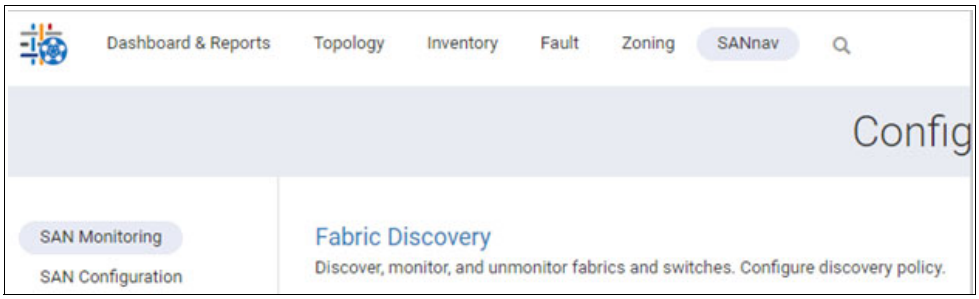


Figure 4-8 Fabric Discovery

The Discovered Fabrics window displays all fabrics that were discovered, as shown in Figure 4-9.

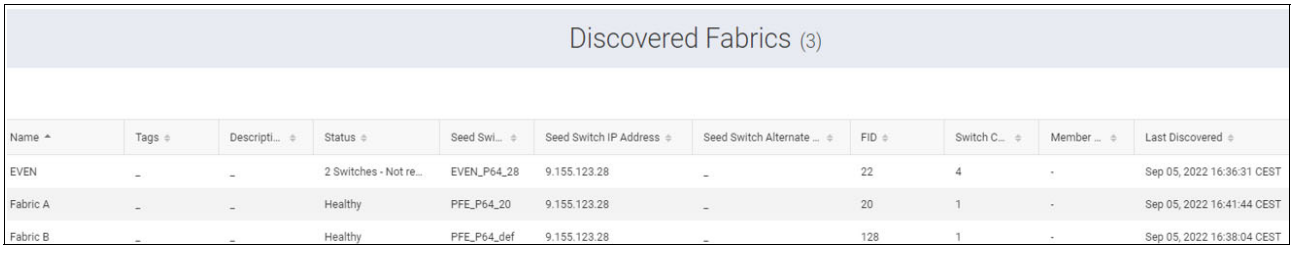


Figure 4-9 Discovered fabrics

2. Click the **+** icon in the upper right to add a fabric, as shown in Figure 4-10.

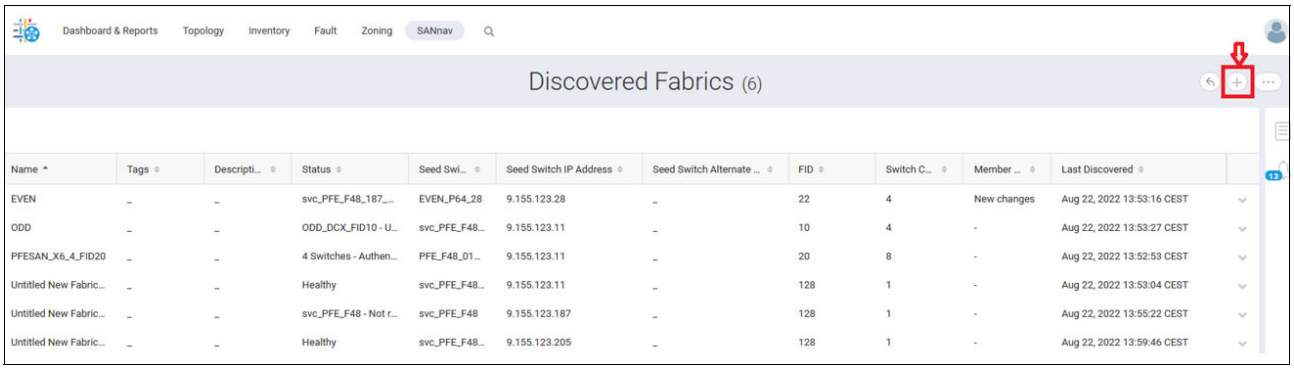


Figure 4-10 Adding a fabric

3. Enter the IP address and login credentials of the seed switch in the Add Fabric dialog box, as shown in Figure 4-11. The IP address can be in IPv4 or IPv6 format, depending on the SANnav configuration.

Tip: If you do not provide login credentials, the default credentials are used. Login credentials for the root user are not allowed.

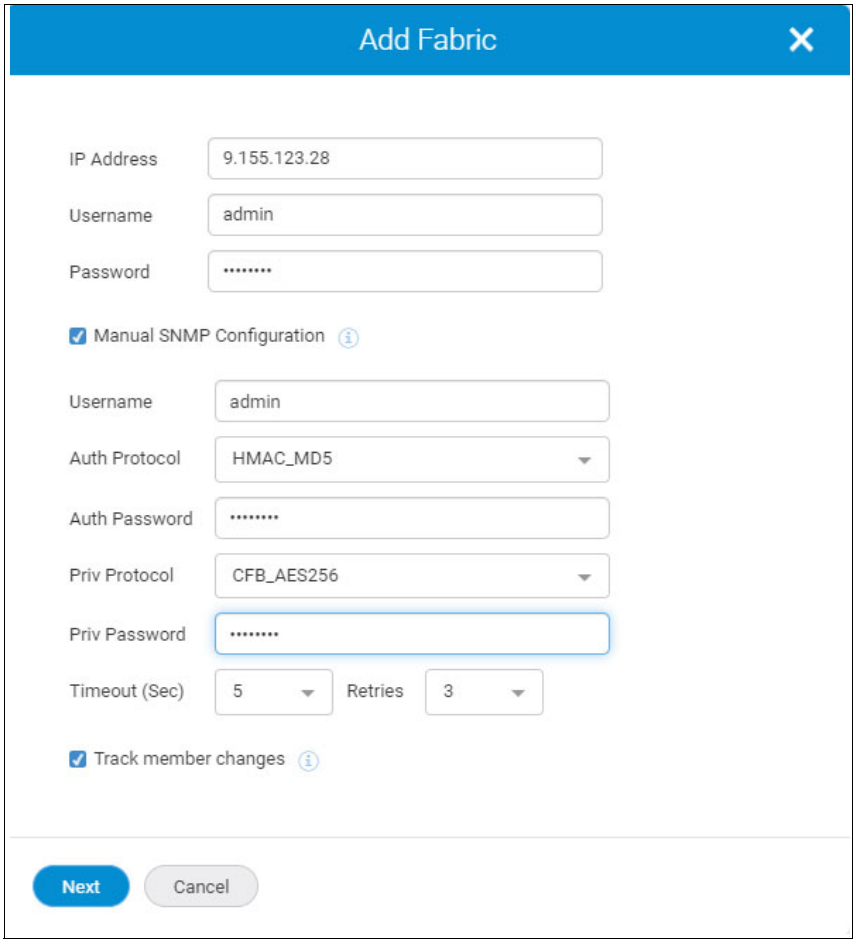


Figure 4-11 Seed switch IP address and login credentials

4. You can disable or enable fabric tracking by selecting the **Track member changes** checkbox.

Note: Fabric tracking is enabled by default. When **Track member changes** is selected, SANnav tracks when switches, end devices, or connections are added to or removed from the fabric.

5. If you want to manually enter the SNMP configuration parameters, select **Manual SNMP Configuration** and enter the information in the dialog box. If **Manual SNMP Configuration** is not selected, SNMP is automatically configured by using predefined SNMPv3 credentials. Click **Next**.

Important: Keep in mind that SANnav supports only SNMPv3.

Note: SNMPv3 must be configured on the switch for SANnav to collect performance metrics for ports and switches.

6. If you selected Manual SNMP Configuration, SANnav prompts you to ensure that the SNMP user has access to all logical fabrics, as shown in Figure 4-12. Click **Next**.

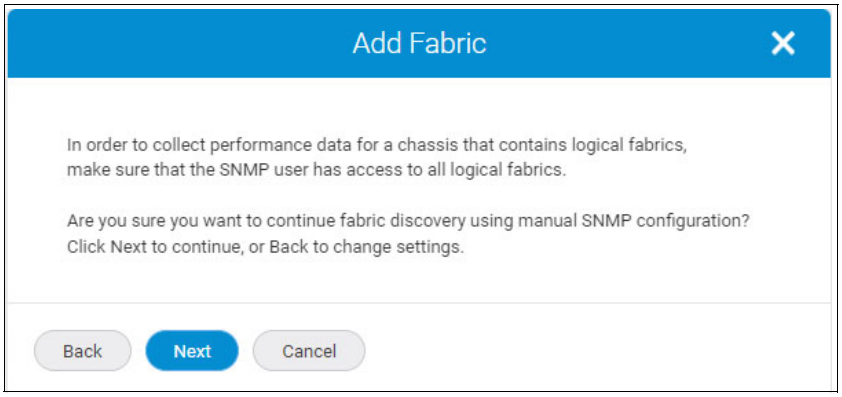


Figure 4-12 Add Fabric with manual SNMP configuration

7. If the seed switch is enabled with Virtual Fabrics and has more than one undiscovered logical switch, select which logical switches to discover.

Note: The Add Fabric dialog box displays a list of the logical switches that are configured on the seed switch. Each logical switch corresponds to a logical fabric, which is indicated by the fabric ID (FID). The Name column displays the logical switch name, not the logical fabric name.

The dialog box displays only the logical switches that have not been discovered.

8. Select one or more logical fabrics to discover and click **OK**, as shown in Figure 4-13.

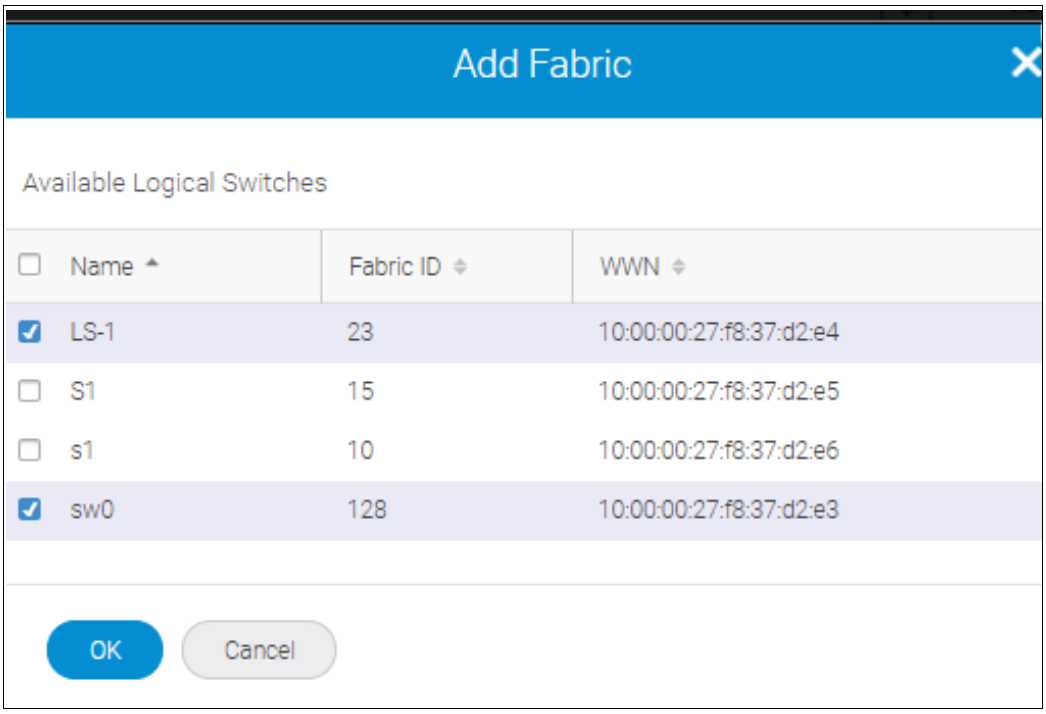


Figure 4-13 Add Fabric

Tip: You can select a maximum of four logical fabrics. If the physical switch (chassis) is configured with more than four logical fabrics, use another switch as the seed switch to discover the remaining logical fabrics. In this way, the asset collection load is distributed across the switches.

The Discovered Fabrics window, as shown in Figure 4-14, displays the newly discovered fabrics.

Figure 4-14 Discovered Fabrics

9. Click the fabric name to open the detail window, where you can change the fabric name, add tags, and view a list of switches in the fabric, as shown in Figure 4-15 on page 73. If a switch name is disabled, the switch is physically disconnected from the fabric. SANnav maintains this information for tracking purposes.

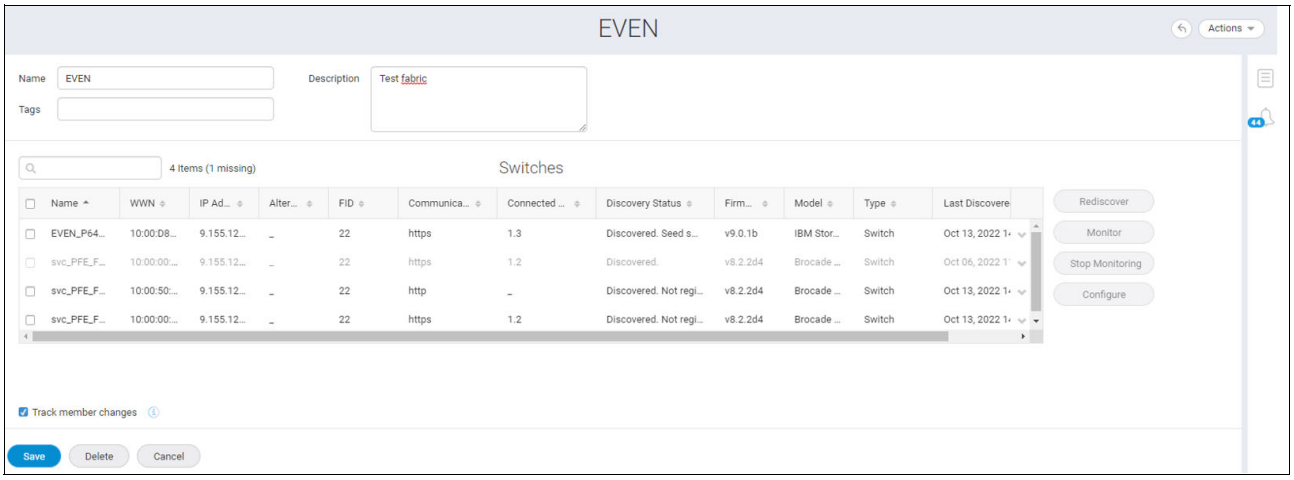


Figure 4-15 Detail window

4.2.2 Rediscovering a switch

Information about discovered fabrics and switches is updated at periodic intervals. You can rediscover a switch if you want the switch information to be updated immediately.

To rediscover a switch, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring Fabric Discovery**. The Discovered Fabrics window displays all fabrics that were discovered.
2. Click the fabric name to open the fabric detail window, which displays the list of switches in the fabric.
3. Select one or more switches, and click **Rediscover** at the right of the Switches table, as shown in Figure 4-16.

Tip: Clicking **Rediscover** at the right of the Switches table rediscovers the selected switches. Clicking **Rediscover** from the **Actions** menu rediscovers the entire fabric.

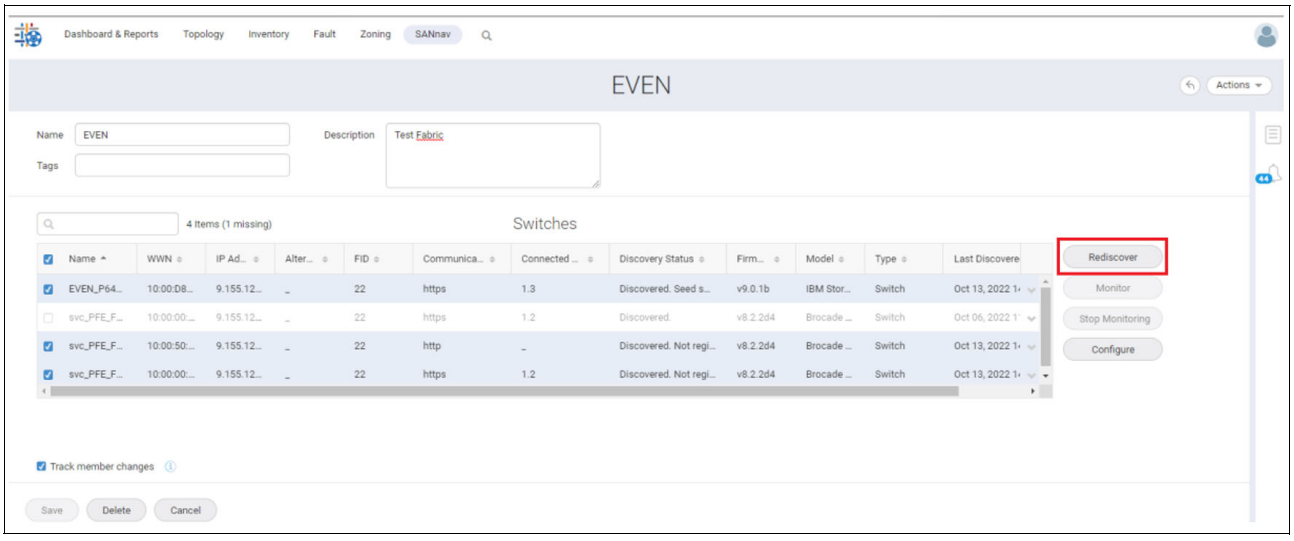


Figure 4-16 Rediscovering switches

The display updates with the latest information from the rediscovered switches.

4.2.3 Rediscovering a fabric

When a fabric is discovered, the displayed information is updated at periodic intervals. If you want the fabric information to be updated immediately, you can rediscover the fabric.

The following steps show how to rediscover a single fabric. You can also rediscover multiple fabrics by using the **Bulk Select** option.

1. Click **SANnav** in the navigation bar, and then select S**AN Monitoring Fabric Discovery**. The Discovered Fabrics window displays all fabrics that were discovered.
2. Locate the fabric that you want to rediscover, click the down arrow at the right of the table entry, and click **Rediscover**, as shown in Figure 4-17.

Figure 4-17 Rediscovering a fabric

The display updates with the latest information from the rediscovered fabric.

4.2.4 Changing the seed switch

If the status of the current seed switch shows that it is not recommended as a seed switch, you should change the seed switch.

You might need to change the seed switch for the following reasons:

- The seed switch is no longer running the latest FOS version in the fabric, which might happen if newer switches join the fabric or the switch firmware version changes on any switch in the fabric.
- The seed switch is going to be taken down for maintenance or replacement.

To change the seed switch, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring Fabric Discovery**.

   The Discovered Fabrics window displays all fabrics that were discovered.
2. Click the fabric name to open the fabric details window, which displays the list of switches in the fabric.
3. Locate the switch that you want to make the seed switch.
4. Click the down arrow in the rightmost column to open the action menu for the switch and click **Seed Switch** or **Seed Switch (Recommended)**, as shown in Figure 4-18 on page 75.

   If the Seed Switch option includes (Recommended), the switch is recommended as a seed switch. The Seed Switch option is available only if the switch can act as a seed switch and the switch is not the seed switch.

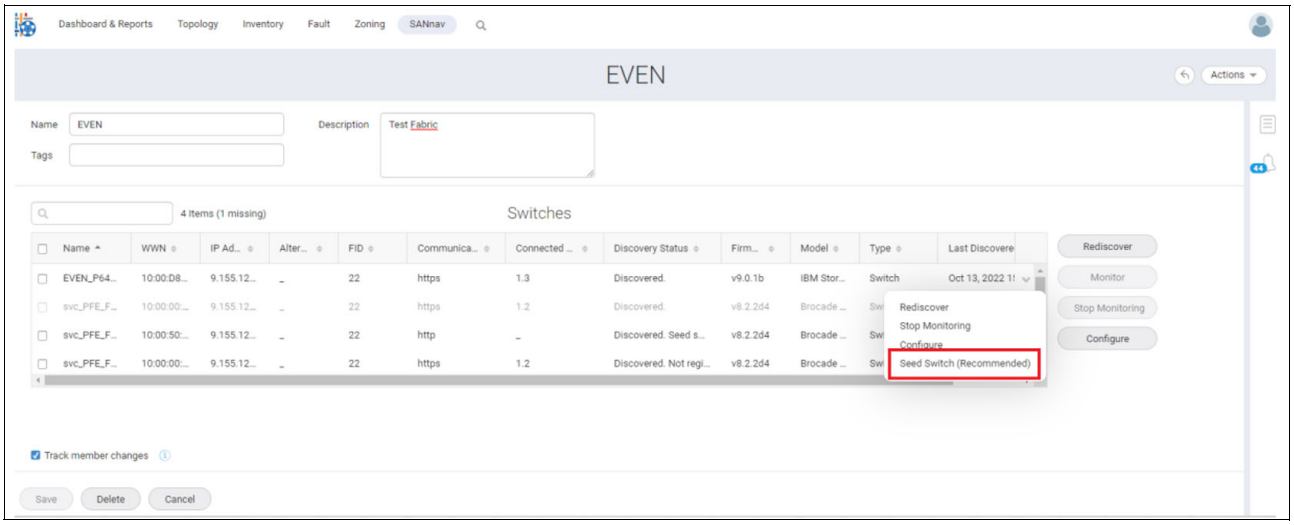


Figure 4-18 Changing a seed switch

The new switch becomes the seed switch, and the switch status updates.

4.2.5 Updating switch credentials

If the login credentials or SNMP configuration changes on the switch, you must update the switch credentials in SANnav Management Portal.

To locate switches with incorrect credentials and update the credentials, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring Fabric Discovery**.

   The Discovered Fabrics window displays all fabrics that were discovered. If a fabric contains switches that have incorrect credentials, SANnav displays “Authentication failed” in the Status column.

2. Search for “failed” in the current view to locate the fabrics that contain switches with incorrect credentials.

3. Hover your cursor over the message in the Status column to see the complete message, including the switch name, as shown in Figure 4-19.

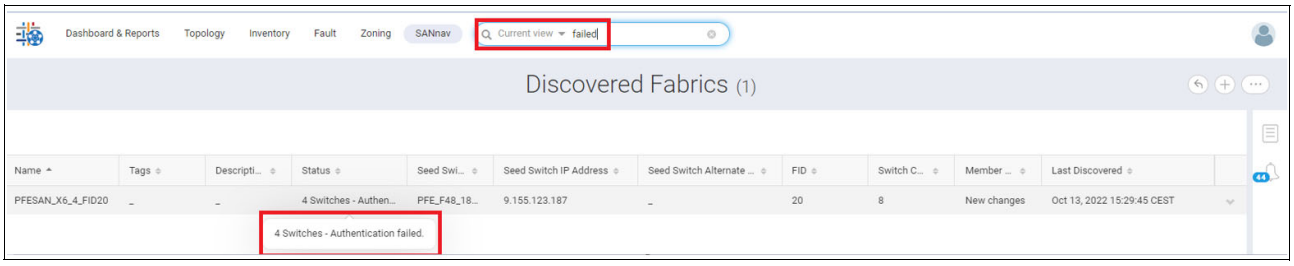


Figure 4-19 Search for switches with the “failed” status

4. Click the fabric name to open the fabric detail window, which displays the list of switches in the fabric, as shown in Figure 4-20.

Note: For switches with incorrect credentials, the Discovery Status column indicates “Discovered. Authentication failed. Not registered for SNMP traps.”

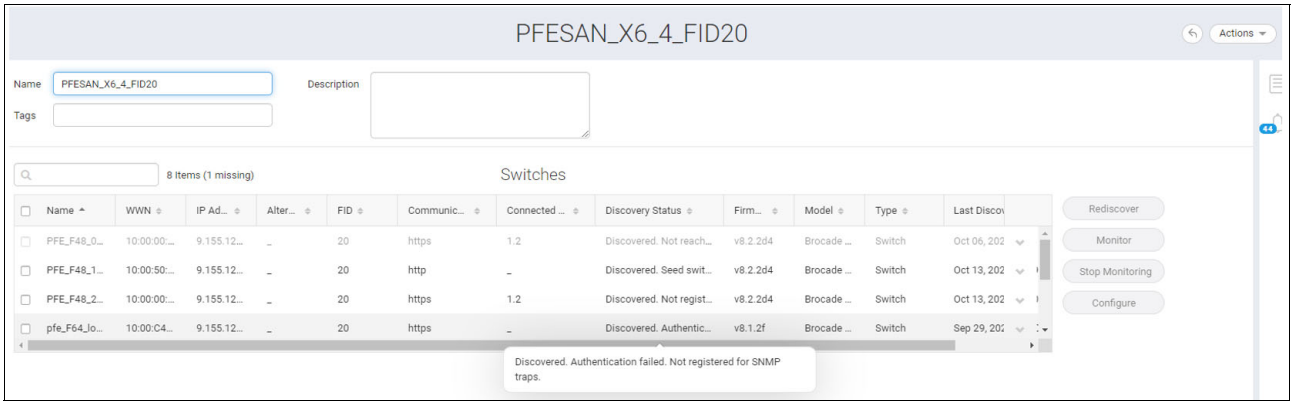


Figure 4-20 Discovery status

5. Select the switches with incorrect credentials and click **Configure**, as shown in Figure 4-21 on page 77.

Tip: If you select one switch, the Configure dialog box is populated with the current values for that switch. If you select multiple switches, the Configure dialog box is empty, and any values that you enter apply to all selected switches.

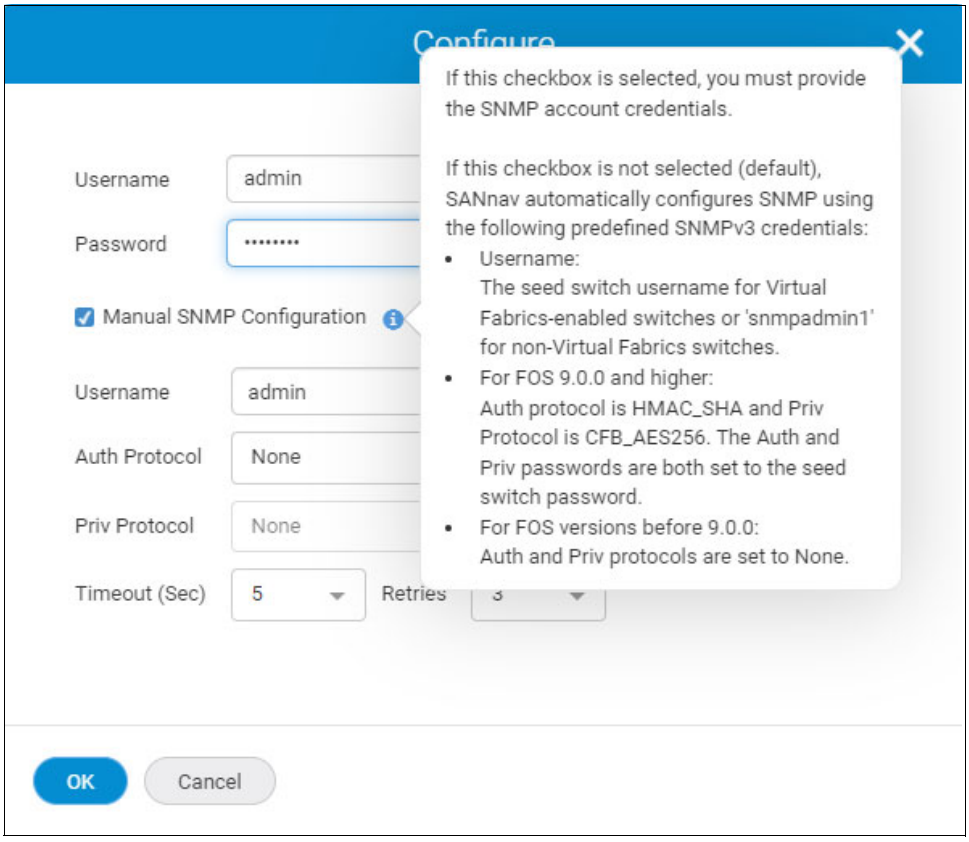


Figure 4-21 Login credentials

6. If the login credentials changed, enter the new login credentials for the switch.
7. If the SNMP configuration changed, select **Manual SNMP Configuration** and enter the updated information in the dialog box.
8. Click **OK**. The credentials that SANnav uses to discover the switch or for SNMP configuration are changed.

4.2.6 Deleting a fabric

If you no longer want SANnav to discover and monitor a specific fabric, you can delete it from the application.

The following information is retained after you delete the fabric:

- Switches: Tags, description, custom properties, and maintenance mode settings.
- Switch ports: Tags, description, and custom properties.
- Hosts and storage: Name, tags, description, model, vendor, type, location, contact, and IP address.
- Host ports and storage ports: Tags, description, custom properties, and port role (initiator or target).

Deleting a fabric also deletes the fabric data on the server (both system-collected data and user-defined data). If you want to preserve the fabric data, you should first stop monitoring the fabric, back up the data, and then delete the fabric. To do so, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** → **Fabric Discovery**. The Discovered Fabrics window displays all fabrics that were discovered.
2. Click the fabric name to display the fabric drill-down window.
3. Click **Delete** at the bottom of the window.
4. Confirm the deletion when prompted.

   On successful removal of the fabric, you are returned to the Discovered Fabrics window. The fabric no longer displays in the list of discovered fabrics.

4.3 Licensing

When you install SANnav, you have a 30-day trial period during which you can use SANnav a no charge without a license. To use SANnav beyond the trial period, you must purchase a license. The 30-day trial period is activated automatically and starts from the time that you install the SANnav product.

SANnav licenses are subscription-based, which means that they expire at the end of the subscription period. If the license expires, you cannot log in to SANnav unless you provide a new license certificate. Before your license expires, you should renew the license to ensure uninterrupted service. By default, SANnav is configured during installation to automatically retrieve and activate renewed licenses.

Note: SANnav Management Portal and IBM SANnav Global View are two separate products, which require separate license certificates and are independent in terms of licensing.

When you install SANnav, whether on a server or on a virtual machine (VM), a server unique ID (UID) is generated for that SANnav instance. The server UID and the transaction key are used to generate a SANnav license. The license is locked to that server UID and SANnav instance.

Note: SANnav v2.2.0 and later use a license certificate (XML file). Earlier versions of SANnav use a license key (text string). These license keys are not supported by SANnav v2.2.0 and later. During migration to SANnav v2.2.1 from Version 2.1.1, the existing license key is automatically converted to a license certificate.

For more information, see the *Brocade SANnav Management Portal Installation and Upgrade Guide v2.2.x*.

You need one license for every SANnav instance, and each license can be used on only one SANnav instance. For example, if you have multiple VMs on a single server and you install SANnav on every VM, each installation generates a separate server UID and requires a separate license. You cannot clone a VM and use the same license on the cloned VM.

If you must move a license from one SANnav instance to another one, for example, if you want to move the installation to a different server, you do not need to purchase a new license; you can “rehost” the license on the new SANnav instance.

4.3.1 Obtaining the server UID

During installation, SANnav generates a server UID, which you need when you generate a license. You can obtain the server UID from the SANnav Licensing window. To do so, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services SANnav Licensing**, as shown in Figure 4-22.

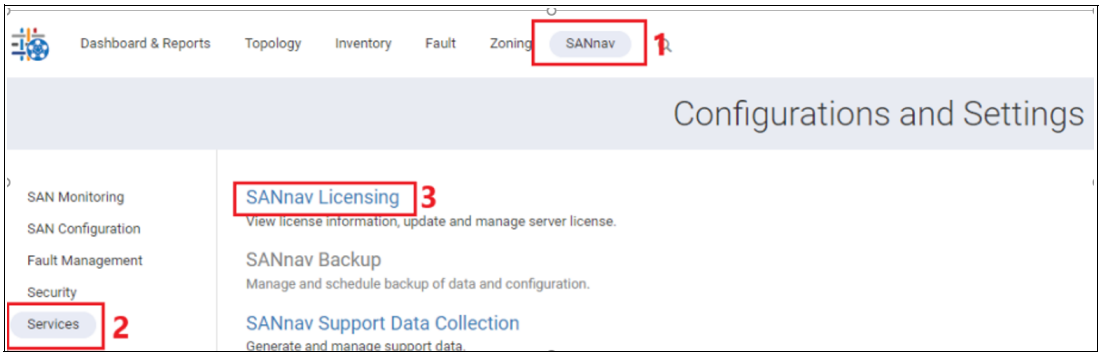


Figure 4-22 SANnav licensing

2. Click the license for which you want to obtain the server UID.
3. When you first install SANnav, only a Trial license displays, so click **Trial**, as shown in Figure 4-23.

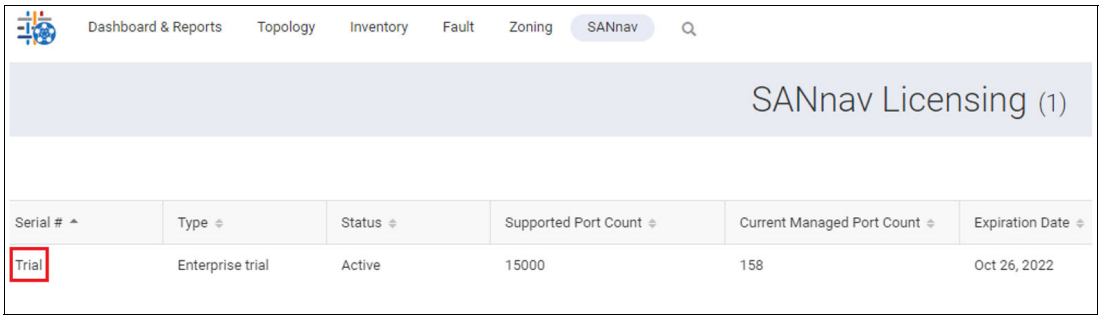


Figure 4-23 SANnav Trial license

4. Copy the server UID so that you can paste it later on Broadcom licensing portal to generate a license certificate, as shown in Figure 4-24.

Tip: Be sure to copy the server UID without missing any characters. An incorrect or partial server UID can lead to an incorrect license being generated from the license portal.

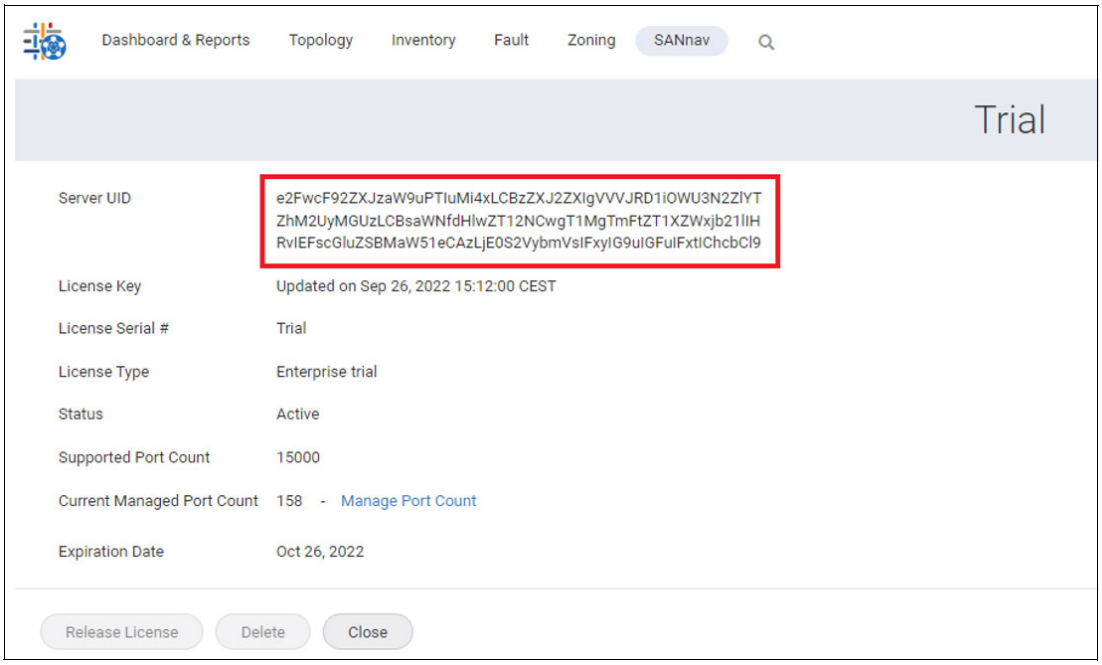


Figure 4-24 Server UID

Additionally, SANnav v2.2 provides a new script that is named **`show-sannav-license-information.sh`**. You can run this script to discover the server UID and license serial that was installed in SANnav, as shown in Example 4-1.

Example 4-1 The show-sannav-license-information.sh script

```
[root@SANNAV10 bin]# ./show-sannav-license-information.sh
License Serial Number: Trial
Server UID:
e2FwcF92ZXJzaW9uPTIuMi4xLCBzZXJ2ZXIgVVVJRD1iOWU3N2ZlYTZhM2UyMGUzLCBsaWNfdHlwZT12NC
wgT1MgTmFtZT1XZWxjb21lIHRvIEFscGluZSBMaW51eCAzLjE0S2VybmVsIFxyIG9uIGFuIFxtIChcbCl9
```

We can also extract the server UID from containers by completing the following steps:

1. Log in to the SANnav server as root or **`sudo`**.
2. Go to the directory where Docker is installed during installation. The default path is `/var/lib/docker`.
3. Once you are in this directory, **`cd`** to the directory `containers`:

   ```
   [root@centos79-44-38 containers]# pwd
   /var/lib/docker/containers
   ```

4. From this directory, run the following command:

   ```
   grep -iR "Encrypted server instance Id" ./
   ```

   Example 4-2 on page 81 shows the output of the command.

Example 4-2 Running the command grep -iR “Encrypted server instance Id”./

```
[root@SANNAV-11 containers]# pwd
/var/lib/docker/containers
[root@SANNAV-11 containers]# grep -iR "Encrypted server instance Id" ./
./0cdd28105379222b91de081e81250386f89e61605890467db051937b3a35d4ae/0cdd28105379222
b91de081e81250386f89e61605890467db051937b3a35d4ae-json.log:{"log":"license-mw -
[INFO ] 19:04:27.235 [main] com.brocade.dcm.licensing.LicenseInitializer\u0009-
Server instance Id:8e52f8a60623263d and Encrypted server instance Id:
e2FwcF92ZXJzaW9uPTIuMi4xLCBzZXJ2ZXIgVVVJRDO4ZTUyZjhhNjA2MjMyNjNkLCBsaWNfdHlwZT12NC
wgT1MgTmFtZT1XZWxjb21lIHRvIEFscGluZSBMaW51eCAzLjEOS2VybmVsIFxyIG9uIGFuIFxtIChcbCl9
\n","stream":"stdout","time":"2022-09-26T17:04:27.235914951Z"}
[root@SANNAV-11 containers]#
```

4.3.2 Generating a license

You should receive an email with the license transaction key in the form of an electronic transaction key from a vendor (for example, IBM). Do not discard the email with the electronic key. Keep it in a safe place in case it is needed for technical support or product replacement.

To generate a license, complete the following steps:

1. Go to https://www.broadcom.com, and then select **Go to Portal** or **Register** from the drop-down Support Portal at the upper right of the web page, as show in Figure 4-25.

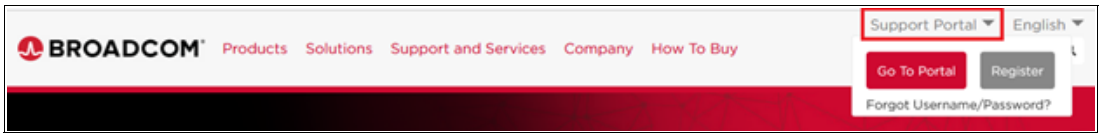


Figure 4-25 Broadcom Support Portal

2. Enter your username and password or create your account by clicking **Register**, and then log in. You are redirected to the Broadcom Support Portal.
3. Click **Brocade Products** or **Brocade Storage Networking**. You are redirected to the Brocade Products page.
4. Click **Licensing** or **License Management**. You are redirected to the Broadcom Licensing Portal page, as shown in Figure 4-26.

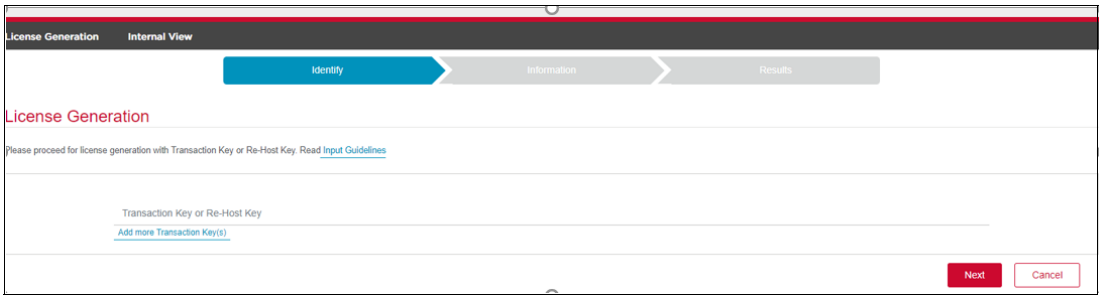


Figure 4-26 License Generation

5. Enter the license transaction key or rehost key in the License Generation window and click **Next**.

6. In the Product Information area, enter the server UID that you obtained from SANnav, as shown in Figure 4-27.

Tip: Be sure to enter the server UID without missing any characters. An incorrect or partial server UID can lead to an incorrect license being generated.

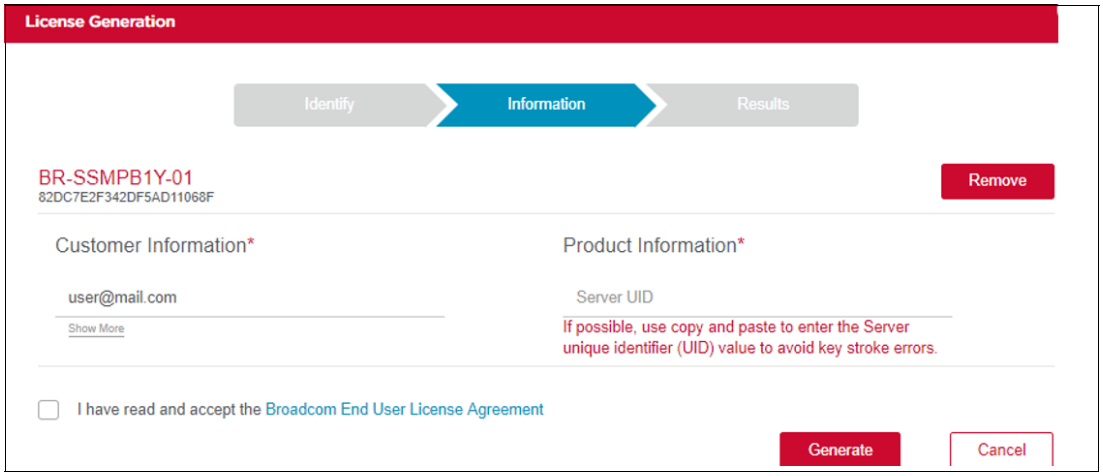


Figure 4-27 Server UID

7. Read the Broadcom End User License Agreement, and if you agree to the terms, select the **I have read and accept Broadcom EULA** checkbox.
8. Click **Generate**. The Results window displays an order summary and the results of the license request.
   - If the license request is successful, the License field contains a hyperlink to the generated license file. The license file is automatically sent by email to the specified customer email address.
   - If the license request fails, the reason for failure and the action to take are displayed on the page.
9. Click the hyperlink in the License field to display the license key.
10. Copy the license key to a `.txt` file and save it. You use this license key when you add the license to SANnav, as shown in Figure 4-28.

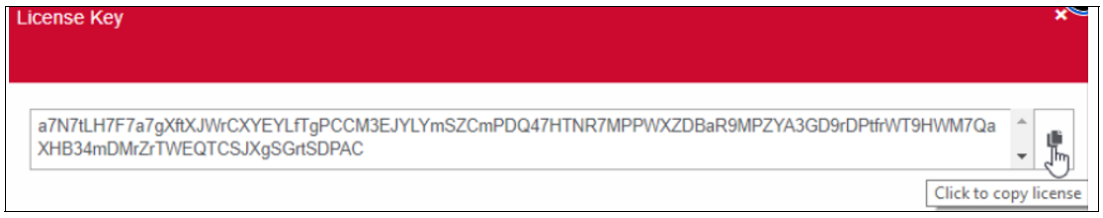


Figure 4-28 License key

11. Click **Export to Excel** to export the results to a Microsoft Excel file, or click **Generate Another License** to generate a license.

Tip: If you fail, you can open a ticket on the IBM Support portal, and IBM SAN Support creates the license for you based on the transaction key and server UID in Figure 4-24 on page 80.

4.3.3 Adding a license to SANnav

After you obtain a license certificate from the Broadcom Licensing Portal, you must add the license certificate to SANnav to activate the license.

The license certificate must be the XML file that was generated for this instance of SANnav (that used the server UID of this instance). The XML file must be installed to enable the license. If SANnav v2.1.1 is still installed, then instead of the XML file, you should have a license key string.

Starting in SANnav v2.2.0, a license certificate (XML file) is used instead of a license key. Any previously issued and installed license keys will not work in SANnav v2.2.0 and later.

During migration, SANnav sets the existing license key to the “Released (Active)” state. When the new SANnav v2.2.0 starts, SANnav attempts to connect to the licensing portal, and if successful, it converts the existing license key to a new license certificate.

If SANnav cannot connect to the licensing portal, the existing license key is valid for 30 days. During this 30-day period, you must obtain the rehosting key from the SANnav v2.2.0 licensing details window and use this key to generate a license certificate from the licensing portal.

Note: Only the active license key is migrated. Any inactive licenses are not migrated.

When you activate a new license, the current license is deactivated, but the expiration date of the current license remains the same. For example, assume you install a 1-year Base license. After 8 months, you purchase and activate an Enterprise license on the same SANnav server. The Base license becomes inactive and expires in 4 months (on the original expiration date).

The following steps show what happens when you add a license:

1. Click **SANnav** in the navigation bar, and then select **Services SANnav Licensing** to view the license list.
2. Click **+** at the upper right of the SANnav Licensing window.

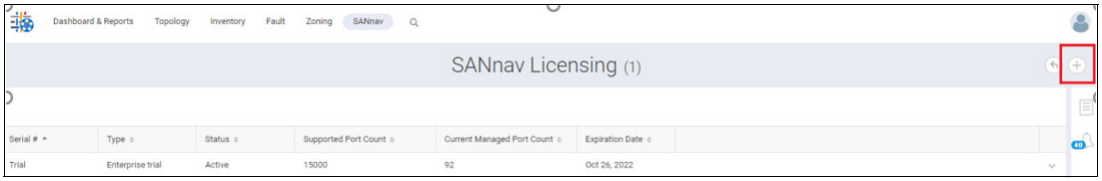


Figure 4-29 SANnav Licensing

3. Click **Browse** and go to the location of the license certificate XML file that you obtained from the Broadcom Licensing Portal, as shown in Figure 4-30. Select this file, and click **OK**.

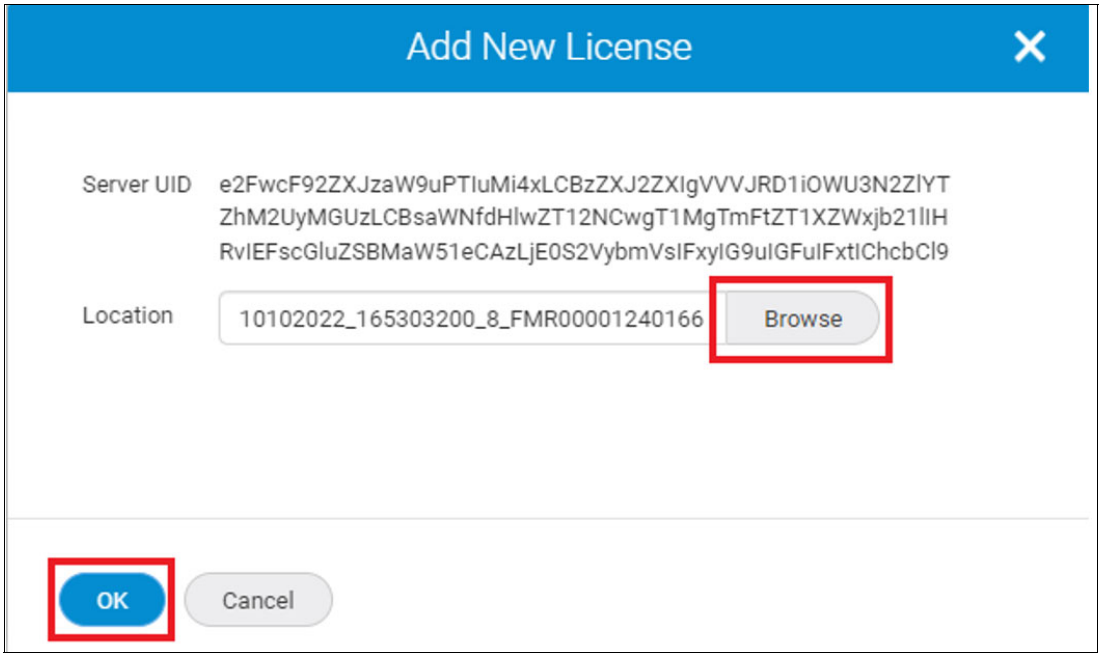


Figure 4-30 Add New License

The new license is added to the SANnav Licensing window (Figure 4-31):

- If the new license has the same serial number as the existing license, the new license replaces the existing license and is automatically activated.
- If the new license has a different serial number from the existing license, the new license is added as a separate entity in the SANnav Licensing window and is in an inactive state.

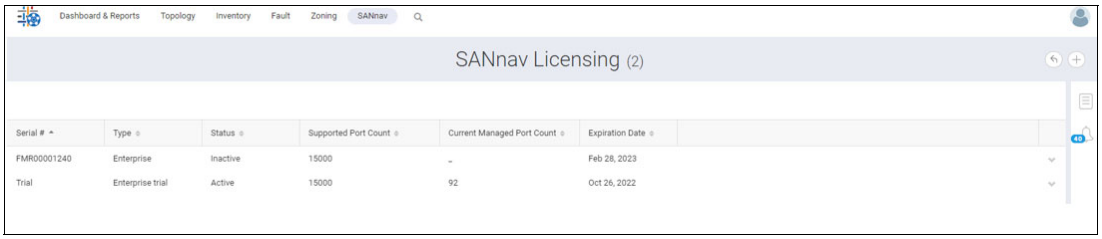


Figure 4-31 Inactive/active license

4. To activate the license, click the down arrow at the right of the license row, and then click **View** to display the license details window, as shown in Figure 4-32 on page 85.

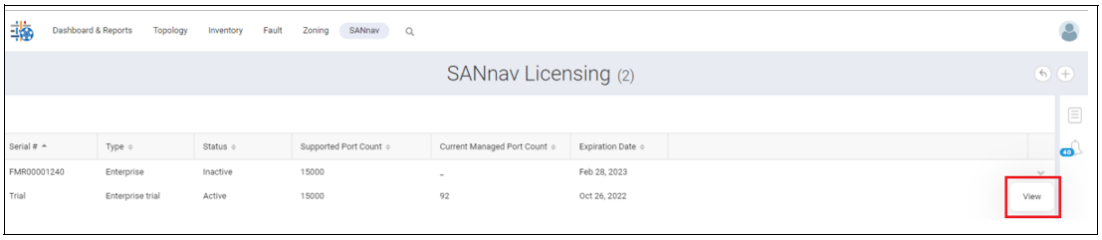


Figure 4-32 Selecting a license key

5. Click **Activate** to activate the license, and then click **OK** to continue activation, as shown in Figure 4-33.

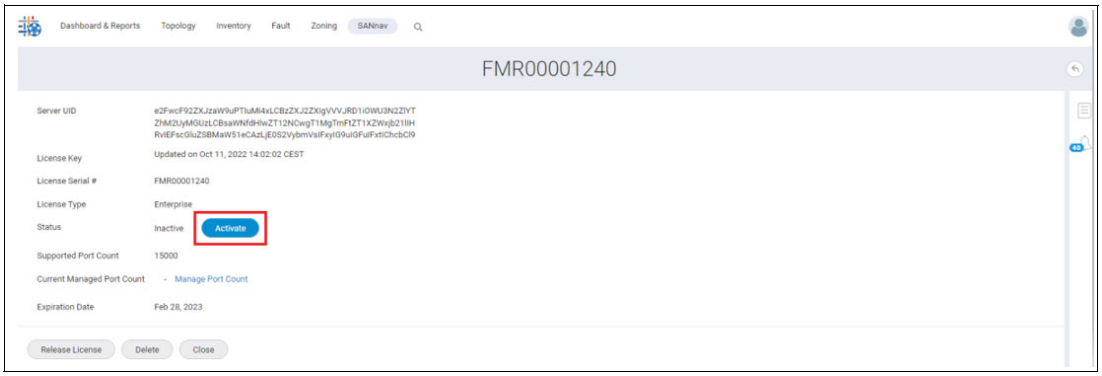


Figure 4-33 Activating a license key

Only one license can be active at a time. When you activate a license, any previously active license is deactivated. You cannot activate expired or released licenses.

6. Your current session will be logged out. Log in to SANnav and return to the SANnav Licensing window. Check the license status, as shown in Figure 4-34.

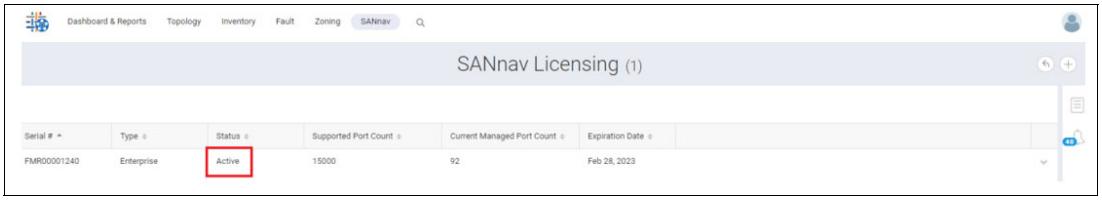


Figure 4-34 Active license

4.3.4 Rehosting a license on a different server: Planned migration

If you want to move SANnav from one server or VM to another one, you need a new license. Instead of purchasing a new license, you can use a rehost key to generate a license for the new server or VM.

Migrating a license from one SANnav instance to another is called *rehosting*. If you want to move SANnav from the current server or VM to another one, you must first release the current license. When you release the license, a rehost key is generated. You must provide the rehost key and the new server UID to get a license for the new SANnav instance.

For more information, see *Brocade SANnav Management Portal and Global View User Guide, 2.0.0*.

4.3.5 Moving a license to a different server: Unplanned migration

If the server on which SANnav is installed experiences a permanent hardware failure and can no longer be used, you can install SANnav on a new server with a replacement license.

Unlike a planned license migration, in this unplanned migration you cannot access SANnav and so you cannot get a rehost key. Instead, you must contact IBM Support or Broadcom directly to get a replacement license certificate. Complete the following steps:

1. Locate the license serial number for the original license.
2. Install SANnav on a new server and obtain the server UID.
3. Contact IBM Support and provide the license serial number and server UID to request a replacement license certificate.

   After you install SANnav on the new server, if you took a SANnav backup, you can restore the backup on the new server.

4.3.6 Deleting a license

You can delete inactive, expired, and released SANnav licenses by completing the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services SANnav Licensing** to view the license list.
2. Click the down arrow at the right of a license row, and then click **View** to display the license details window.
3. Click **Delete** to delete the license.

4.4 SANnav Management Portal backup and restore

Taking regular backups of SANnav Management Portal helps to protect the SANnav Management Portal data and configuration in a disaster, such as a server failure. You can create schedules for regular daily and weekly backups. You also can create a backup on demand, such as when you want to start a new SANnav server.

If SANnav data is deleted or corrupted or if you start a new SANnav server, you can restore the data from a previous backup. Restoring is done through the CLI and not through the SANnav user interface.

Notes:

- As a best practice, back up the file `ssh-keypair.ser` from `<Installation_Folder>/conf/security` before uninstalling the application. After reinstalling SANnav Management Portal, restore the backup file to the same location.
- The trial license does not support taking a backup of the SANnav environment.

4.4.1 Core backup (default)

The default backup file includes the following information:

- Fabric information
- Inventory data
- Server configuration
- Switch asset information
- Zone configuration

If a SANnav patch was applied, a folder for the patch is included in the backup file. If multiple SANnav patches were applied, only the latest patch folder is included in the backup. The patch folder increases the size of the backup file. During a restore operation, the latest patch is applied.

4.4.2 Optional backup

You can optionally select more information to include in the backup:

- Product, port, and telemetry data
- Events
- Reports

SANnav does not purge older backups. Make sure to check the disk space periodically and delete those backup files that you do not need.

SANnav Management Portal does not back up any firmware files that were imported into the repository. After the backup file is restored, you must import the firmware files again by selecting **SANnav** → **SAN Configuration** → **FOS Version Management** → **Repository**.

Before starting a backup, ensure that the SANnav Management Portal services are working. You can use the **`check-sannav-status.sh`** script, which is in the `<install_home>/bin` folder on the SANnav server.

The best practices for backup are shown here:

- Perform a full backup weekly because a daily full backup might slow down the server.
- Make sure that your backup location has enough disk space before you back up your data.
- Make sure that your backup location is different from the location where SANnav Management Portal is installed.
- For scheduled backups, occasionally check whether the backup data size has any abnormal patterns, such as some files being too large or too small.

4.4.3 Configuring a backup file location

Before you can back up SANnav, you must configure a location where the backup files will be saved. You can configure up to two locations, but you must configure at least one.

The following rules apply to both locations:

- The backup locations must be accessible from the SANnav server.
- The backup locations must have enough disk space to accommodate the backup files.

Also, note the following best practices for backup locations:

- The backup location should be an accessible path on the server on which SANnav is installed, but it should be different from the actual installation folder.
- You can specify a location on your local machine or on external storage. If the location is on external storage, the external storage should be mounted locally.
- Make sure that you check the disk space periodically so that your backups are successful.

To configure one or two backup locations, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services** → **SANnav Backup**.
2. In the Backup Location field, enter the Linux location where you want to save the backup file.
3. In the Alternate Backup Location field, enter another Linux location where backup files can be saved.
4. Click **Validate All Locations**.

   A green checkmark indicates that the location is valid, as shown in Figure 4-35. If both locations are invalid, you must provide a valid location before continuing.

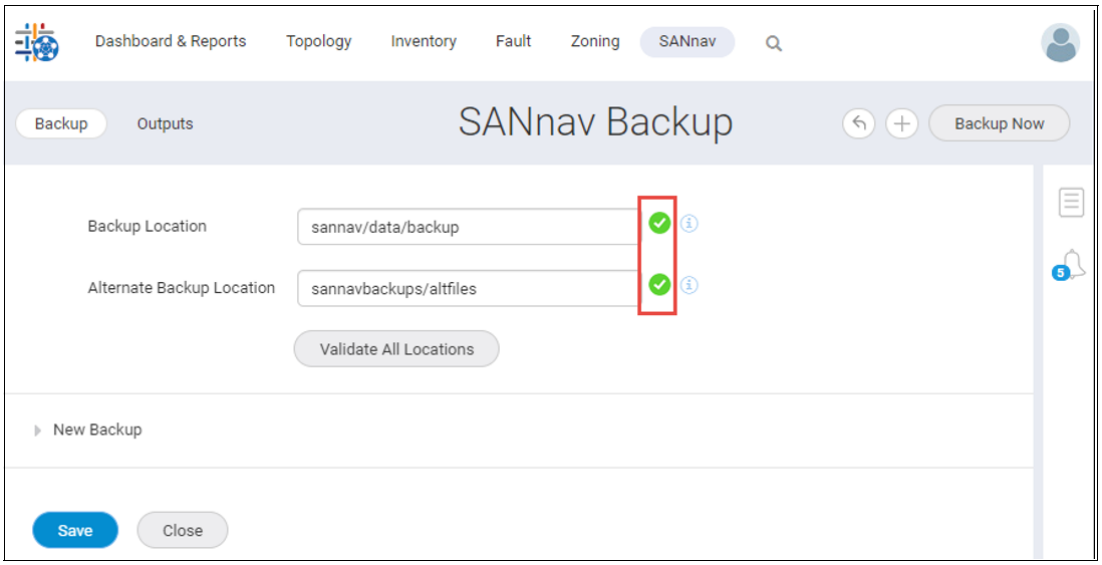


Figure 4-35 Backup location

5. Click **Save**.

   These locations can now be selected when you perform SANnav backups.

4.4.4 Configuring a scheduled backup

You can schedule up to two backups of the SANnav server data. For example, you can schedule a daily backup and a weekly backup.

When scheduling a backup, you specify a location for the backup file to be saved, and the time for the backup to start. You can save the backup file on your local machine or on external storage. The external storage should be mounted locally. Make sure that you check the disk space periodically so that your scheduled backups are successful.

The following steps create two backup schedules: a daily backup that includes database and configuration files, and a weekly backup that also includes historical statistics, events, and reports.

1. Click **SANnav** in the navigation bar, and then select **Services** → **SANnav Backup**.
2. Select the **New Backup** drop-down menu and enter a name for the backup.
3. Select the backup location from the **Location** drop-down menu.
4. Select **Daily** from the **Backup** drop-down menu and enter the start time for the daily backup. By default, the backup includes database and configuration files.
5. Select **Enable** to activate the backup and click **Save**.

   Figure 4-36 shows the backup window.

Tip: If **Save** is not active, check that you specified a name and selected a location for the backup.

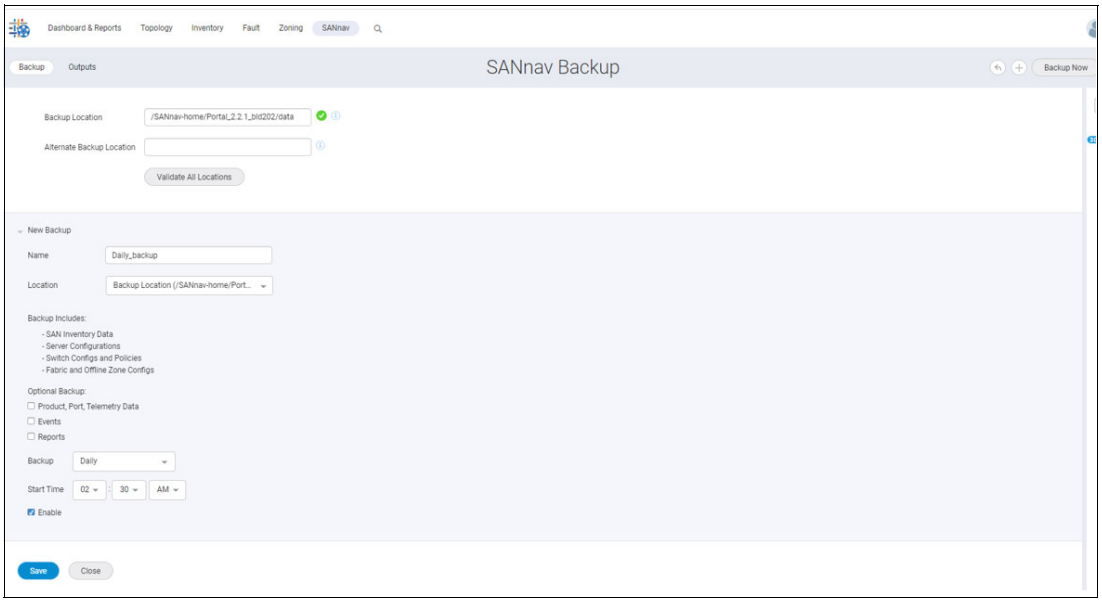


Figure 4-36 Scheduled daily backup

6. Click **+** at the upper right of the window to add another backup.
7. Enter the name for the second backup in the Name field.
8. Select a backup location from the list. The location can be different from the location of the first backup.
9. Select **Weekl**y from the **Backup** drop-down menu, and then select the day and start time.

Note: There must be more than a 3-hour difference between the start times of the two backups. For example, if the daily start time is 00:30, the weekly start time must be set to more than three hours before or after the daily start time, for example, 9:30 PM or 3:30 AM. If you create two weekly backups, in addition to the three-hour time difference, the weekly backups must start on two different days.

10. Check **Enable** to activate the second scheduled backup, and click **Save**, as shown in Figure 4-37.

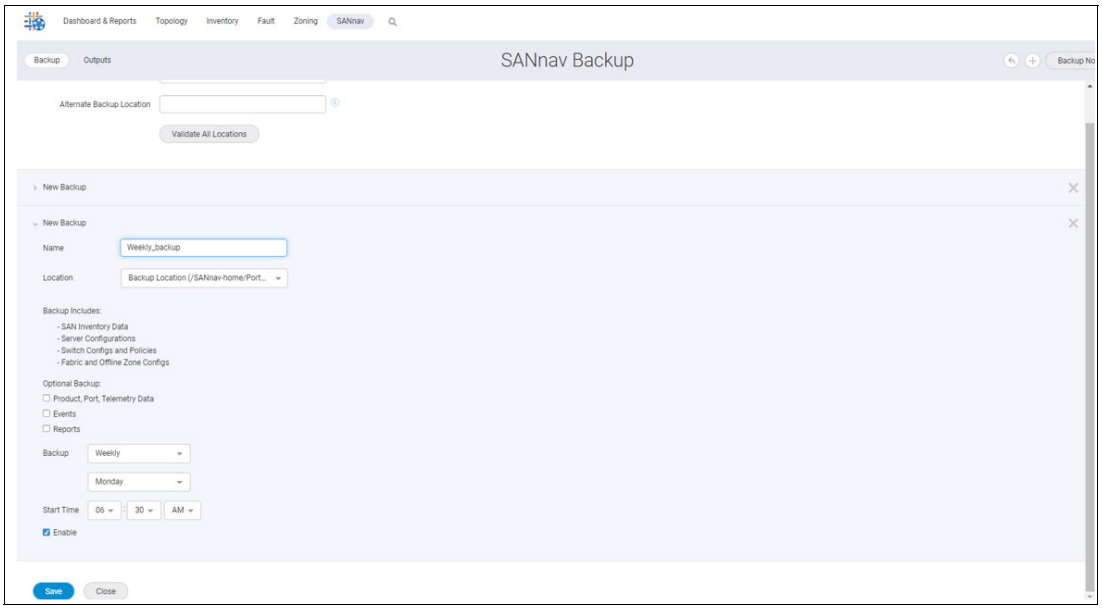


Figure 4-37 Scheduled weekly backup

Notes:

- You must enable each scheduled backup to generate that backup.
- You can create a maximum of two scheduled backups. You can schedule one weekly backup and one daily backup, or you can schedule two weekly backups. You cannot schedule two daily backups.

SANnav verifies the storage location and starts the backup as scheduled. The backup files are saved as a `.tar.gz` file in the specified location. The **Outputs** tab lists the completed scheduled backups that are present in the current schedule location.

Notifications are sent when the backup completes or if the backup fails.

11. If you want to delete a scheduled backup, click the **X** that is on the right side of the schedule name. You cannot delete the last backup, but you can clear the **Enable** checkbox to disable it.

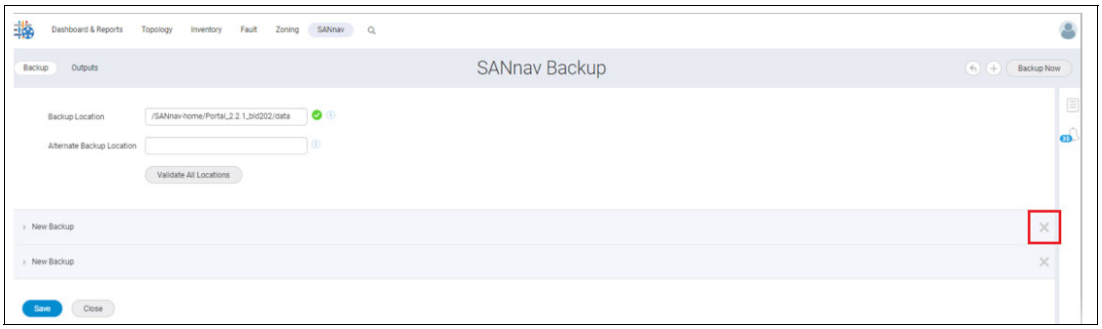


Figure 4-38 Deleting a backup

4.4.5 Backing up manually

You can back up the SANnav server data at any moment to save the latest configurations. For example, you can back up the application before you update the SANnav version.

If the upgrade does not complete successfully or if the existing data is corrupted or deleted, you can use the backup file to restore your data.

To do a manual backup, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services** → **SANnav Backup**.
2. Click **Backup Now** at the upper right of the window.

   The Backup dialog box opens. The Backup Location field is automatically populated with the scheduled backup location. If no scheduled backups are configured, this field is empty.
3. If the Backup Location field is empty or if you want to change the backup location, enter the location where you want to save the backup file and click **Validate Location**.

Note: The backup location must be accessible from the SANnav server.

   A green checkmark indicates that the location is valid.

   If a backup location has already been configured (see 4.4.3, “Configuring a backup file location” on page 87), select the backup location from the **Location** drop-down menu.
4. Select **Optional Backup** checkboxes if you want to back up more data.
5. Click **OK**, as shown in Figure 4-39.

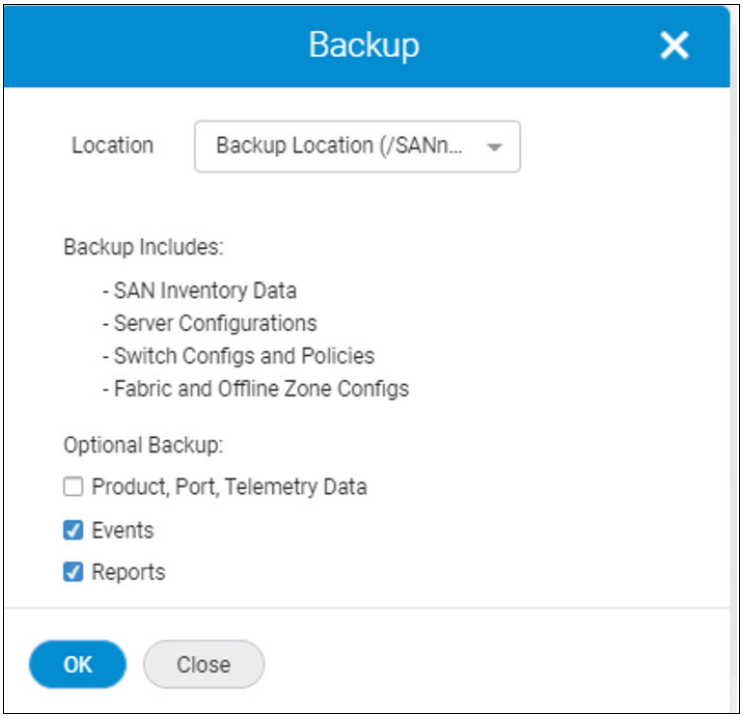


Figure 4-39 On-demand backup

The backup starts immediately. The backup files are saved as a `.tar.gz` file in the specified location. **Backup Now** is disabled while the backup is in progress.

6. You can view the list of on-demand backup files in the **Outputs** tab. Notifications are sent when the backup completes or if the backup fails.

4.4.6 Managing and deleting SANnav backup files

Backup files can use much disk space. Periodically check the list of saved backups and delete the ones that you do not need. You can delete backup files on demand, or you can schedule a backup file to be deleted at a future time.

To manage or delete the files, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services** → **SANnav Backup**.
2. Click the **Outputs** tab, as shown in Figure 4-40.

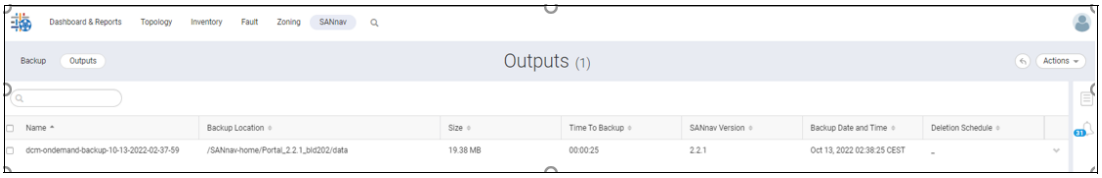


Figure 4-40 Listing the backup files

3. To see the list of items that are included in the backup, click the down arrow to the right of a table entry and select **Show Details**, as shown in Figure 4-41.

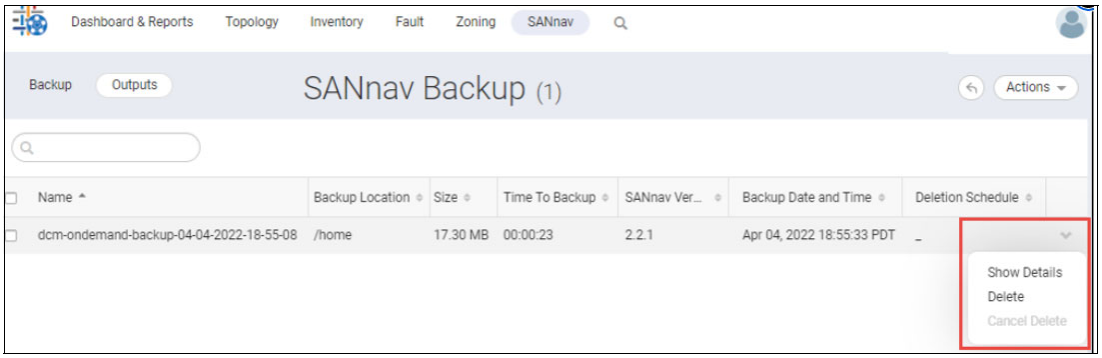


Figure 4-41 Managing backup files

Figure 4-42 on page 93 shows the Backup details window.

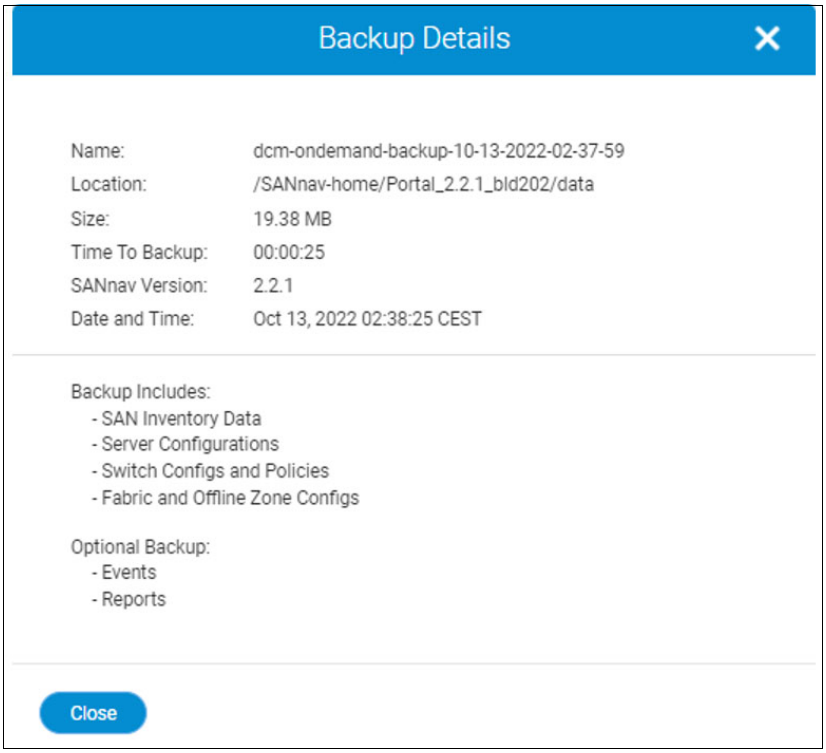


Figure 4-42 Backup details

4. To delete a backup file, click the down arrow and select **Delete**. You can also select multiple backup files and select **Delete** from the **Actions** menu in the upper right.
5. To delete a backup file that is not scheduled for deletion, complete the following steps:
   a. Click the down arrow and select **Delete**. You can also select multiple backup files and select **Delete** from the **Actions** menu in the upper right.
   b. Select either **Delete Now** or **Delete Later** in the Delete dialog box.

If you select **Delete Later**, you must select the date and time when the backup files will be deleted, as shown in Figure 4-43.

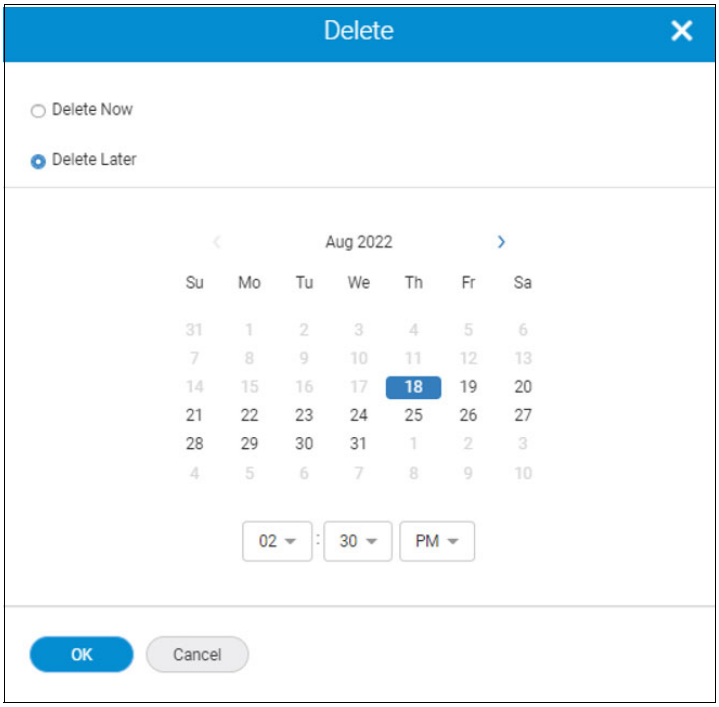


Figure 4-43 Delete Later scheduled backup

c. Click **OK** in the confirmation dialog box.

Deleted backup files are removed from the SANnav Backup window. For backup files that are scheduled for deletion later, the Deletion Schedule column indicates the date and time when the files will be deleted. This column is empty if the backup files are not scheduled for deletion.

6. To cancel a future backup file deletion, click the down arrow and select **Cancel Delete**.

The Cancel Delete option is available only when a deletion is scheduled.

Application events are raised if you delete a backup file, schedule a backup file for deletion later, or cancel a backup file deletion.

4.4.7 Restoring SANnav backup files

Restoration is done by using a CLI script. You cannot use the SANnav user interface to restore the backup files.

The restoration process stops all SANnav services, restores the data from the backup files, and then restarts the SANnav services. The restoration time depends on the size of the backup file.

Before you start the restore process, ensure that all users log out of SANnav.

The following points apply to the restore process:

- During a restore process, the ports that are configured in the backup server are carried over to the restore server. SANnav provides custom port input if the existing ports are unoccupied.
- SANnav does not restore custom certificates, so you must manually reconfigure the custom certificates after the restore is complete.
- SANnav does not restore the license or any license-related attributes, such as port count and expiration date. The license on the restore server remains the same after the restore process completes.

Restrictions for restoration

The following items are restrictions for restoration:

- Both the backup server and the restore server must have the same SANnav version and build.
- Both the backup server and the restore server must have the same IP configuration type (IPv4 or IPv6).
- Patch versions can be different on the backup server and the restore server if the main version is the same. The patch version of the backup must be later than or the same as the patch version of the restore server. For example, you can restore a v2.2.xb backup on a v2.2.xa server.
- If disaster recovery (DR) is enabled, you cannot restore a backup on the primary node or on the standby node. A backup that is collected from the primary node is intended to be restored on a different SANnav instance.

The backup server and the restore server do not need to be the same installation type. You can take a backup from either an Open Virtual Appliance (OVA) installation or a non-OVA installation and restore it to either an OVA installation or a non-OVA installation.

To restore the backup file by using a CLI script, complete the following steps:

1. Log in to the SANnav server and go to `<install_home>/bin/backuprestore`. Log in by using an account with administrator privilege.
2. Run the **`./restore.sh`** script and provide the full path to the backup file, including the file name.

   The backup file must be a `.tar.gz` file that was previously generated from the SANnav user interface. The backup file contains a checksum file, which ensures that the file is not corrupted and is a valid backup file.

   Example 4-3 shows an example of the **`./restore.sh <backup_file_path>`** command.

Example 4-3 Example restore command

```
[root@SANNAV10 backuprestore]# ./restore.sh
/SANnav-home/Portal_2.2.1_bld202/data/dcm-ondemand-backup-10-13-2022-02-37-59.tar.
gz
################################################################################
#######################
##                                  RESTORE
##
################################################################################
#######################

Important: Log out all clients before the restore operation.
```

```
This operation is going to bring down all services and restore the specified
backup.
Do you want to continue? (Y / Yes / N / No): [No]
Y

User accepted. Starting restore operation.

Do you want to restore certificates? (Y / Yes / N / No): [No]
Y

User accepted. Certificates will be restored.

Do not interrupt the restore process. Press Enter to continue.


Stopping all services except postgres before the restore operation.
Not stopping dcm_2_2_1_dcm-postgres-db

Going to sleep for 2 minutes for services to scale down.

Checking if PostgreSQL service is ready...
9.155.122.139:5432 - accepting connections
PostgreSQL service is ready.

Dropping PostgreSQL dcmstats and dcm schemas...
Schema drop operation completed.

Restoring PostgreSQL core schema...
Restore operation completed for PostgresSQL core schema.


Dropping PostgreSQL Events and Map Events tables...
Events & Maps Events tables drop operation completed.
Restoring Events and Map Events Database...
Restore operation completed for PostgresSQL Events and Map Events Database.

Restoring reports...

Restore operation completed for reports.


Restoring mediation database...

Restore mediation database completed.

Going to restore compose and configuration files...
Current host UUID and backup UUID are equal.

Restoring kafka certificates.

Restoring software ID tag...

Restore operation completed for software ID tag.
Restoring the northbound streaming certificates...
```

```
Restore operation completed for compose and configuration files.
55ed009a618a

Removing Docker stack...
Creating keystore truststore secret.
Created keystore truststore docker secrets for kafka.

Port 443 is not in use. Assigning port 443.

Port 22 is not in use. Assigning port 22.

Port 162 is not in use. Assigning port 162.

Port 514 is not in use. Assigning port 514.

Port 6514 is not in use. Assigning port 6514.

Port 5432 is not in use. Assigning port 5432.

Starting the server...
Checking that all ports required for SANnav Management Portal are free. This
operation can take up to 15 seconds.
No Patching Required.
Note: License will not be restored, user has to manually apply the license after
the restore operation.
The server is successfully restored and started. Server startup may take up to 15
minutes. To check the server status, run
/SANnav-home/Portal_2.2.1_bld202/bin/check-sannav-status.sh. Launch the client
using [https://9.155.122.139].
```

3. If you also want to restore self-signed and third-party certificates, respond `Yes` when prompted. The default is to *not* restore certificates.
4. When the restore is complete, wait a few minutes for the SANnav services to start. You can check the status of the services by using **`check-sannav-status.sh`** script:

   ```
   [root@SANNAV10 bin]# ./check-sannav-status.sh
   SANnav server is Healthy. All the services are currently in running state
   ```

5. If the backup server and the restore server are different, after the restore you must stop and restart monitoring of the discovered fabrics for SNMP and Syslog registration with the restore server IP address.

Note: If you restore certificates from one server to another one, you must maintain the same FQDN on the restored server as that of the backup server. If the common name is different on both servers, the browser issues a warning message the next time you log in to the SANnav client.

4.4.8 IBM Call Home

You can use the IBM Call Home feature to send an email alert to one or more support centers to report problems that are based on events that are configured on FOS devices.

When an IBM Call Home event is triggered, SANnav Management Portal automatically collects product status information and sends an email for faster fault diagnosis, isolation, and remote support operations. You can also enable a supportsave action for an IBM Call Home event. When the event occurs, the location where the supportsave data is stored is sent by email. In addition, some Monitoring and Alerting Policy Suite (MAPS) and application events are identified as IBM Call Home events.

SANnav supports configuring a buffer time to trigger an IBM Call Home email for the “switch not reachable” event. If the buffer time is configured, SANnav does not trigger an IBM Call Home email immediately for the temporary reachability loss of switches.

Note: A new property `callhome.notification.interval` was introduced to configure the buffer time for an IBM Call Home email. You can configure this property by using the **`update-callhome-notification-interval.sh`** script. You can configure the buffer time 15 - 720 minutes. If you want to revert the configuration, you can configure buffer time as zero.

SANnav receives “switch not reachable events” and does not trigger the IBM Call Home email until the configured interval time. After the configured interval time expires, the IBM Call Home email is triggered based on the switch status. An IBM Call Home email is triggered if the switch is not reachable even after waiting for the configured interval time. If the switch is reachable within the configured interval time, the IBM Call Home email is not triggered.

The following support centers are predefined in SANnav for IBM Call Home:

- Brocade Email
- IBM Email
- Dell EMC
- NetApp Email

For more information about how to configure IBM Call Home, see Configuring IBM Call Home Notifications.

4.5 User management

Access to SANnav is controlled by authentication and authorization of users. Authentication is the process of validating usernames and passwords. Authorization is the process of validating the roles, privileges, and areas of responsibility (AORs) for each user.

You can configure SANnav to perform authentication and authorization locally or by using an external server (such as Active Directory LDAP Server or Computer Associates LDAP Server, Active Directory Global Catalog, Remote Access Dial In User Service (RADIUS), or Terminal Access Controller Access-Control System Plus (TACACS+)).

User management involves the following general steps:

- Configuring password policies
- Creating roles
- Creating AORs
- Setting up user accounts

4.5.1 Configuring password policies

You should configure password policies first because when you create user accounts, you assign a password to the account, and you must assign passwords that conform to the password policies. The password policies are applicable for SANnav users only when you select primary authentication as the local database.

4.5.2 Creating roles

You can create custom roles to use in addition to the preconfigured roles that are provided by SANnav. If you create custom roles, you should do so before setting up the user accounts because you assign roles when you create the accounts.

4.5.3 Creating AORs

You can create custom AORs to use in addition to the preconfigured AOR (All Fabrics) that is provided by SANnav. If you create custom AORs, you should do so before setting up the user accounts because you assign AORs when you create the accounts.

4.5.4 Setting up user accounts

When you create a user account, you assign a password, roles, and AORs to that account.

For more information about user management, see User Management.

4.6 Stopping and restarting SANnav

If you must perform maintenance on the physical server or move the server from one rack to another, you must first shut down SANnav gracefully. To do so, complete the following steps:

1. Log in to the SANnav server and go to `<install_home>/bin`.
2. Log in by using an account with administrator privileges. You also can use **`sudo`**.

3. Run the **sannav-management-console.sh** script. You are presented with a list of options from which to choose, as shown in Example 4-4.

Example 4-4 The sannav-management-console.sh script

```
Select an option to execute and press Enter:
  1) Check SANnav status
  2) Restart SANnav
  3) Stop SANnav
  4) Start SANnav
  5) Show SANnav configuration
  6) Show opensource code attribution
  7) Update SANnav configuration
ESC) Press Esc and Enter to exit
```

4. Select the `Stop SANnav` option. The output that is shown in Example 4-5 appears.

Example 4-5 Stop SANnav option

```
Are you sure you want to stop SANnav? (Y / y / N / n): [Y/y]y
Stopping SANnav Management Portal services.
```

5. Check the SANnav status by using option 1 to ensure that SANnav is down.
6. To start SANnav, run the same script and select the `Start SANnav` option. The output that is shown in Example 4-6 appears.

Example 4-6 Start SANnav option

```
Starting SANnav Management Portal services.
 [|]
SANnav Management Portal services started successfully.
SANnav Management Portal server has been successfully started.
SANnav Management Portal server startup may take up to 15 minutes.
To check SANnav Management Portal server status, run
/SANnav-home/Portal_2.2.1_bld202/bin/check-sannav-status.sh
When startup has completed, launch the client using [https://9.155.122.139].
```

7. Wait 15 minutes and check whether all services are running by using option `1) Check SANnav status`. You should see the following output:

   ```
   SANnav server is Healthy. All the services are currently in running state
   ```

4.6.1 Scripts for managing the SANnav Server

When you run these scripts, SANnav services must be running. You can check that all services are running by using the script **check-sannav-status.sh**.

All scripts are in the `<install_home>/bin folder` (for example, `/SANnav/Portal_2.2.0_bld374/bin`).

All scripts include a **- - help** parameter, which shows detailed usage guidelines for the script. Figure 4-44 on page 101 shows an example.

```
[root@vm-sannav2 bin]# ./install-sannav.sh --help
NAME:
  install-sannav.sh - Installs the SANnav server

DESCRIPTION:
Use this script to install the SANnav server.

The SANnav server is installed on a single node. Multi-node installation is not supported.

This script first checks that a number of prerequisites are met, such as available disk space, memory, CPU speed, number of CPUs, and whether port 80 is free.
If any check fails, the installation exits with error messages. If this happens, you must fix the reported issues, uninstall the application, and then re-run this script.
If all of the prerequisite criteria are met, then installation proceeds.

This script next installs Docker and enables the Docker swarm cluster.

This script prompts you for the following customization options:
  * IPv4-only installation or IPv4 and IPv6 installation
  * Allow or Disallow HTTP port 80 to HTTPS redirection
  * Server-to-switch communication preference (HTTP or HTTPS)
  * Server-to-switch single sign-on preference
  * Customized ports (for syslog, SNMP traps, and more)
  * Default database and internal SFTP/SCP passwords
  * Default license auto-renewal
  * Allow usage data collection to be sent to Broadcom

After the installation completes, SANnav starts after a few minutes.

ARGUMENTS:
  Mandatory: None
  Optional: --help   Display this help and exit.

EXAMPLES:
  ./install-sannav.sh --help
```

Figure 4-44 The check-sannav-status.sh script

Another useful script is **`./sannav-management-console.sh`**.

You are presented with a list of options from which to choose, as shown in Figure 4-45.

```
[root@vm-sannav2 bin]# ./sannav-management-console.sh

Select an option to execute and press enter:
  1) Check SANnav status
  2) Restart SANnav
  3) Stop SANnav
  4) Start SANnav
  5) Show SANnav configuration
  6) Show opensource code attribution
  7) Update SANnav configuration
(ESC) Press Esc and Enter to exit
```

Figure 4-45 ./sannav-management-console.sh script

5

Main features

This chapter describes the main features of SANnav with several examples and best practices.

This chapter includes the following topics:

- Licensing
- Configuration management
- Chassis password management
- Policy-based configuration
- Configuration backup and restore
- Managing zoning in SANnav
- Dashboards
- Investigation Mode
- Reports
- Fault Management

5.1 Licensing

When you install SANnav, you have a 30-day trial period during which you can use SANnav at no charge without a license. To use SANnav beyond the trial period, you must purchase a software license.

Note: The 30-day trial period is activated automatically and starts from the time that you install the SANnav product.

SANnav licenses are subscription-based, which means that they expire at the end of the subscription period. If the license expires, you cannot log in to SANnav unless you provide a new license certificate. Before your license expires, you should renew the license to ensure uninterrupted service. By default, during installation SANnav is configured to automatically retrieve and activate renewed licenses.

SANnav Management Portal and IBM SANnav Global View are two separate products, which require separate license certificates and are independent in terms of licensing.

When you install SANnav, whether on a server or on a virtual machine (VM), a server unique ID (UID) is generated for that SANnav instance. The server UID and the transaction key are used to generate a SANnav license. The license is locked to that server UID and SANnav instance.

Note: SANnav v2.2.0 and later use a license certificate (XML file). Earlier versions of SANnav use a license key (text string). These license keys are not supported by SANnav v2.2.0 and later. During migration to SANnav v2.2.1 from SANnav 2.1.1, the existing license key is automatically converted to a license certificate.

For more information, see *Brocade SANnav Management Portal Installation and Upgrade Guide, v2.2.x*.

You need one license for every SANnav instance, and each license can be used on only one SANnav instance. For example, if you have multiple VMs on a single server and you install SANnav on every VM, each installation generates a separate server UID and requires a separate license. You cannot clone a VM and use the same license on the cloned VM.

If you must move a license from one SANnav instance to another one, for example, if you want to move the installation to a different server, you do not need to purchase a new license; you can “rehost” the license on the new SANnav instance.

5.1.1 SANnav licensing terminology

The following terms are used in this document:

License certificate An XML file that enables you to use a SANnav instance. A license certificate has an expiration date after which you can no longer use SANnav unless you renew the license. The license certificate is generated from the Broadcom licensing portal.

Rehost key A key that is used when you want to move the SANnav application from one server or VM to another one or when the MAC address of the server changes. The rehost key is generated by SANnav when you release the current license.

Server UID A unique ID that identifies the physical server or VM on which SANnav is installed. The server UID is used with a transaction key to generate and download a software license from the Broadcom licensing portal. The server UID is generated when you install the SANnav application. The server UID is not the same as the VMware UUID.

Transaction key A unique key, along with the server UID, which is used to generate a SANnav license from the Broadcom licensing portal. You obtain the transaction key from your vendor when you order a SANnav license.

5.1.2 SANnav license types

SANnav Management Portal supports two license types: Base and Enterprise. Both licenses support the same software feature set.

- The Base license enables management of up to 600 ports and can be used to manage fixed-port switches. The Base license cannot be used to manage directors or for disaster recovery (DR).
- The Enterprise license enables management of up to 15,000 ports and can be used to manage fixed-port switches and directors.

During the 30-day trial period, SANnav Management Portal has the same functions as the Enterprise license except that SANnav server backup and restore and DR are not supported.

5.1.3 How SANnav licensing works

Using a combination of the server UID and the transaction key, you can generate a license certificate to activate the SANnav license.

When you install SANnav on a server or VM, a server UID is generated. You can view this server UID and copy it from the SANnav Licensing window.

When you order a license, IBM provides you with a transaction key that is issued by Broadcom as fulfillment of your license purchase. The transaction key and server UID are used to generate a license certificate and license serial number from the Broadcom licensing portal.

After you obtain the license certificate, add it in SANnav, and activate the license. This flow is illustrated in Figure 5-1.

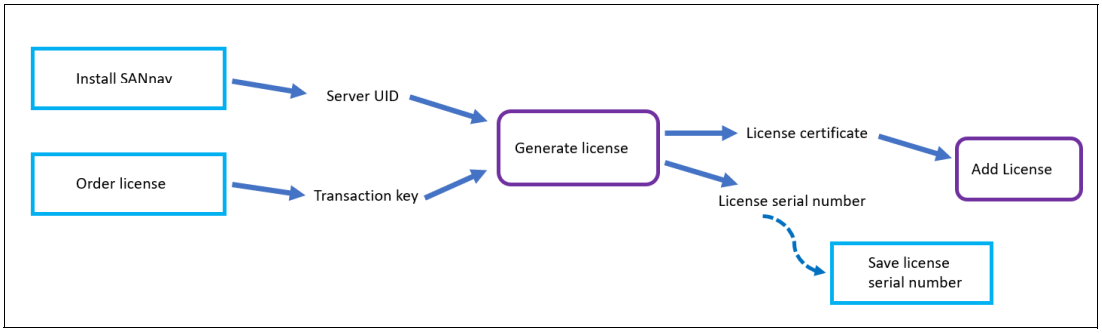


Figure 5-1 Licensing flow

Keep a record of the license serial number. You need the license serial number if you contact support. The license serial number can also be obtained from the Licensing window of the SANnav user interface.

5.2 Configuration management

SANnav applies consistent switch and monitoring configurations across environments with the policy-based configuration management feature, which allows users to view switches that experienced configuration drifts and examine what exactly changed in the environment. When such drifts occur, IBM SANnav Management Portal allows the administrator to rectify the problems by enforcing the configuration policy on the switches that are associated with the policy, which ensures operational stability and maximum uptime.

5.3 Chassis password management

SANnav allows you to manage switch passwords for multiple user accounts across multiple chassis. You can view the chassis user accounts for one or more selected chassis.

Note: Chassis password management is supported on platforms running Fabric OS (FOS) 8.2.1 or later.

To change the chassis password, you must have the Element Manager - Product Administration and Fabric Configuration privileges with read and write permissions.

5.3.1 Viewing a list of user accounts for a chassis

To view a list of user accounts for a chassis, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Security** → **Chassis Password Management**. The Chassis window opens with a filtered list of chassis running FOS 8.2.1 or later, as shown in Figure 5-2.

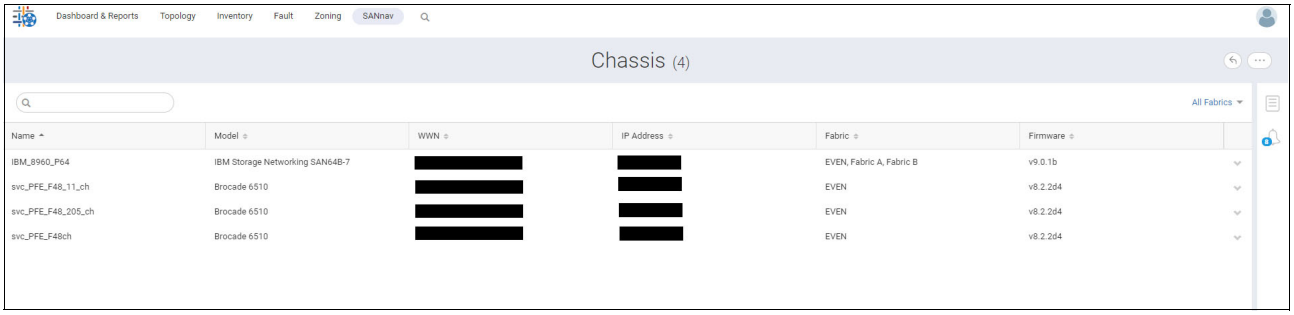


Figure 5-2 Chassis window

2. Click **View** from the action menu for the chassis. The chassis details window opens with a list of users. You can edit the chassis password for any user by selecting **Change Password** from the action menu, as shown in Figure 5-3 on page 107.

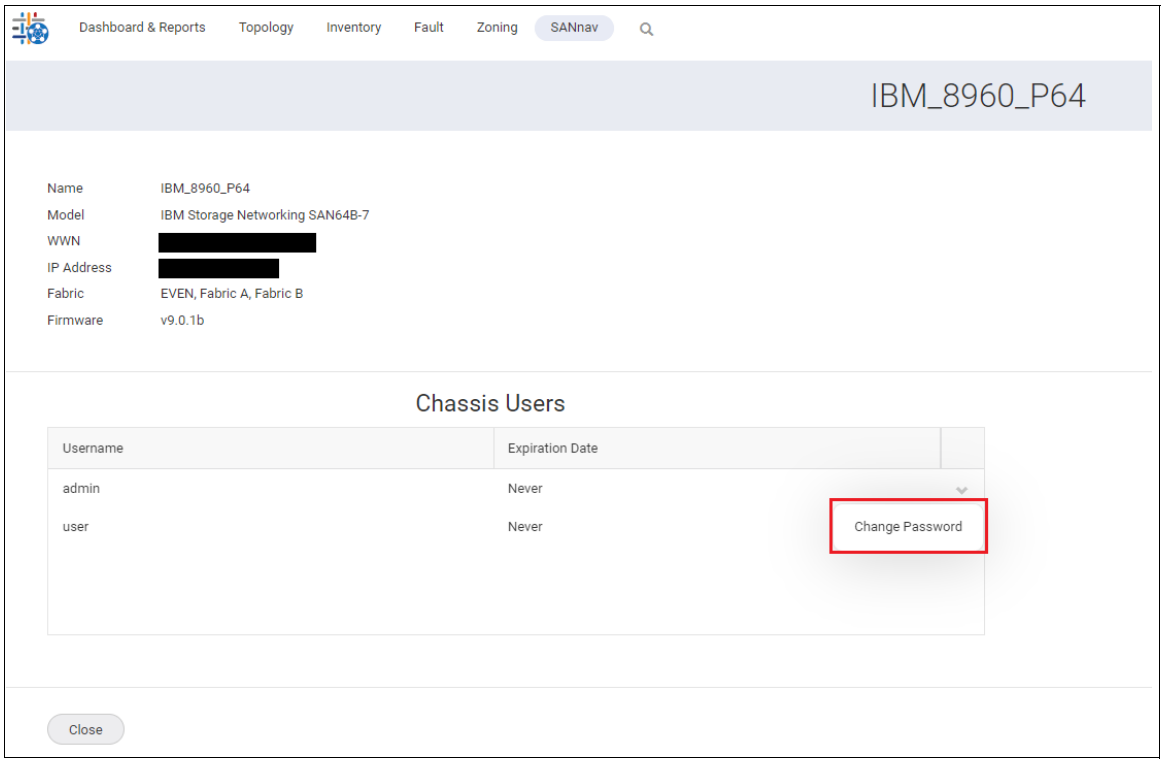


Figure 5-3 Change Password

Changing the chassis password for a specific user

To change the chassis password for a specific user, complete the following steps:

1. For admin users, enter the current password in the Old Password field.
2. Enter the new password in the New Password and Confirm fields and click **Change**. A “Password changed successfully” message appear, and a password change application event shows on the Events window when the event completes. Expand the event to show the event details. The SANnav Username field shows the name of the user who changed the password. If changing the password fails, a Details window opens with the reason why it failed.
3. Click **Close** on the chassis details window.

Changing the chassis password on a group of chassis

You can change the chassis password for all users on a group of chassis (up to 30 chassis) by using the **Bulk Edit** option. You can also change the chassis password for all users on a single chassis.

To change the chassis password on a group of chassis, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Security** → **Chassis Password Management**.
2. Click **More** (**...**) in the upper right of the window and select **Bulk Edit**. A column of checkboxes appears at the left of the table.
3. Select the checkbox for each chassis (up to 30) on which you want to change the user passwords.
4. Click the **Actions** drop-down menu and click **Change Password**. The Change Passwords window opens.

5. Click the username to change the password. This action changes the user password on each of the selected chassis. The Change Passwords window shows the common usernames on the group of chassis, as shown in Figure 5-4.

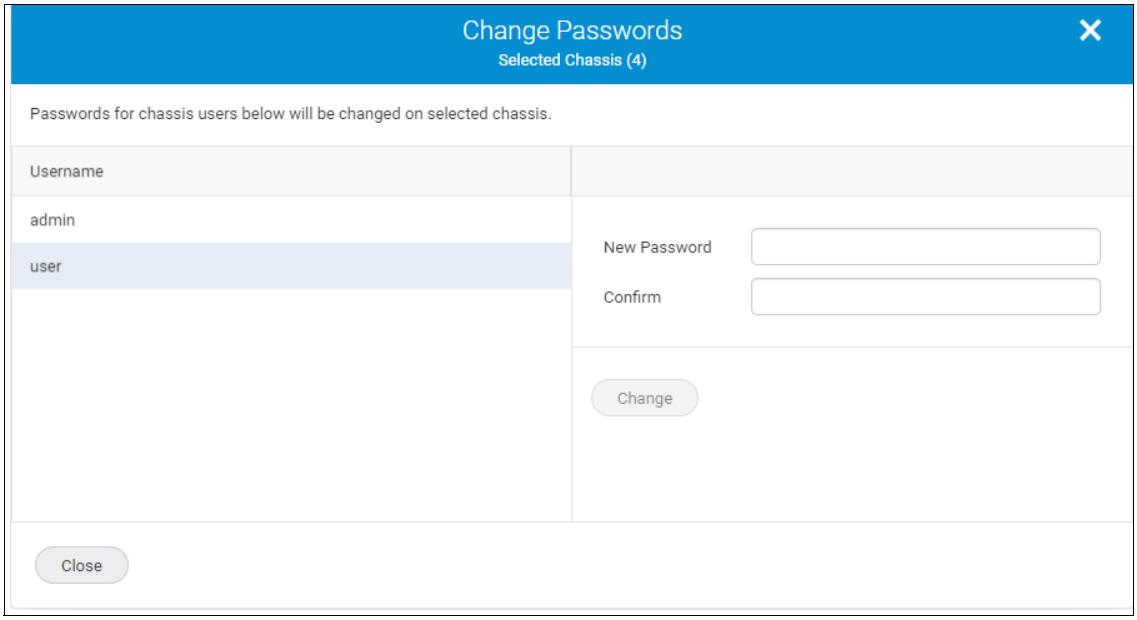


Figure 5-4 Changing the chassis passwords in bulk

6. For admin users, enter the current password in the Old Password field. If you discover a chassis that uses a non-admin user (for example, `admin1`) that has the `admin` role, you must enter your old password to complete the password change. However, when performing a bulk update, if `admin1` is not used for fabric discovery on some of the chassis, you are not prompted for your old password to change your password. In this instance, the password change fails on each chassis that uses the `admin1` user for fabric discovery.
7. Enter the new password in the New Password and Confirm fields and click **Change**. A “Password changed successfully” message opens, and a password change application event appears on the Events window when the event completes. If one or more of the chassis are unreachable, a Warning dialog box opens with a list of the unreachable chassis.
8. Repeat steps 4 on page 107 - 7 for each user whose password you want to change.
9. Click **Close** in the Change Passwords window.

5.4 Policy-based configuration

You must maintain consistent configuration settings on all switches in the same fabric because inconsistent parameters such as inconsistent PID formats can cause fabric segmentation.

The configuration policy feature in SANnav Management Portal allows you to make sure that all switches in the SAN conform to a defined configuration. SANnav can periodically check that the switches are conforming to the policy; identify switches that are not conforming; show the configuration drifts; and allow you to synchronize the switches to the policy.

A SANnav configuration policy contains a set of blocksets (which can be of type Basic Configuration and Monitoring and Alerting Policy Suite (MAPS) Policy) that can be associated with a set of switches. The SANnav configuration policy can be monitored or pushed on the associated switches.

Using the SANnav configuration policy, you can provision new switches and monitor switches for configuration drifts:

- Provisioning switches

  SANnav Management Portal makes provisioning new switches easier by allowing you to import configuration settings from one switch and save the configuration to multiple switches. For example, if you are setting up a fabric, you can define the configuration on one switch and then save that configuration to all other switches.

- Configuration drifts

  SANnav also allows you to monitor switches for configuration drifts, which are changes to the switch configuration that are different from what is defined in the configuration policy. The configuration policy does not need to be the entire configuration file, but only those configuration blocks that you are interested in monitoring for drifts. SANnav monitors configuration drifts at 15-minute intervals, that is, at the 0, 15, 30, and 45 minutes of every hour. Configuration drifts can be monitored through the Configuration Drifts widget.

A configuration policy represents the collection of configuration parameters of a switch. A single configuration policy can be applied to multiple switches. However, switches cannot modify the policy. You can create multiple configuration policies. A configuration policy is associated with blocksets that must contain unique blocks and associated products. The associated switches are a set of unique switches or access gateways.

5.4.1 Creating a configuration policy

You can use configuration policies to monitor switches for drifts in the configuration. You can also create a configuration policy for one switch and then apply the policy to multiple switches. To create a configuration policy, you must have the Configuration Policy Manager privilege with the read/write permission.

Before you create a configuration policy, you must determine how to use it:

- If you are going to use the configuration policy to monitor for drifts, you might want to create a policy with a subset of the full configuration to monitor only the configuration blocks of interest.
- If you are going to create a configuration policy for one switch and then apply the policy to multiple switches, you might want to create a policy with the complete configuration.

Think about applying policies to groups of switches. For example, all switches in Fabric A must conform to Policy A, or all directors must conform to Policy B, or all switches in the San Jose data center must conform to Policy C.

To create a configuration policy, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** → **Configuration Policies Management** → **Policies**. The Policies window opens.
2. Click **+**, and then select **Create New** to create a configuration policy. The Create New SANnav Policy window opens.
3. Enter a name, tags, and a description of the policy. The name can contain up to 32 alphanumeric characters and the underscore. The policy name must be unique.

4. Click **Add** from the **Blocks** list to associate blocksets to the policy. You can either add existing blocksets or create new blocksets.

   The Add Blocks window, as shown in Figure 5-5, shows a complete list of configuration blocksets, including incomplete draft blocksets. The incomplete or invalid draft blocksets are marked by red icons beside their names.

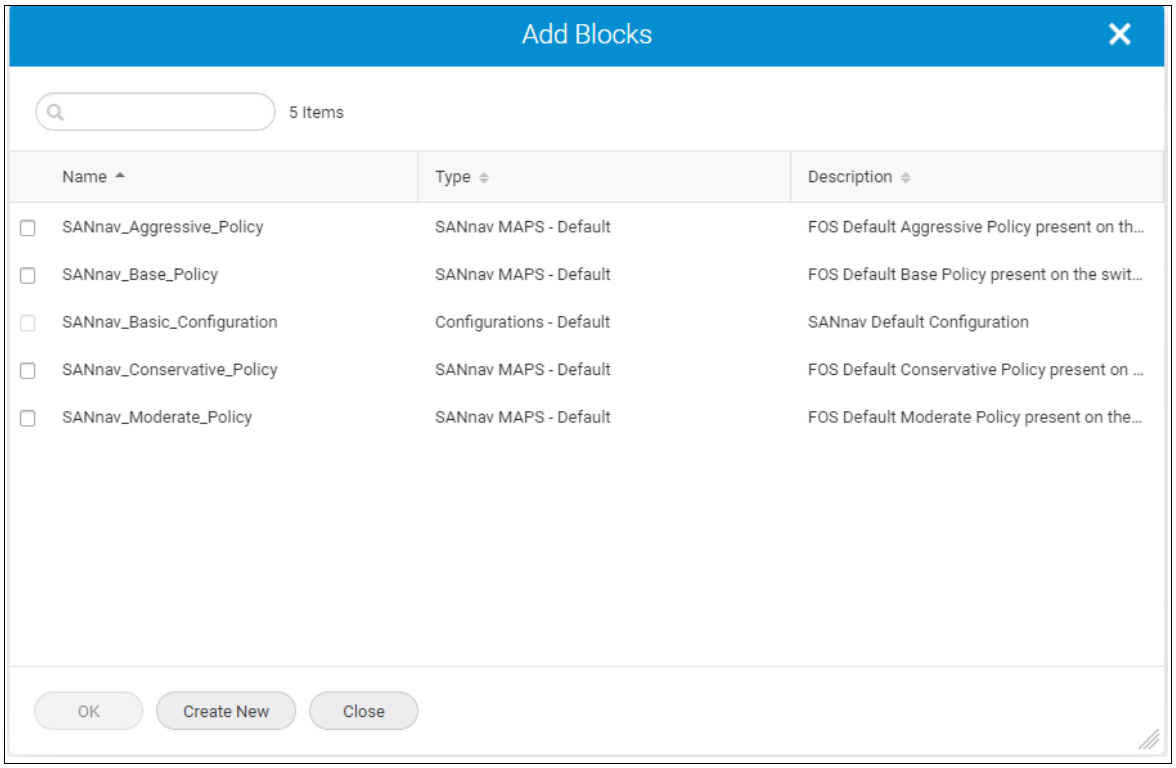


Figure 5-5 Add Blocks

5. If you want to add existing blocksets, select the blocksets that you want to associate with the policy, and click **OK**.

Notes:

- You cannot add the default SANnav Basic Configuration blockset to a policy configuration. However, you can customize the default blockset by cloning it, and then you can add it to the policy.
- SANnav does not support adding blocksets with the same block type. For example, if there are two blocksets with the FTP config block type, you cannot associate both of these blocksets to a policy.
- A policy can have both Basic Configuration and SANnav MAPS blocksets.
- Incomplete draft blocksets (blocksets with errors) cannot be associated with a policy.
- A switch can be by monitored by more than one policy with the same blocks. But the policy itself cannot contain the duplicate block. For example, a policy cannot contain two Basic Configuration blocksets with the FTP block in both of them.
- Unlike config blocksets, only one MAPS blockset can be added at one time.

6. If you want to create a block and then add it to the policy, click **Create New**. The Add Blocks window opens, as shown in Figure 5-6 on page 111.

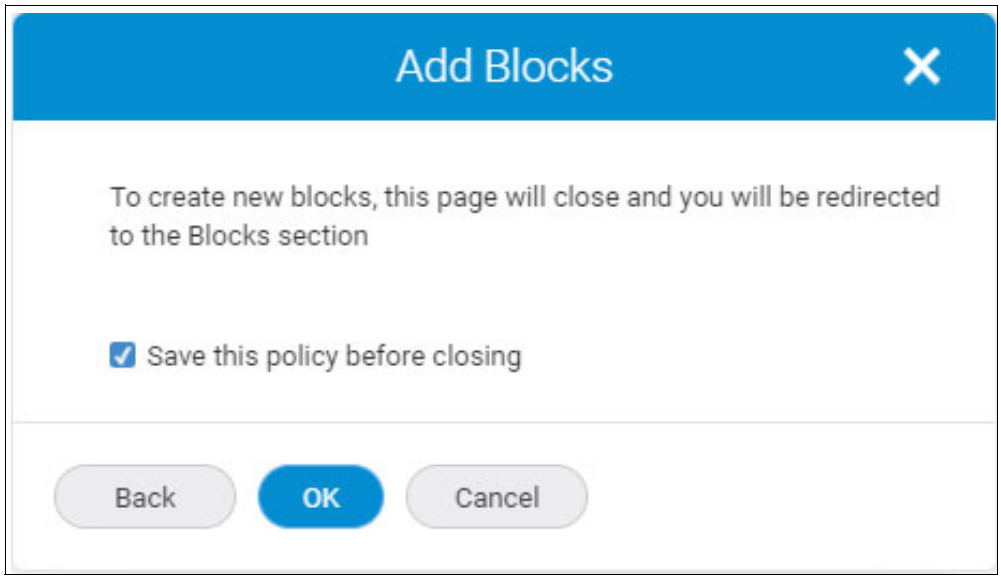


Figure 5-6 Add Blocks

7. Select the **Save this policy before closing** checkbox to save the policy, and then click **OK**. The window closes, and you are redirected to the Blocks window to create blocksets.

Notes:

- To set the password of the FTP configuration block for the switches with FOS earlier than Version 9.0.0, the password must be the switch encrypted password.
- The **Create New** option is disabled when you select existing blocksets from the Add Blocks window.

8. Apply the policy to switches by using the following steps:
   a. Click **Add** from the **Associated Switches** list.
   b. Select the switches to which the policy is to be applied, as shown in Figure 5-7.

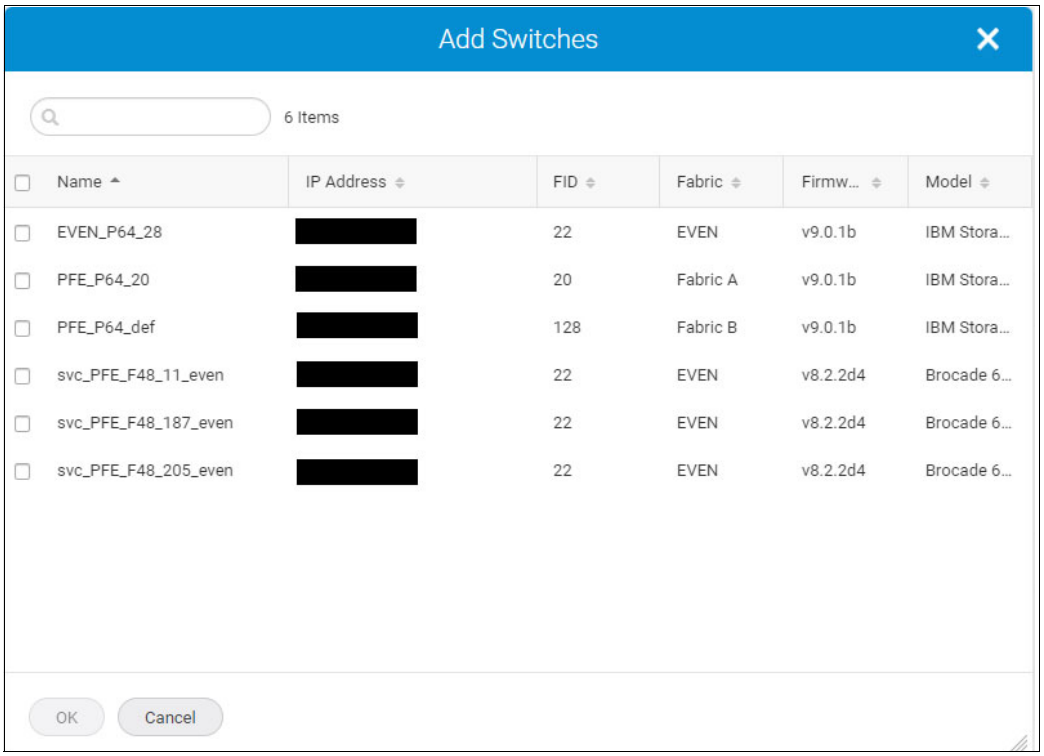


Figure 5-7 Add Switches

   c. Click **OK**.
9. Select the **Monitor** checkbox at the bottom of the **Create New SANnav Policy** window to monitor the policy for drifts. The **Monitor** checkbox is disabled if no switches or blocksets are associated with the configuration.
10. Click **Save** to save your changes and return to the Policies window, or click **Push to Switches** from the **Actions** menu to save your changes and apply the configuration to the associated switches. The **Push to Switches** option is disabled if no switches or blocksets are associated with the configuration. If pushing the configuration to the switches fails, the Push to Switches window shows the switch IP address, the status of the operation, and the reason for failure.

Notes:

- If the policy contains configuration blocksets that are not supported on the switch, SANnav filters such configurations and does not push them to the switch.
- SANnav does not support pushing a disruptive configuration to the switches. A disruptive configuration is only for monitoring purposes.

5.4.2 Managing a configuration policy

In the Policies window, you can view policy details. You can monitor or unmonitor a policy. You can also view the switches that are associated with a policy.

To manage a configuration policy, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** → **Configuration Policies Management** → **Policies**. The Policies window opens. You can view policies by selecting either the **Policy** list or the **Switch** list. By default, the **By Policy** option is selected.
2. You can do the following tasks when you view the **Policies** window by using the policy view option, as shown in Figure 5-8.

Figure 5-8 Managing policies

- To view the configuration policy details window, click the down arrow in the rightmost column of the configuration policy, and then select **View**.
- To monitor an existing unmonitored policy, click the down arrow in the rightmost column of the configuration policy that you want to monitor, and then select **Monitor**.
- To stop calculating drift for a policy, the policy must be unmonitored. To unmonitor an existing policy, click the down arrow in the rightmost column of the configuration policy that you want to unmonitor, and then select **Stop Monitoring**.
- To view drifts for a monitored policy, click the down arrow in the rightmost column of the configuration policy for which you want to view drifts, and then select **Show Drifts**. Monitoring configuration drifts is described in 5.4.3, “Monitoring configuration drifts ” on page 114.
- To view the switches that are associated with the policy, click the down arrow in the rightmost column of the configuration policy, and then select **Show Switches**.
- To delete a policy from the Policies window, click the down arrow in the rightmost column of the configuration policy that you want to delete, and then select **Delete**. You cannot delete a policy with the Monitored status from the Policies window. However, you can delete a policy from the Policy details window.

3. You can view the Policies window by the switch view option. You can filter switches from the **All Fabrics** drop-down menu. To view the configuration policies that are associated with a switch, click the down arrow in the rightmost column of the switch, and then select the **Show Policies** option, as shown in Figure 5-9.

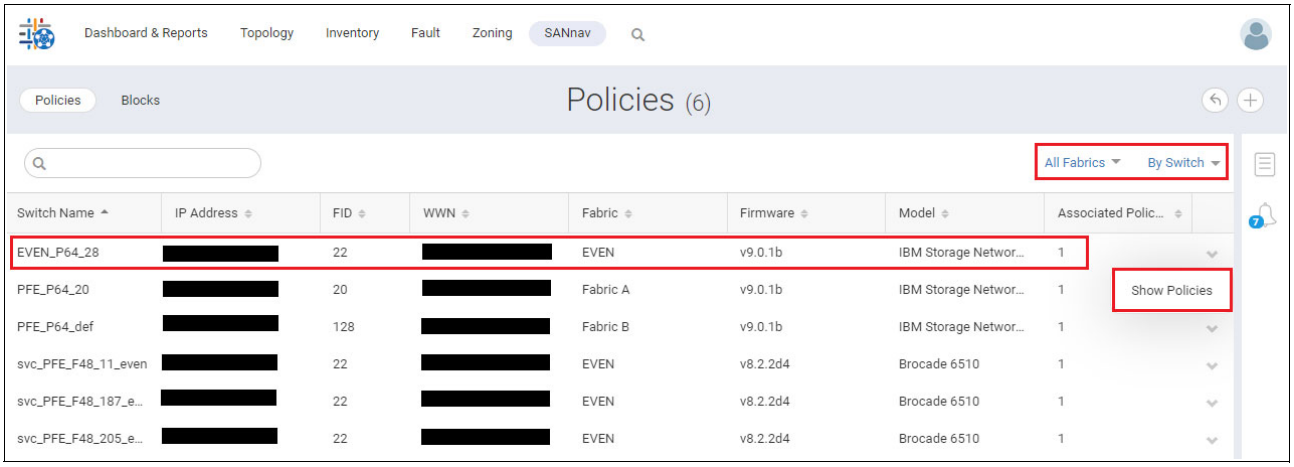


Figure 5-9 Show Policies By Switch

4. The Configuration Policies window opens and lists associated policies for a switch. Click the **View Policy** option from a policy. The selected policy details window opens, as shown in Figure 5-10.

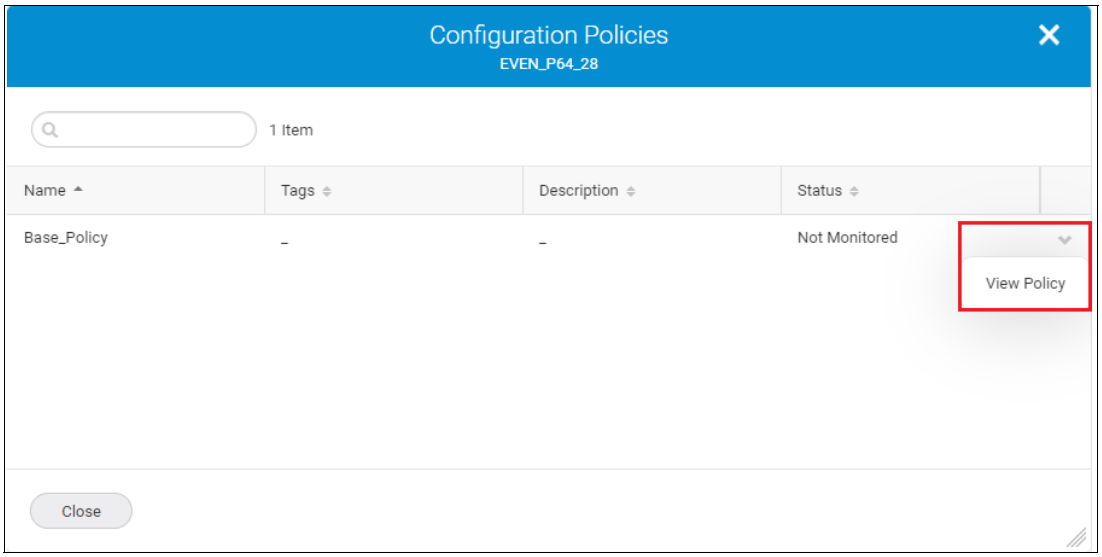


Figure 5-10 Configuration policies view

5.4.3 Monitoring configuration drifts

As part of your daily operations, you must check switches for drifts between the switch configuration and the configuration policy.

This task of monitoring configuration drifts assumes that configuration policies were created and are being monitored. To monitor the configuration for drifts, you must have the Configuration Policy Manager privilege with the read permission.

A policy must be monitored to calculate and find drifts for that policy. Enabling monitoring for a policy can be done from both the policy list window and the policy details window. A configuration drift generally means an uncontrolled change or an exception that happened on the switch. SANnav monitors switches for configuration drifts at 15-minute45 minutes45 minute of every hour.

Notes:

- The drift calculation is made based on the supported configuration blocks and the applicable parameters, which are part of the saved policy configuration.
- If a block is part of a blockset, and the blockset that is part of the saved policy is not supported on the switch, SANnav does not perform the drift calculation for that block. The calculation is skipped for that switch.
- If the switch where the drift calculation is required has an extra block compared to the saved policy, the block is not considered for the drift calculation, and the block is not listed in the Show Drifts window.

For a SANnav MAPS policy, drifts are calculated based on the respective metadata and performed based on the applicable rules:

- If the SANnav default MAPS blockset is pushed or monitored, the drift check is calculated based on the MAPS policy name on the switch.
- If a custom MAPS policy blockset is pushed or monitored, the drift check is calculated based on the following details:
  - If the active MAPS policy name on the switch is different from the MAPS blockset name in the SANnav configuration policy, the drift information contains the name difference, and no details about policy definitions are included.
  - If the active MAPS policy name on the switch is the same as the MAPS blockset name in the SANnav configuration policy, the drift information includes a list of all the differences that are encountered between policy definitions.
- For a default MAPS rule in a blockset:
  - If the rule is not available on the destination switch, the rule is skipped.
  - If the rule is available on the destination switch but the measure (Monitor) is not applicable, the rule is skipped.
  - If the rule is available on the destination switch with the applicable measure (Monitor), the rule is showed as a drift if it is not present in the active policy or if the rule content is different.
  - Only the group name, not the content of the group, is considered in the drift calculation.
- For a user-defined rule in a blockset:
  - If the category or measure name (Monitor) or time base (Monitor) of the rule is not supported in the switch, the rule is skipped from the drift calculation.
  - If the quiet time of the rule is less than the minimum quiet time (`minquietTime`) of the measure in the destination switch, the rule is skipped from the drift calculation.
  - Only the group name, not the content of the group, is considered in the drift calculation.
  - Drift calculations are performed only on the supported actions on the switch.

The following MAPS configurations are monitored as part of the complete policy configuration, and a drift is detected when the switch configuration and the SANnav configuration differ:

- Rule type
- Severity
- Measure
- Active policy
- MAPS action
- MAPS email settings
- Fabric Performance Impact (FPI) profiles and enabled FPI profiles for E_Ports and F_Ports
- Quiet time

Note: For a basic configuration, the password and secret property for the applicable blocks are not considered for drift detection.

To monitor configuration drifts, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** → **Configuration Policies Management** → **Policies**. The Policies window opens.
2. Check the Monitoring Status column of the Policies list to see a list of switches that are being monitored for configuration drifts. The Monitoring Status column is updated as Monitored after the policy is monitored. The Drift Status column indicates the drift status. After the policy is configured and monitored, it is scheduled for a drift check. If the drift calculation is not done, the Drift Status column shows a hyphen. If the policy configurations are in sync with all the associated switches and no drifts are seen, the status is In Sync. If policy configurations are not in sync with all the associated switches and drifts are detected, the status is `Drift Detected`. If the status is `Check Failed`, SANnav cannot contact the switch, or there might be other exceptions. If the policy configuration is in sync or not in sync with some of the switches and the drift check failed on some switches, the status is `Drift Detected, Check Failed`.
3. For switches with drifts, click the down arrow in the rightmost column and select **Show Drifts**. You can view the drifts of a specific existing policy after selecting the **Show Drifts** option for the specific policy, as shown in Figure 5-11.

Note: The Show Drifts window does not show switches and blocksets that are associated with the policy if there are no drifts.

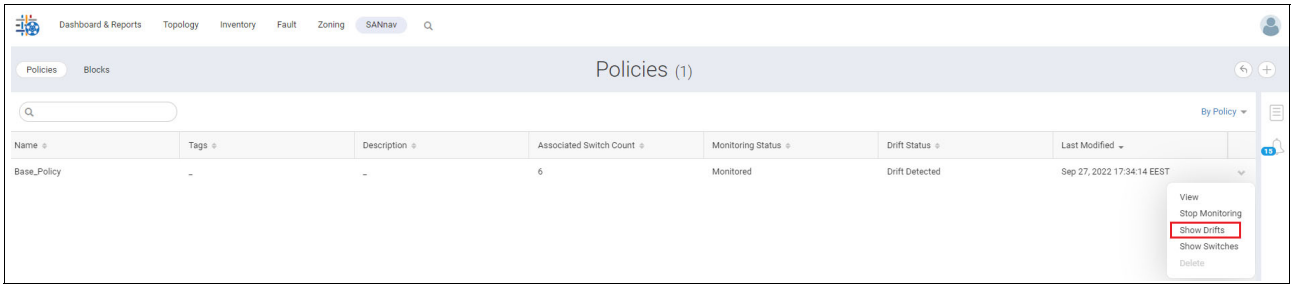


Figure 5-11 Show Drifts

The Show Drifts window shows switches that are associated with the policy and the blocksets with drifts.

4. Select a switch from the **All Switches** drop-down menu to view the drifts for the specific switch of the respective policy. By default, you can view drifts for all switches of the respective policy. Expand the configurations to view the drifts, as shown in Figure 5-12.

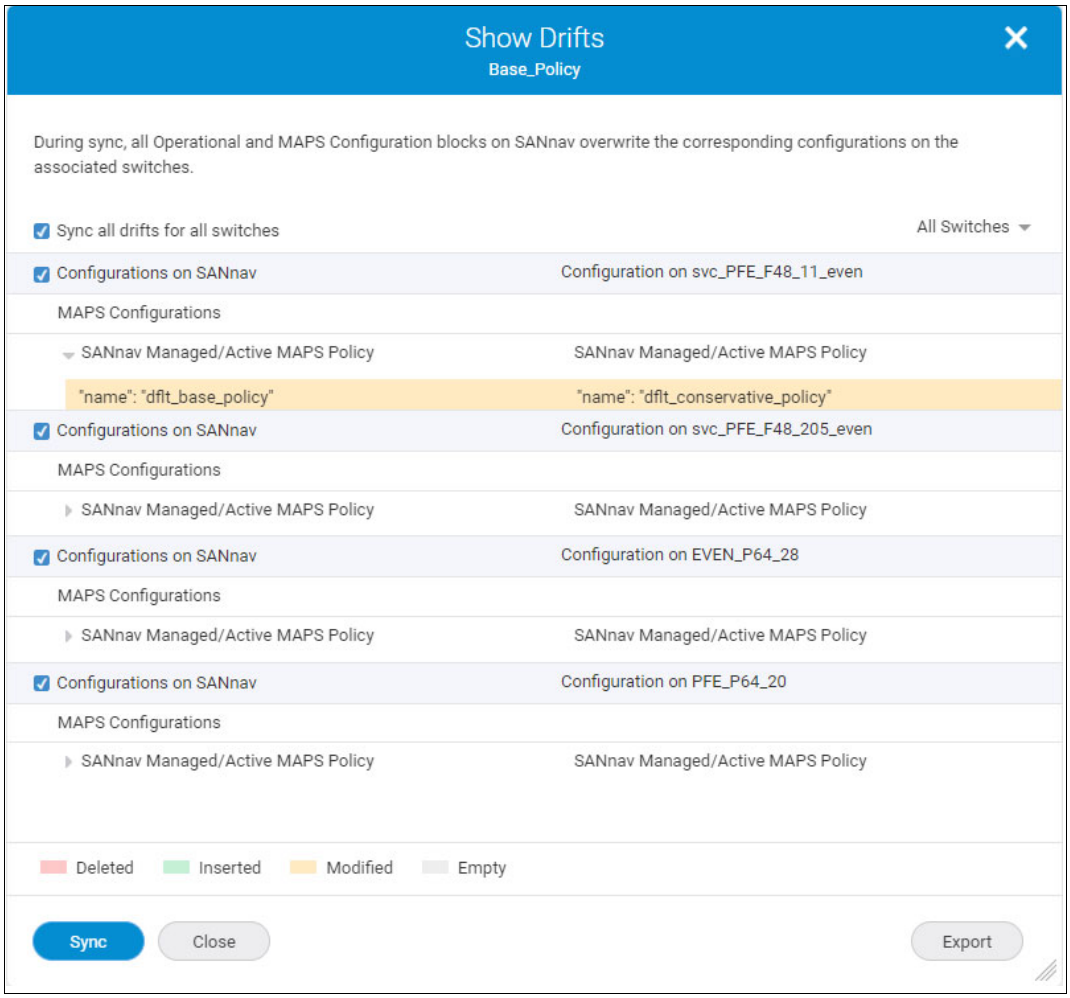


Figure 5-12 Show Drifts

5. You can view the deleted, inserted, modified, and empty configurations between SANnav and the switch. You can export configuration drifts in PDF format by clicking **Export.**

6. You also can check the dashboard to quickly see switches with configuration drifts. The Configuration Drifts widget shows a bar chart that lists the number of switches in all the monitored policies per fabric with the corresponding `Drift Detected` or `Check Failed` states. Click the **All** drop-down menu to see the switches for a specific fabric, as shown in Figure 5-13.

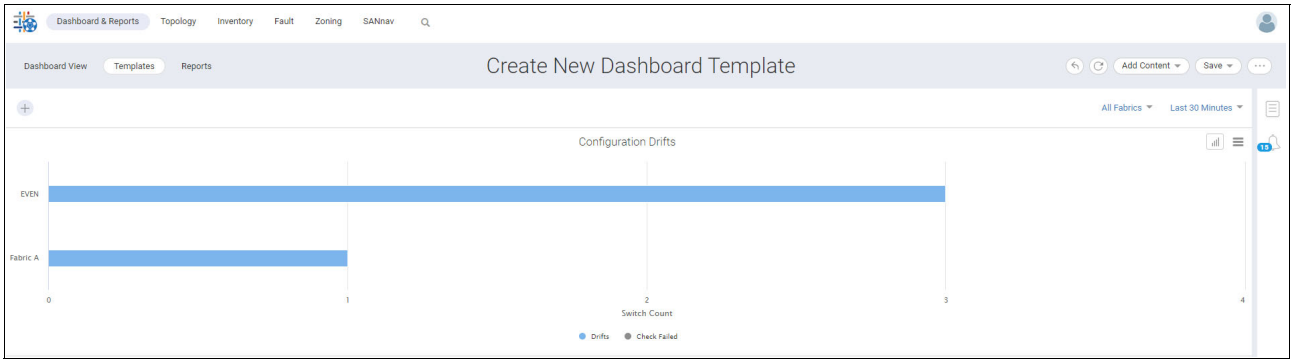


Figure 5-13 Configuration Drifts dashboard

7. When you click the bar chart, the Switches with Drifts list for each fabric appears. You can view the list of configuration drifts for each switch by selecting the **Show Drifts** option, as shown in Figure 5-14.

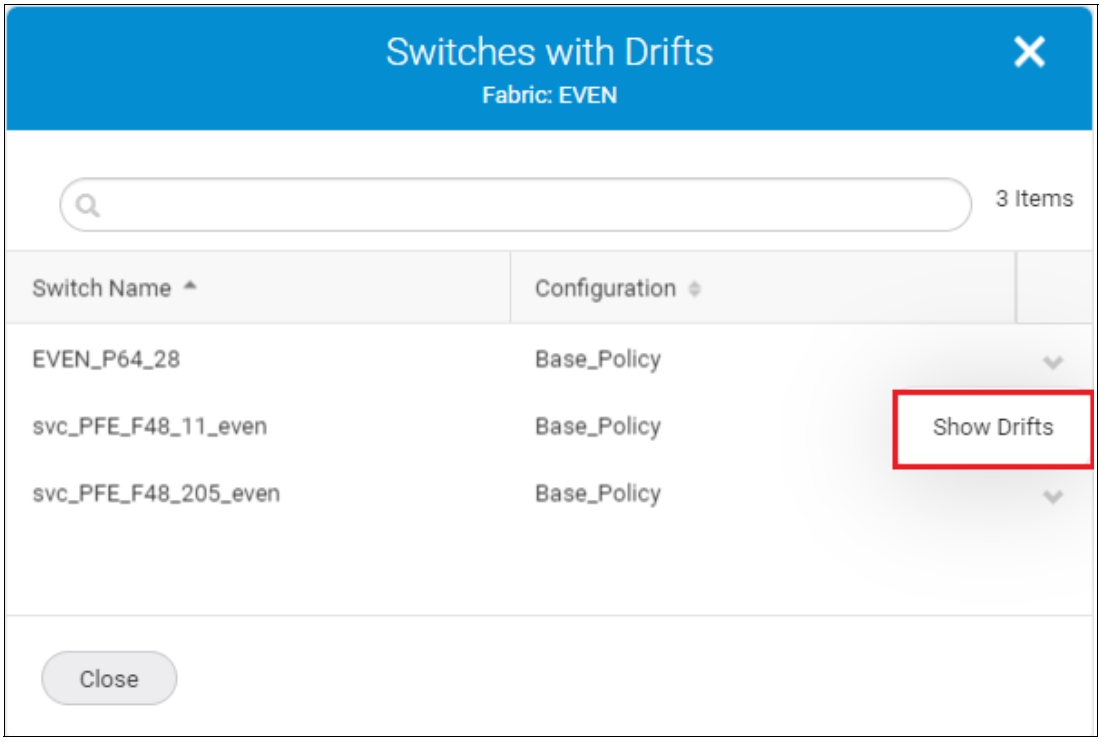


Figure 5-14 Configuration Drifts dashboard

5.4.4 Resolving configuration drifts

If configuration drifts occur between the switch configuration and the configuration policy, you can resolve the drifts immediately.

To resolve configuration drifts, you must have the Configuration Policy Manager privilege with read/write permission.

When a drift is detected, you can synchronize the configuration in the policy with the switch by using the sync operation in the Show Drifts window. During the sync operation, all operational and MAPS configuration blocks on SANnav overwrite the corresponding configurations on the associated switch.

Complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** → **Configuration Policies Management** → **Policy**. The Policies window opens.
2. For policies with the `Drift Detected` status, click the down arrow in the rightmost column and select **Show Drifts**. You can view the drifts of a specific existing policy after selecting the **Show Drifts** option for the specific policy. The Show Drifts window opens.
3. From the Show Drifts window, you can sync switches in accordance with the policy. You can sync the configuration policy of either all switches or a specific switch:
   - If you want to replace the configuration of all switches with the configuration that is defined in the policy, select the **Sync all drifts for all switches** checkbox, and then click **Sync**.
   - If you want to replace the configuration of a specific switch with the configuration that is defined in the policy, select the specific checkbox, and then click **Sync**.

The policy configuration is replaced on the switch, as shown in Figure 5-15.

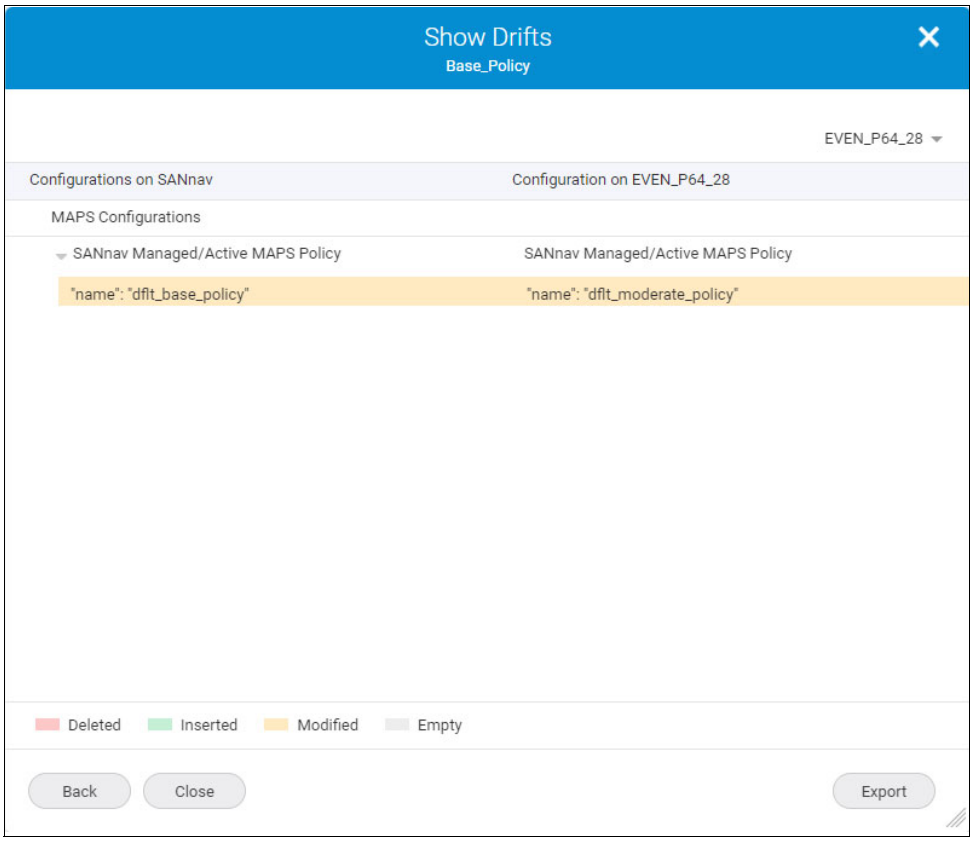


Figure 5-15 Show Drifts

If the sync operation fails, a failure message appears and states the switch name, status, and reason for failure:

- The configuration blocks that are part of the saved policy are updated in SANnav.
- If the switch has extra configuration blocks in comparison to the configuration blocks in the policy, the additional configuration blocks do not merge with the saved policy.

5.4.5 Blocksets

SANnav supports creating a policy configuration that is based on the basic configuration and SANnav MAPS policy blocksets.

A blockset is a set configuration of blocks that can be of two types:

- Configurations: The basic configuration blockset represents a set of configuration blocks (that is, FTP Setting, Audit configuration, SNMPv3, and so on). You can associate multiple (0 and more) basic configuration blocksets to the policy, where the blocksets must not contain common blocks in the associated blocksets. You can create the basic configuration blocksets with the blocks that are supported on all switch platforms and firmware versions.
- SANnav MAPS Policy: The MAPS policy blockset represents a SANnav MAPS policy containing all MAPS rules for all FOS versions and all switch platforms and models. The MAPS policy blockset contains a set of MAPS rules. You can create the SANnav MAPS policy blockset containing the MAPS rules that are supported on all switch platforms and firmware versions. You can associate only one MAPS blockset to one SANnav policy.

You can create and manage blocksets that contain a group of configuration blocks:

- For a basic configuration blockset, you can group the following configuration blocks:
  - Operational configuration blocks of the switch.
  - Operational configuration blocks of the chassis.
  - MAPS configurations.
- For a SANnav MAPS policy blockset, you can group the following configuration blocks:
  - A SANnav MAPS policy has different MAPS categories that are represented as blocks under the Blocks window.
  - You can add, edit, or delete rules under each MAPS category or block.

Note: When you upgrade to SANnav v2.2, the migrated blocksets might have errors. You must validate the migrated blocksets before a push or sync operation.

5.5 Configuration backup and restore

A configuration backup is a backup copy of the switch configuration file. As part of standard configuration maintenance, you should keep individual backup files for all switches in the fabric.

You can back up the configuration to the SANnav repository, and you can also export the configuration to a file as an extra safety measure.

Configuration backups are triggered in several ways:

- Discovery: Switch or fabric discovery automatically triggers a backup for all switches in the fabric that have the correct user credentials.
- Event Triggered: Configuration backups are automatically triggered when a switch undergoes configuration changes and when audit events are received in the master log. SANnav must be registered as an SNMP trap or a Syslog recipient for an event-triggered backup to occur.
- Manual: You can back up a switch configuration on demand.

In addition to these three ways, SANnav performs a routine backup of all discovered switches once a day.

Configuration backups are stored in a repository in the SANnav database.

One configuration backup type (Chassis, Logical Fabric, or Switch) for each switch is designated as the baseline. By default, the first configuration backup is designated as the baseline, but you can change the baseline configuration. The baseline configuration is kept indefinitely.

5.5.1 Backing up switch and logical fabric configurations

When a switch configuration backup is initiated, the chassis and logical fabric backups are generated automatically. SANnav performs a routine backup of all discovered switches once a day (at 00:30).

You must have the Configuration File Manager privilege with read permission to back up a configuration on demand.

The four types of backup configurations are as follows:

- Switch
- Chassis
- Logical fabric
- Imported configuration

Note: Configuration backup files that are taken as part of the import, drift, push, or sync operations are updated as the Imported configuration type. SANnav does not support restoring the imported backup type.

A logical fabric configuration backup is triggered in the following scenarios:

- When a new switch is discovered.
- When an on-demand backup is initiated (**Backup Now**).
- When the following RASLOG events are received:
  - Creating a logical switch
  - Deleting a logical switch
  - Moving ports between the logical switch
  - Changing the base switch
  - Enabling IBM FICON® on the logical switch
- As part of the everyday scheduled backup.

To back up switch and logical fabric configurations, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services** → **Switch Configuration Backups**. The Switch Configurations Backups window opens, as shown in Figure 5-16.

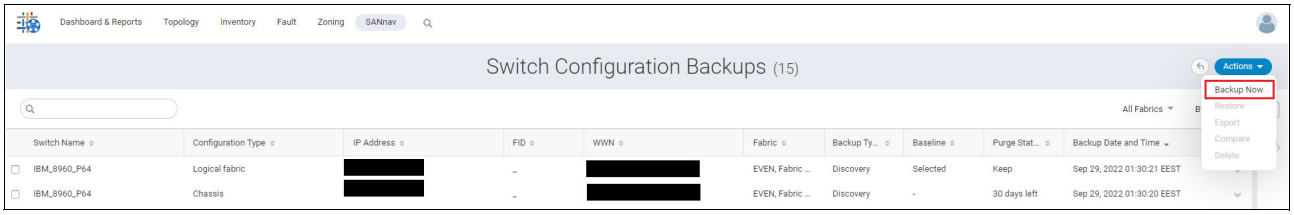


Figure 5-16 Backup Now

2. Click **Backup Now** from the **Actions** menu to back up a configuration immediately. The Select Switches window opens.
3. When configuring the backup, you can choose to back up a single switch or multiple switches. Select switches, and then click **OK**.

When the backup operation for the switches is successful, entries such as Switch, Chassis, and Logical fabric are added to the Switch Configurations Backups window as a configuration type.

5.5.2 Restoring chassis, logical fabric, and switch configurations

When you restore a configuration file, you overwrite the existing switch configuration with a previously backed up configuration file.

Before you can restore a configuration to a switch, you must have at least one previously saved configuration for that switch. You must have the Configuration File Manager privilege with the read/write permission.

If a virtual fabric (VF) is enabled on a director or on a chassis (switch or director), SANnav backs up following files:

- One backup file for the chassis.
- One backup file for the virtual fabric.
- One backup file for each configured logical switch that is discovered in SANnav. If 16 logical switches are configured in the chassis, SANnav supports backing up a maximum of 16 configuration files.

If VF is disabled on a director or on a chassis (switch or director), SANnav supports backing up a single file for the switch and chassis.

If VF is enabled, you must restore all configuration files one by one in the order of chassis followed by the virtual fabrics, and finally one file per logical switch:

- Restoring the chassis, logical fabric, and switch configurations to the same switch all at once.
- Restoring the chassis, logical fabric, and switch configurations to the same switch individually.
- Restoring the chassis, logical fabric, or switch configuration of a missing switch to multiple applicable switches.

Notes:

- Restoring a configuration is a disruptive operation.
- A switch can have more than one backup configuration type, so be sure to select the correct configuration type. You can search on the switch name to show only the configurations for that switch. You can select multiple switches to restore concurrently. For example, you can select a specific fabric and restore the configuration on all switches in that fabric.

To restore chassis, logical fabric, and switch configurations, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services** → **Switch Configuration Backups**. The Switch Configurations Backups window opens.
2. To restore the chassis, logical fabric, and switch configurations to the same switch all at once, complete the following steps:
   a. Select the chassis, logical fabric, and switch configurations whose configuration you want to restore, and click **Restore** from the **Actions** menu. The Restore Switch Configurations window opens, as shown in Figure 5-17.

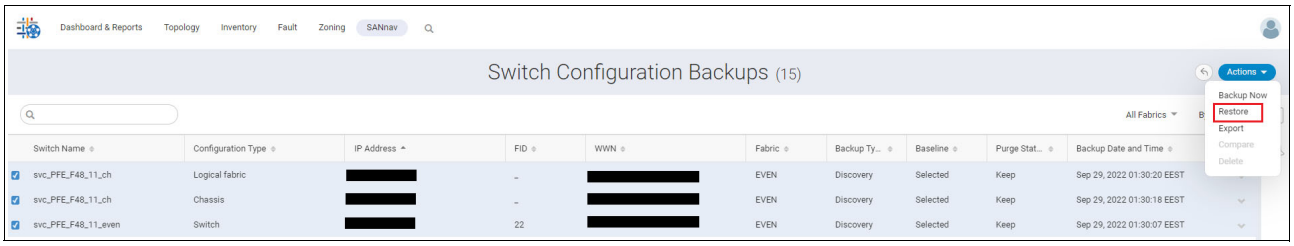


Figure 5-17 Restoring a backup

This operation restarts the switch once, enables or disables the switch multiple times for each chassis or switch backup restore, disables all ports on the switch, and also disrupts the traffic going through the switch.

   b. Click **OK** in the confirmation window, and then click **Done**.
3. To restore the chassis, logical fabric, and switch configurations to the same switch individually, complete the following steps:
   a. Select the chassis backup configuration type for the chassis that you want to restore, and click **Restore**.
   b. Click **OK** in the confirmation window, and then click **Done** to restore the configurations.

   Complete similar procedures to restore the configurations of a logical fabric followed by a switch:

   – When you restore the switch or chassis configuration to the same switch, it disables and enables the switch. Disabling the switch disables all ports on the switch, disrupts the traffic going through the switch, and also reconfigures the fabric.
   – When you restore the logical fabric configuration to the same switch, the switch restarts and creates the logical switches based on the logical fabric configuration.

4. To restore the chassis, logical fabric, or switch configuration of a missing switch to multiple applicable switches, complete the following steps:

   a. Select **Unmonitored** from the **By Fabric** drop-down list, as shown in Figure 5-18.

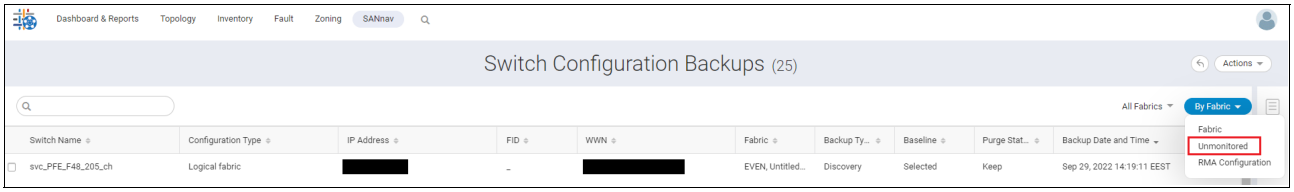


Figure 5-18 Selecting Unmonitored

   The backup entries for all missing switches appear.

   b. Click the down arrow in the rightmost column of a chassis and select **Restore**, as shown in Figure 5-19.

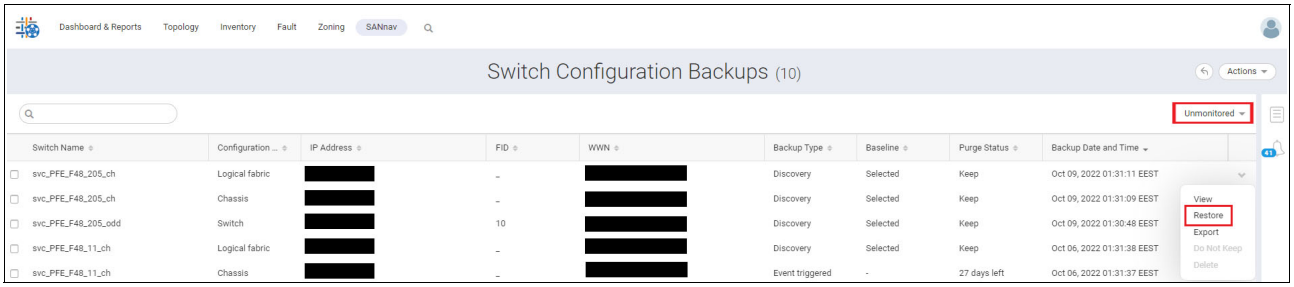


Figure 5-19 Unmonitored restore

   The Restore Switch Configurations window opens. This window shows the list of switches for which you can restore the configuration. This window shows all applicable switches based on the type of backup entry, the switch model, and the version.

   Complete similar procedures to restore the configurations of a logical fabric followed by a switch.

c. Select the switch and select **OK**, as shown in Figure 5-20.

Figure 5-20 Restore

This operation replaces the current configuration on the switch and restarts the switch.

d. Click **OK** in the confirmation window to trigger the restore operation. You can view the progress dialog box, and then click **Done**.

5.5.3 Managing switch configuration backups

You can back up configurations of one or more switches on demand. You can view, delete, and export these backups, designate a backup as a baseline, and compare two configurations. Configuration backups are listed in the Switch Configuration Backups window. You can save backups to an offline location and restore them to switches based on need by using the command-line interface (CLI).

To manage configuration backups, you must have the Configuration File Manager privilege with the read/write permission.

The first configuration backup for a switch is automatically designated as the baseline, but you can designate a different backup as the baseline.

To manage the switch configuration backups, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services** → **Switch Configuration Backups**. The Switch Configurations Backups window opens with a list of configuration backups, as shown in Figure 5-21.

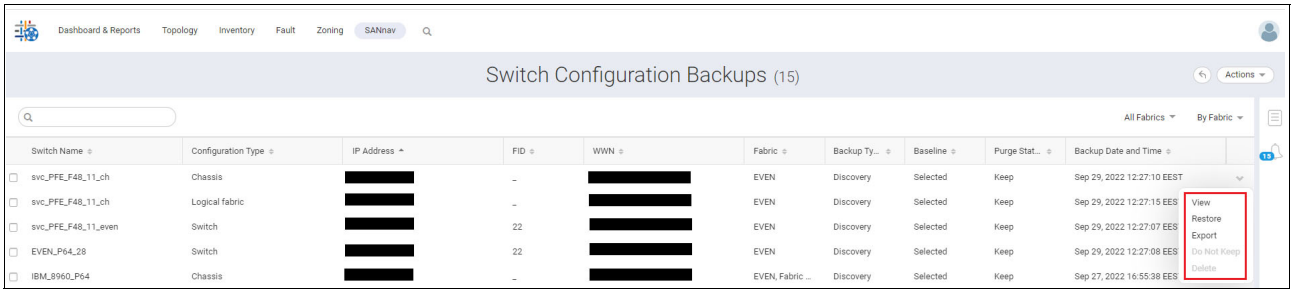


Figure 5-21 Managing configurations

2. To view the configuration of a chassis, a logical fabric, or a switch, click the down arrow next to the switch, and then select **View**.
3. To designate a configuration as a baseline, click the down arrow next to the switch, and then select **Select Baseline**.

   Baseline configurations are kept indefinitely. A switch can have only one baseline configuration for each configuration type and virtual fabric ID (VFID) combination, such as one baseline logical fabric configuration (if VF is enabled), one baseline chassis configuration (if VF is enabled), and one baseline switch configuration for each logical switch with different virtual fabric ID (if VF is enabled). If VF is disabled, SANnav supports backing up a single file for the switch and chassis.
4. To change the retention period for a configuration backup, click the down arrow next to the switch, and then select one of the following options:
   - To retain a backup indefinitely, select **Keep**.
   - To delete backup after the retention period, select **Do Not Keep**. If a baseline is selected, the **Do Not Keep** option is disabled.
   - To delete a backup immediately, select **Delete**.
5. To export a configuration file, click the down-arrow next to the configuration and select **Export**. The configuration is written to a text file and downloaded to your local machine.
6. To compare two configurations for the same switch, select two backups, and then click **Compare** from the **Actions** menu. You can compare backups only from the same switch and from the same type**.**

For more information about configuration topics, see *Brocade SANnav Management Portal User Guide, v2.2.x*.

5.6 Managing zoning in SANnav

Managing SAN zoning is a common practice. Every time a new server is added to a network, an administrator must decide with which storage array ports the HBA ports on the newly added server must communicate.

A fabric might contain many hosts and storage ports that are connected to it that might range from a few hundreds to several thousands of device ports that are connected to the fabric. Thus, managing zoning is like managing a large object and its associations.

Figure 5-22 shows the basic layout of the **Zoning** tab.

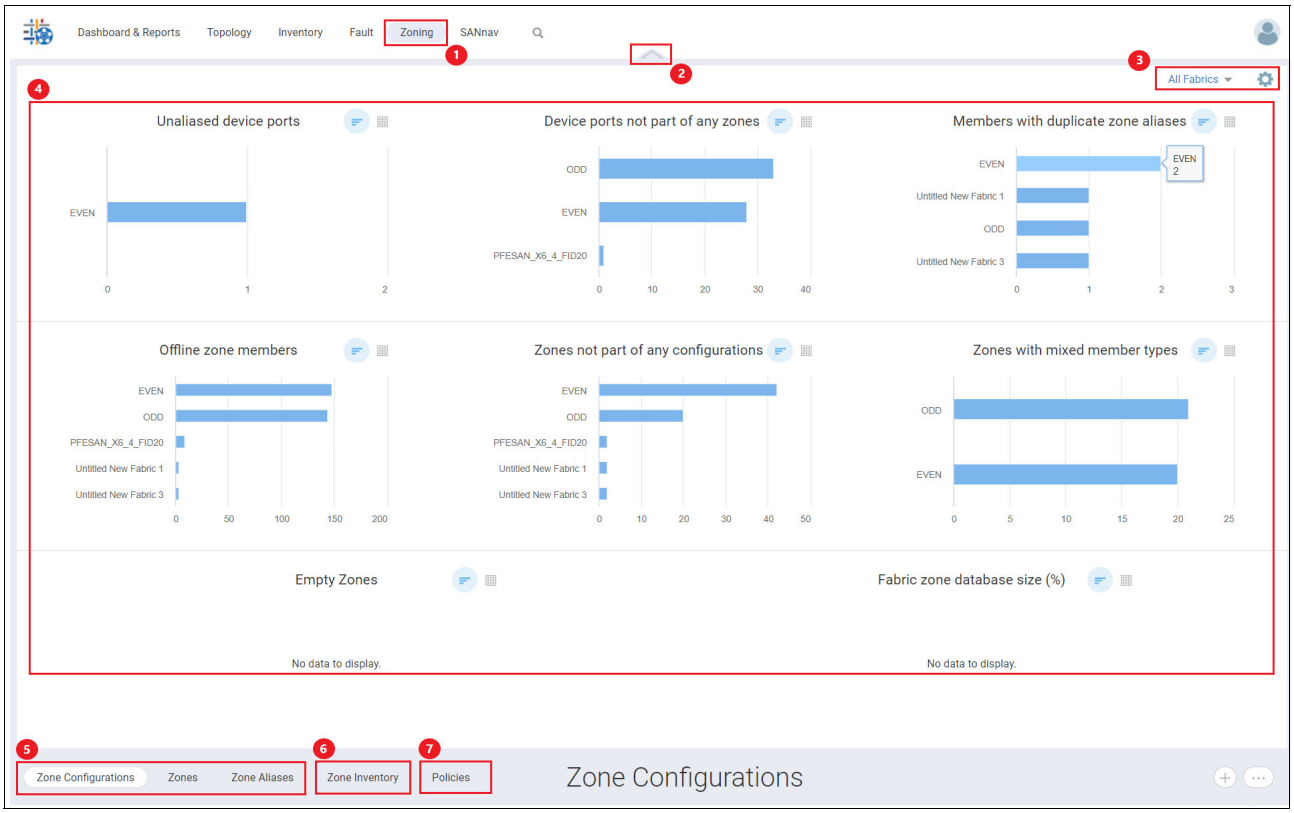


Figure 5-22 Zoning tab

1. From the **Zoning** tab, you can perform all zoning actions.
2. Drop-up or drop-down icon

   With this icon, you can open or close a window that shows zoning detail widgets. The screen capture shows an OPEN detail window.
3. All Fabrics and Settings

   By default, you can view zone summary widgets across all fabrics. This drop-down icon can be used to select the fabrics that you want to look at. The Settings icon is used to edit and reorder the zone summary widgets.
4. Zone summary widgets

   You can perform zoning operations based on the predefined filters that are available in the zone summary widgets.
5. **Zone Configurations**, **Zones**, and **Zone Aliases** subtabs

   You can perform basic zoning operations by using these three subtabs.
6. **Zone Inventory** subtab

   By using this subtab, you can show detailed information about all zone members and also see a member-centric view. You can perform various zoning operations directly from the Zone Inventory window.
7. **Policies** subtab

   Using this subtab, you can set the default zoning policy to all access or no access on a per fabric basis.

5.6.1 Creating zone aliases

A zone alias can be either a combination of a switch domain ID plus a port index or a device worldwide name (WWN). Zone aliases facilitate zone configuration by using the alias instead of selecting individual WWNs or Domain, Port Index numbers. While searching for zone aliases in the Zone Aliases list, the search option is restricted to the zone alias name, tags, and description columns only. You can create a single zone alias or multiple zone aliases. If there are unaliased devices (hosts or storage ports) in a fabric, SANnav supports creating aliases directly for these devices. A zone alias can be created from the Zone Aliases and Zone Inventory windows. This section describes the procedure to create a zone alias from the Zone Aliases window, exporting or importing zone aliases, and reverse lookup for zone aliases.

Creating a single zone alias

To create a single zone alias, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab. The Zone Aliases window opens.
2. Select the fabric from the **Select Fabric** drop-down list, and then click **OK**. The Zone Aliases window opens all the zone aliases that are defined in the selected fabric.
3. Click the **+** icon in the upper right of the window, and then select the **Create Single** option from the available options, as shown in Figure 5-23.

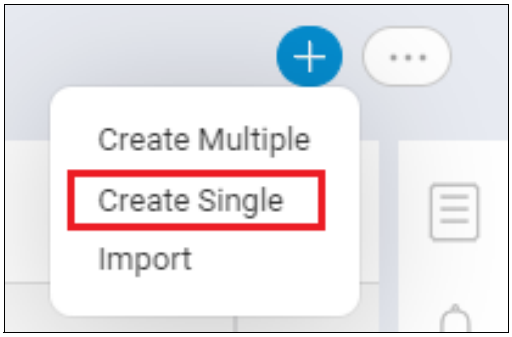


Figure 5-23 Create Single option

The Create New Zone Alias window opens.

4. Define the zone alias name based on the set of properties in the Name field. As a best practice, create multiple zone aliases because the user can choose the naming properties to define the alias name.
5. Add members to the zone alias. A maximum of 255 members can be added to a single zone alias.

Notes:

- As a best practice, define one zone alias per WWN (host or storage port).
- SANnav does not support creating zone aliases with mixed-member types.
- If FICON mode is enabled, the Domain, Port Index must be searched with a comma in the Add Members window. If you want to search a domain value, it must be prefixed with a comma (for example, “,0x5”). If you want to search a port value, it must be suffixed with a comma (for example, “0x23,”).

a. Click **Add**.

b. Select either **Select discovered devices/port** to choose the member from a list or **Enter manually** to enter the member yourself.

c. Select the type of zone member (`WWN` or `Domain, Port Index`) from the drop-down list.

d. Select the discovered members or enter the name of the offline members, and then click the right arrow to move them to the Selected Members list.

6. Click **OK** to add the members to the zone alias, as shown in Figure 5-24.

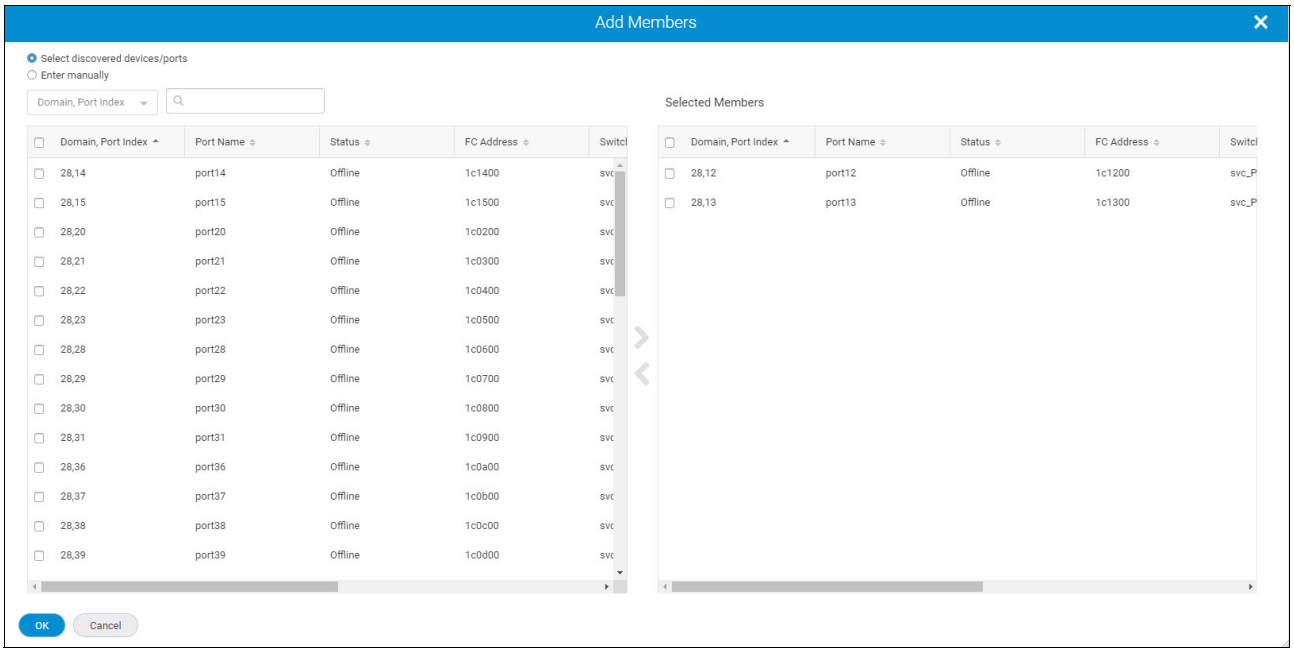


Figure 5-24 Create Single alias: Adding members

The members are added to the Members list.

7. Click **Save** to save the zone alias. The zone alias is created and showed under the Zone Aliases window.

Notes:

- To delete a single zone alias, drill down to the zone alias that you want to delete, and then select the **Delete** option. If this zone alias is part of an effective zone configuration, then to apply the changes, you must activate the corresponding defined zone configuration.
- You cannot edit or delete a single zone alias with mixed-member types.

Creating multiple zone aliases

Multiple aliases can be created in a single workflow by using the **Create Multiple** option. This process creates zone aliases that consist of one member each. It is an easy way to assign zone aliases for multiple ports. You can alias all unaliased host or storage ports (WWN members) or switch ports (Domain, Port Index). You can also create zone aliases directly for the unaliased devices.

To create multiple zone aliases in a single workflow, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select **Zone Aliases**. The Zone Aliases window opens.
2. Select the fabric from the **Select Fabric** drop-down list, and then click **OK**. The Zone Aliases window opens and shows all zone aliases that are defined in the selected fabric.
3. Click the **+** icon in the upper right of the window, and then select the **Create Multiple** option, as shown in Figure 5-25.

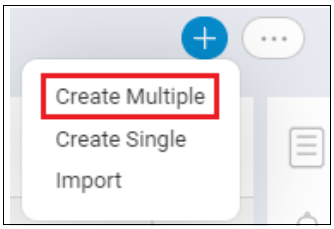


Figure 5-25 Create Multiple aliases option

4. If the fabric contains unaliased devices, click **OK** in the Added Devices window. The Create Zone Alias window opens.
5. Add members to the zone alias.

Note: If FICON mode is enabled, the Domain, Port Index must be searched with a comma in the Add Members window. If you want to search a domain value, it must be prefixed with a comma (for example, ",0x5"). If you want to search a port value, it must be suffixed with a comma (for example, "0x23,").

6. Select either **Select discovered devices/ports** to choose the members from a list or **Enter manually** to enter them yourself.
7. Select the type of zone member (`WWN` or `Domain, Port Index`) from the drop-down list.
8. Select the discovered members or enter the name of the offline members, and then click the right arrow to move them to the Selected Members list.
9. Click **Next** to choose the method of naming the aliases. You can create zone aliases either automatically or manually.
10. Click **OK**. The zone aliases are created and showed under the Zone Aliases window.

Notes:

- To delete zone aliases in bulk, click **More (...)** at the upper right of the window, and then select **Bulk Select**. Select rows in bulk, and then select **Delete** from the **Actions** menu.
- You can delete zone aliases in bulk for mixed-member types.

5.6.2 Exporting zone aliases

You can export zone aliases. For example, if a device is relocated to another fabric, you can use this alias in the other fabric. You can use this zone alias as a backup if all zone databases are lost.

To export a zone alias, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab.
2. Click **Select Fabric** to select a fabric to export and click **OK**.
3. Click **More** (**...**) at the upper right of the window, and then select **Export**, as shown in Figure 5-26.

Figure 5-26 Exporting aliases

The zone aliases of the selected fabric are downloaded as a CSV file to your local machine.

5.6.3 Importing zone aliases

You can import zone aliases from your local machine. To import zone aliases from your local machine, complete the following steps.

Note: Only CSV files are supported.

1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab.
2. Select the fabric from the **Select Fabric** drop-down menu into which to import the zone aliases, and then click **OK**.
3. Click **+** in the upper right of the window and select **Import**.
4. Browse through the folders to select the file that contains the zone aliases.
5. Click **Open** to import the zone aliases. The Import Zone Aliases window opens, as shown in Figure 5-27 on page 133.

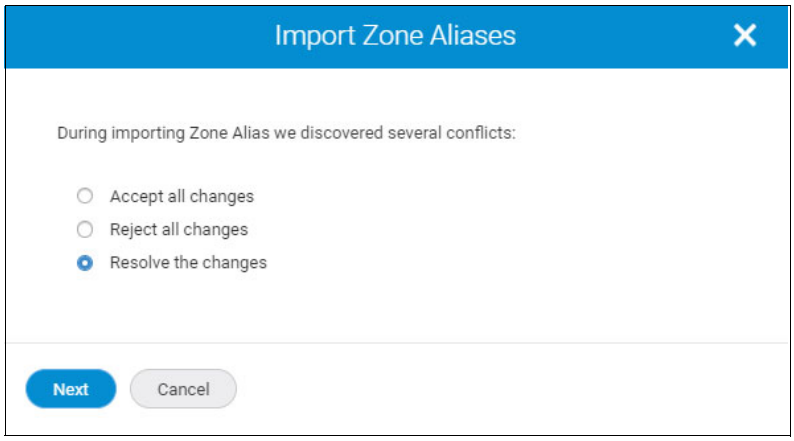


Figure 5-27 Import Zone Aliases

6. Select the action for when a conflict occurs:
   a. Select **Accept all changes** to apply to all the conflicts.
   b. Select **Reject all changes** to reject only the conflicts. For example, if there is a member name M1 and alias name A1 in a fabric and if you try to import the same member name M1 with alias name A2, a conflict occurs.
   c. Select **Resolve the changes**, and then select **Next**.

   The Import Zone Aliases window opens (Figure 5-28). Select the members and select the **Allow Multiple Members** option. You can select the members from the conflicts. You also can remove the member by clicking **Remove**.

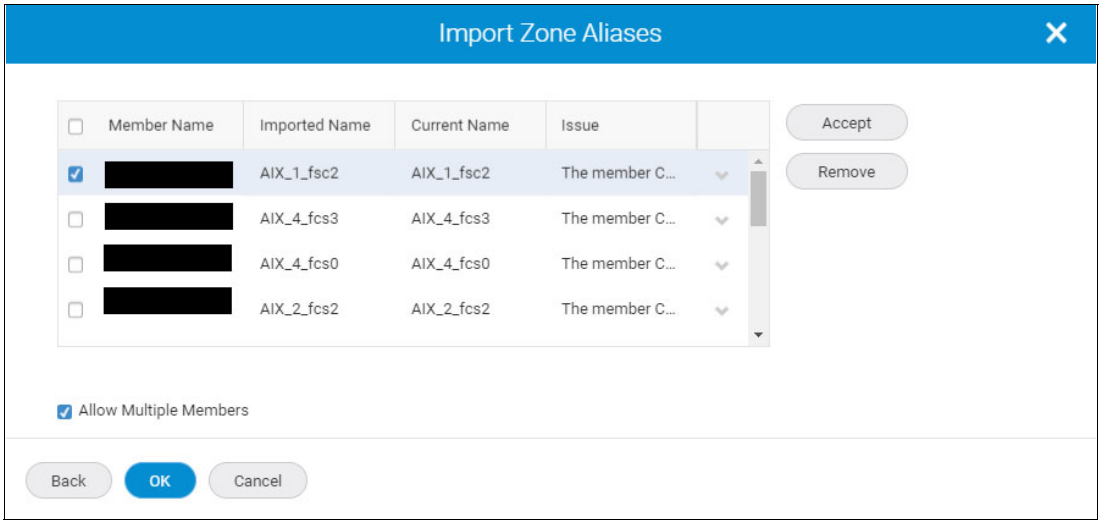


Figure 5-28 Import Zone Aliases: Allow Multiple Members

7. Click **OK** to confirm the selected action.

5.6.4 Supporting reverse lookup for zone aliases

SANnav supports the reverse lookup feature for zone aliases. The reverse lookup feature allows you to navigate from zone aliases to zones and from zones to zone configurations.

To view the zone alias details, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab. The Zone Aliases window opens.
2. Select the **Show Details** option for an individual zone alias from the action drop-down menu. The Zone Alias Details window opens. The Zone Alias Details window shows the zone aliases, zones, and zone configuration details. You can navigate from zone aliases to zones and from zones to zone configurations, as shown in Figure 5-29.

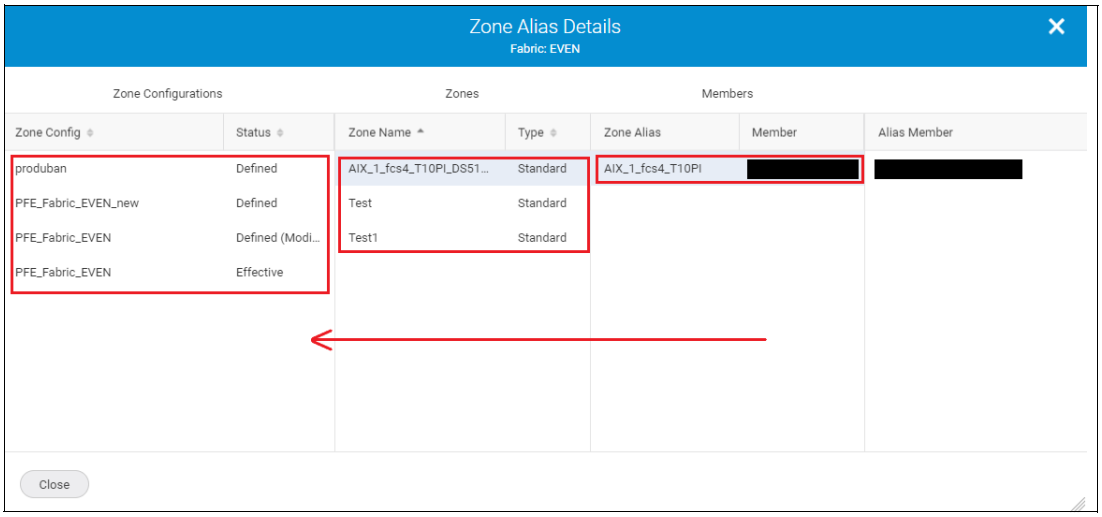


Figure 5-29 Reverse lookup alias

Configuring zones in a fabric

You can create zones for a fabric. If you want to create a different type of zone, you can select from any of the zone types.

You can create any of the following four types of zones:

- LSAN zones: You can create an LSAN zone to allow the devices to communicate with the other devices that are present in other fabrics that are connected through the Fibre Channel (FC) router without merging the fabrics. You can select any edge fabric or backbone fabric to create an LSAN zone.
- LSAN peer zones: An LSAN peer zone combines the properties of both LSAN zoning and peer zoning. You can select any edge fabrics or backbone fabric to create an LSAN peer zone.
- Peer zones: A peer zone can be created with one or more devices that are designated as a principal device for that zone. All nonprincipal devices in the peer zone can access only the principal devices and cannot communicate with each other. The principal devices can communicate with all other nonprincipal devices. Peer zoning results in less RSCN traffic on zoning and device changes, and it creates fewer zones.
- Standard zones: Standard zones allow communication between all members in the zone.

Note: SANnav does not support the following zones:

- Boot LUN (BLUN) zones
- Frame redirect (RD) zones
- Target-driven zones (TDZ)
- Traffic isolation (TI) zones

If these zones are created by using other interfaces, like the CLI or Brocade Web Tools, you can view these zones in SANnav but cannot modify them. If boot LUN or TDZs are in a zone configuration, you cannot remove them from a zone configuration. However, you can edit such a zone configuration and can add or remove other zones to the zone configuration.

Creating zones

Zones can be created from the Zone Aliases, Zones, and Zone Inventory windows.

To create a zone, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zones** tab.
2. Select a fabric for which to create a zone, and then click **OK**.
3. Click **+** in the upper right of the window to create a zone.
4. Enter a name for the zone, along with any tags and descriptions. For LSAN and LSAN peer zones, the zone name must begin with `LSAN_` followed by the name. The Broadcast zone is deprecated from FOS 9.0.1 onward. SANnav does not allow creating a Broadcast zone. When configuring an LSAN and LSAN peer zone, SANnav does not support aliases of the same name with the same member in the other edge fabric.
5. Select the zone type from the **Zone Type** drop-down menu (Figure 5-30). If the zone type is other than standard, peer, LSAN, or LSAN peer, you cannot delete or edit a zone.

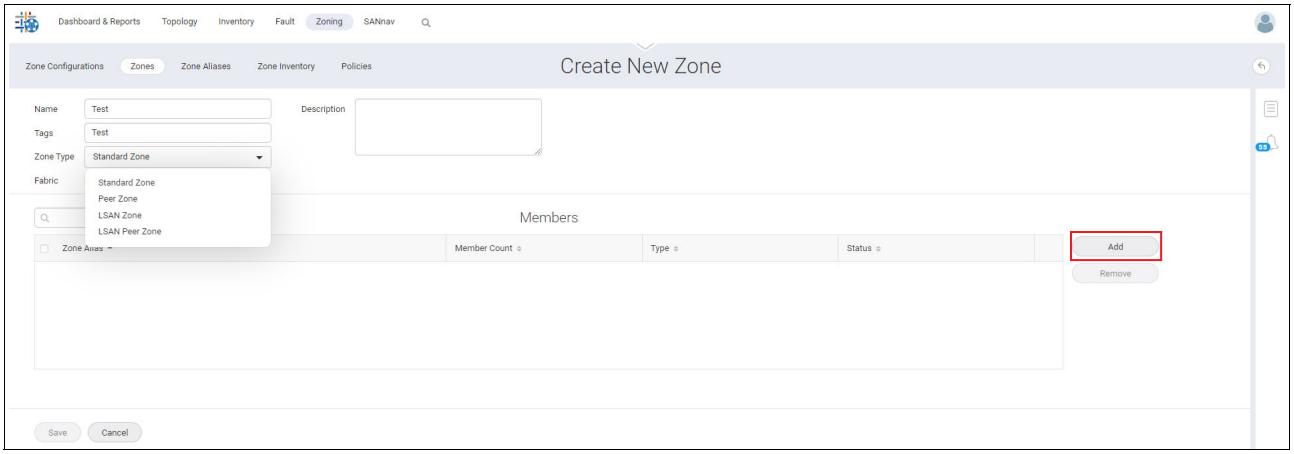


Figure 5-30 Creating a zone

6. Add members to the zone:
   a. Click **Add** in the Create New Zone window.
   b. Select the type of zone member from the drop-down list: **WWN** or **Domain, Port Index**, or **Alias**.

Notes:

- It is a best practice to have only zone aliases in a zone. With zone alias names, you can easily understand the name for a WWN or a port index.
- A mixed zone contains more than one of the following member types:
  - WWN
  - Domain, Port Index
  - Zone Alias - WWN
  - Zone Alias - Domain, Port Index
  - Zone Alias - WWN and Domain, Port Index

  To clean up a mixed zone, you can edit the mixed zone to include a single member type. You can add or delete members from the zone. However, you cannot save a modified mixed zone.
- If a zone configuration contains mixed zones, you cannot remove such zones from the zone configuration. The **Delete** option is not available for such zone configurations. You cannot add such non-editable zones to any zone configuration. However, you can edit the zone configuration and can add or remove zones to the zone configuration.
- For LSAN and LSAN peer zones, select the type of zone member from the drop-down list. **WWN** or **Alias Only** aliases that are configured with WWN members are listed.
- If newly created LSAN or LSAN peer zones are part of an active zone configuration, and if you activate the defined copy of the active zone configuration for one edge or backbone fabric, zone configurations for all connected fabrics are activated automatically.
- If an LSAN or LSAN peer zone contains a DP alias or DP member, that particular zone cannot be removed from a zone configuration, and you cannot perform any operations if it is part of a zone configuration.

c. Select members in the zone, and click the right arrow to move them to the Selected Members list.

d. You can also select **Enter manually** and enter the name of offline members.

Note: For WWN members, the search option is restricted to the device node WWN, zone alias name, device port WWN, host or storage name, vendor, slot or port number, and active zone count. For domain, port index members, the search option is restricted to the domain, port index value, port name, status, FC address, switch name, zone alias, slot or port number, and active zone count. For alias members, the search option is restricted to the member name, type, member count, and status.

Figure 5-31 on page 137 shows the Add Members window.

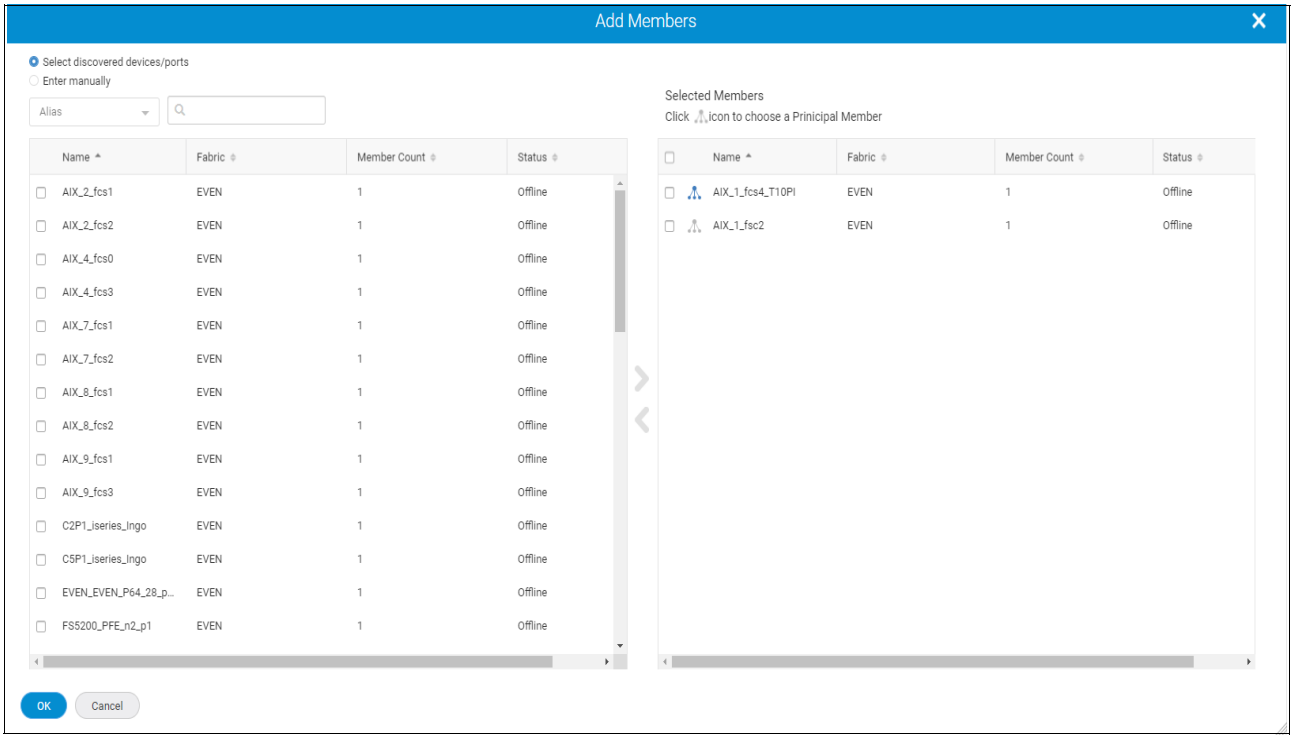


Figure 5-31 Adding zone members

7. Click **OK** and then click **Save**.
8. To modify an existing zone, select **Save** from the **Save** drop-down menu and perform the required changes. You cannot modify the zone type of an existing zone. You can modify only zone members from a zone.
   - To clone an existing zone with a different name, select **Save As** from the **Save** drop-down menu.
   - To delete an existing zone, drill down to the zone that you want to delete, and then select the **Delete** option. You can delete multiple zones by selecting the **Delete** option from the **Actions** menu.

Notes:

- SANnav does not support deleting the last zone from the effective zone configuration because an effective configuration cannot be empty.
- You can delete only an inactive zone.
- When you delete a zone from a zone configuration and the zone is the last member of the zone configuration, the zone configuration is also deleted from the fabric.
- You can delete a single zone and multiple zones in bulk with mixed-member types.

Adding multiple zone aliases to a zone

The bulk select feature allows you to select multiple zone aliases and add to one or more zones. You can add multiple zone aliases to a zone in the following ways:

- Adding the selected zone aliases to an existing zone.
- Adding multiple zone aliases to create a new zone.

To add multiple zone aliases to a zone in bulk, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab. The Zone Aliases window opens.
2. Click **More (…)** at the upper right of the window, and then select **Bulk Select**, as shown in Figure 5-32.

Figure 5-32 Bulk Select alias

The select options for the zone aliases appear.

3. Select the zone aliases to add them to a new or existing zone, and then select the **Add to Zone** option from the **Actions** drop-down menu.
4. To add a single zone alias to the zone, click the drop-down arrow next to a zone alias, and then select the **Add to Zone** option, as shown in Figure 5-33.

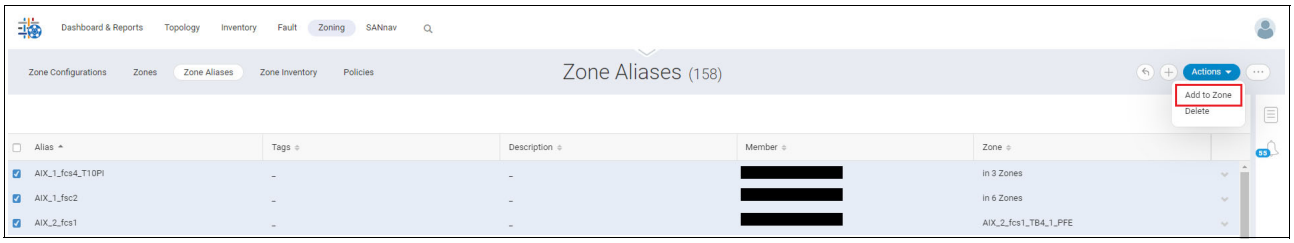


Figure 5-33 Bulk Select alias add to zone

Note: You can delete multiple zone aliases by selecting the **Delete** option from the **Actions** menu.

The Add to Zone window opens, as shown in Figure 5-34 on page 139.

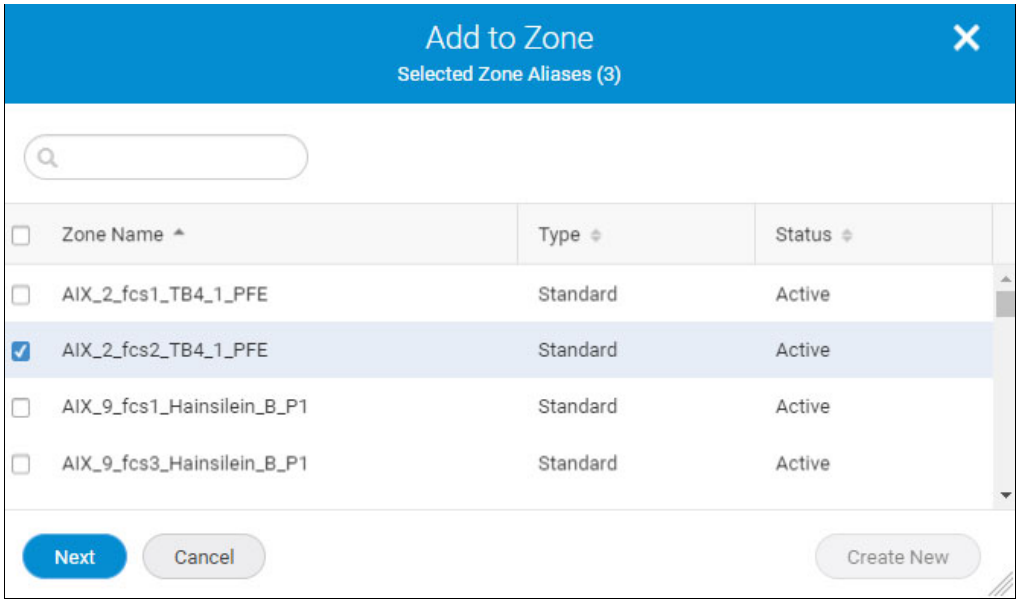


Figure 5-34 Add to Zone window

5. You can either add aliases to an existing zone or add them to a new zone:
   - To add aliases to an existing zone, select one or more existing zones and click **Next**.
   - To add aliases to a new zone, click **Create New**. Enter a zone name and zone type, and then click **OK**, as shown in Figure 5-35.

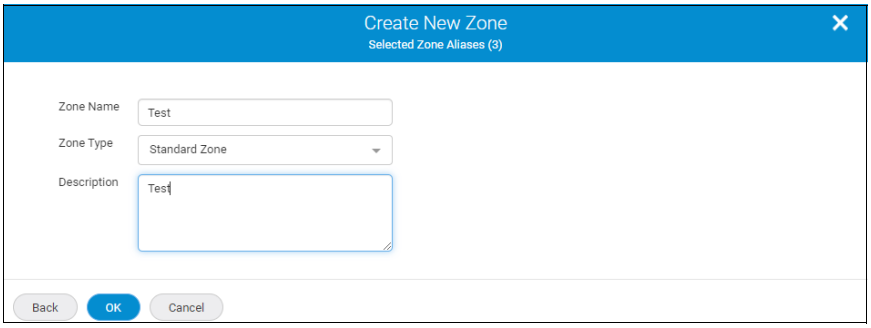


Figure 5-35 Create New Zone when adding alias

6. In the confirmation window, click **Next** to add the zone to a zone configuration or click **Close** to exit, as shown on Figure 5-36.

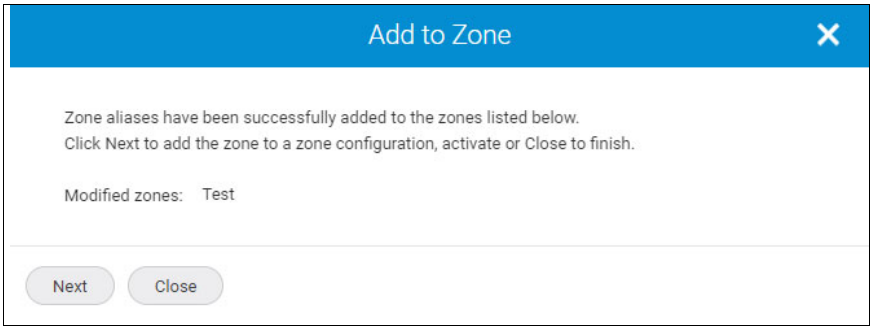


Figure 5-36 Confirmation window

For more information about activating the zone configuration, see “Activating a zone configuration” on page 142.

5.6.5 Creating zone configurations

A zone configuration is a group of one or more zones. A zone can be included in more than one zone configuration. When a zone configuration is activated, all zones that are members of that configuration are in effect.

Several zone configurations can be in a fabric concurrently. However, a fabric can have only one active zone configuration. For example, you might want to have one configuration that is enabled during business hours and another one that is enabled overnight.

If no zone configuration is active, either all devices can communicate with each other, or no devices can communicate with each other, depending on the zoning policy. For more information, see 5.6.9, “Policy-based zone creation” on page 156.

When the zones are created and you want to activate the zones, you must add the zones to a zone configuration, and then activate the zone configuration.

Notes:

- Empty zone configurations and zones cannot be created from SANnav. If empty zone configurations and zones are created by using the CLI, you can view the empty zone configuration and zones in SANnav. You cannot delete empty zone configurations in SANnav. You cannot add empty zones to a zone configuration, and you cannot edit them in SANnav.
- If an empty zone is a part of the zone configuration, you cannot remove the empty zone from the zone configuration. However, you can add or remove the other zones from the zone configuration.
- When a multiple zone selection contains an empty zone, **Remove** is disabled.

When you edit a zone configuration, you can filter and sort the zones in that zone configuration.

The newly added zones appear as the uppermost rows of the Zones list regardless of the sort order or sort column. The removed zones do not appear when the Zones list is sorted. You can save a zone configuration regardless of whether the Zones list is empty after search.

To create a zone configuration, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select the fabric and click **OK**. By default, the Zone Configurations window opens.
2. Click **+** at the upper right of the Zone Configuration window. The Create New Zone Configurations window opens.
3. Enter a name for the zone configuration, along with any tags and a description.
4. Click **Add**.
5. In the Add Zones dialog box, select one or more zones to add to the configuration or click **Create New** to create a zone and add it to the configuration, as shown in Figure 5-37 on page 141. For more information, see “Creating zones” on page 135.

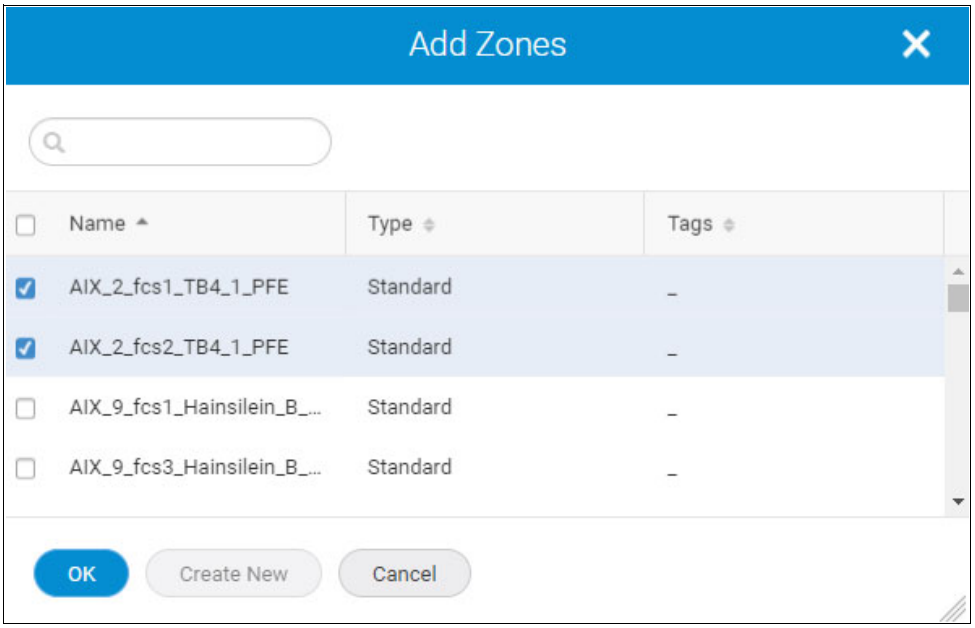


Figure 5-37 Add Zones to a new configuration

Note: While searching for zones in the Zones list, the search option is restricted to the zone name, type, tags, and description columns only.

6. In the Create New Zone Configuration window, click **Activate** from the **Actions** drop-down menu. While creating a zone configuration, if you want to activate the zone configuration, you can use the **Activate** action, which automatically creates and activates the zone configuration. For more information, see “Activating a zone configuration” on page 142.
7. If you want to activate the zone configuration later, click **Save**, and then click **OK**. You can compare the zone configuration with the effective zone configuration by selecting the **Compare** option. For more information, see “Comparing defined with the effective zone configurations” on page 147.

To delete an existing zone configuration, drill down to the zone configuration that you want to delete, and then select the **Delete** option.

Notes:

- SANnav does not support deleting a defined copy of the effective zone configuration.
- SANnav does not support deleting an effective zone configuration.

Here are the behavioral changes of the LSAN zone configuration when it is activated:

- If there are online members of LSAN or LSAN peer zones that belong to different edge or backbone fabrics, SANnav automatically creates or overwrites those LSAN zones in those edge or backbone fabrics.
- If other edge or backbone fabrics do not have an active zone configuration, SANnav automatically creates a zone configuration; adds the LSAN or LSAN peer zones; and activates them. The zone configuration name is `LSAN_CFG_`. For example, if a zone configuration is created on 24 November 2021, the zone configuration name will be `LSAN_CFG_20211124`.

- If LSAN or LSAN peer zones are modified to remove any existing online members, traffic might be disrupted for those members.
- If a defined zone configuration that is effective is in the modified state in other edge or backbone fabrics, the zone configuration is activated automatically in those fabrics.

Activating a zone configuration

To activate a zone configuration, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zone Configurations** tab.
2. Select a fabric from **the Select Fabric** drop-down menu, and then click **OK**.
3. Drill down to the zone configuration with the `Defined`, `Defined (Copy)`, or `Defined (Modified)` status that you want to activate.
4. Select **Activate** from the **Actions** menu, as shown in Figure 5-38.

Figure 5-38 Activating a configuration

The Activate Zone Configuration window shows a confirmation message.

5. Read the confirmation message, and then click **Next** to compare the defined zone configuration with the effective zone configuration, as shown in Figure 5-39. For more information, see “Comparing defined with the effective zone configurations” on page 147.

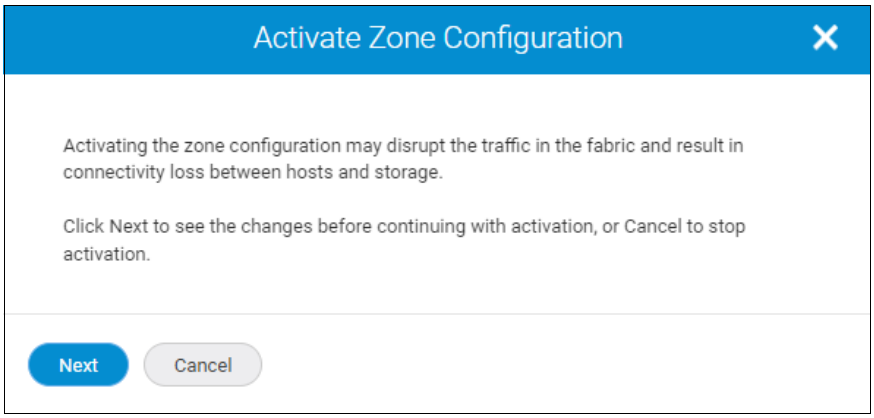


Figure 5-39 Activating the configuration confirmation message

6. The Compare and Activate Zone Configuration window opens. Click **Activate** to activate the zone configuration, as shown in Figure 5-40 on page 143.

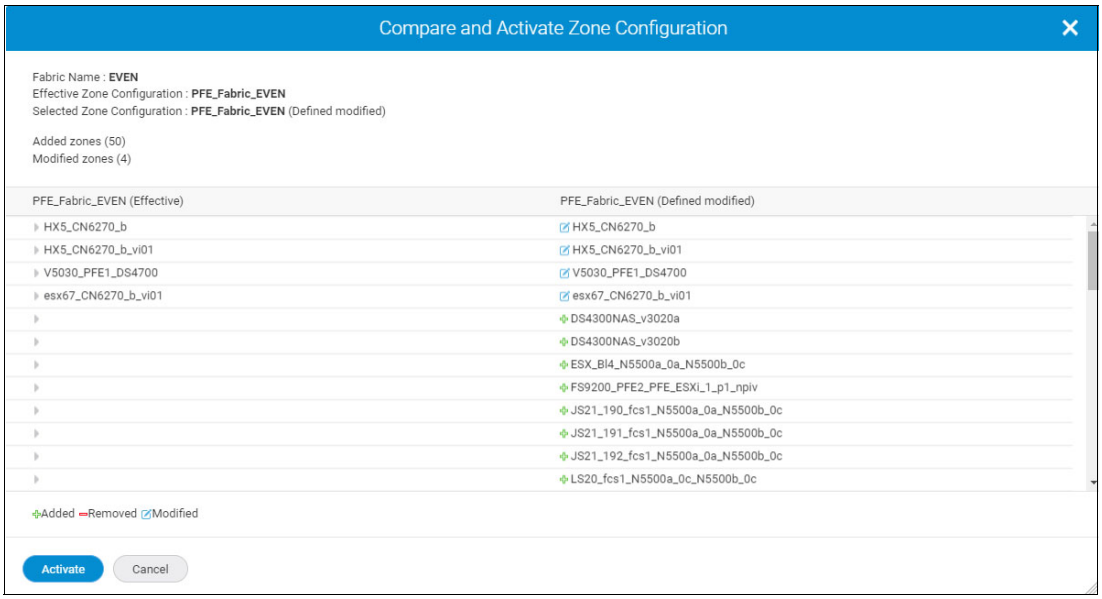


Figure 5-40 Compare and Activate

The zone configuration is activated and showed under the Zone Configurations window.

Deactivating a zone configuration

If the default zoning policy of the fabric is **Enabled (All Access)**, deactivating a zone configuration enables connectivity between all hosts and storage in that fabric. If the default zoning policy is **Disabled (No Access)**, deactivating a zone configuration results in loss of connectivity between all hosts and storage in that fabric. Regardless of the default zoning policy, traffic might be disrupted.

To deactivate a zone configuration, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zone Configurations** tab. The Zone Configurations window opens.
2. Drill down to the effective zone configuration of the fabric. You can deactivate only an effective zone configuration.
3. Select the **Deactivate** option from the **Actions** menu, as shown in Figure 5-41.

Figure 5-41 Deactivating a configuration

The Deactivate Zone Configuration window opens.

Note: Compare is not available when the user deactivates the effective zone configuration.

4. Read the confirmation message and click **OK**. The effective zone configuration is deactivated and the Zone Configurations window shows the zone configurations with the `Defined` status.

Modifying a zone configuration

If the content of the defined zone configuration is the same as the content of the effective zone configuration, the status appears as `Defined (Copy)`. If the content of the defined zone configuration is modified but not activated, the status appears as `Defined (Modified)`. The status of the effective zone configuration appears as `Effective`. The status of the saved zone configuration appears as `Defined`.

To modify a zone configuration, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zone Configurations** tab. The Zone Configurations window opens.
2. Select a fabric from the **Select Fabric** drop-down menu, and then click **OK**.

   The Zone Configurations window lists effective, defined (copy), and defined zone configurations (Figure 5-42). You cannot modify an effective zone configuration.

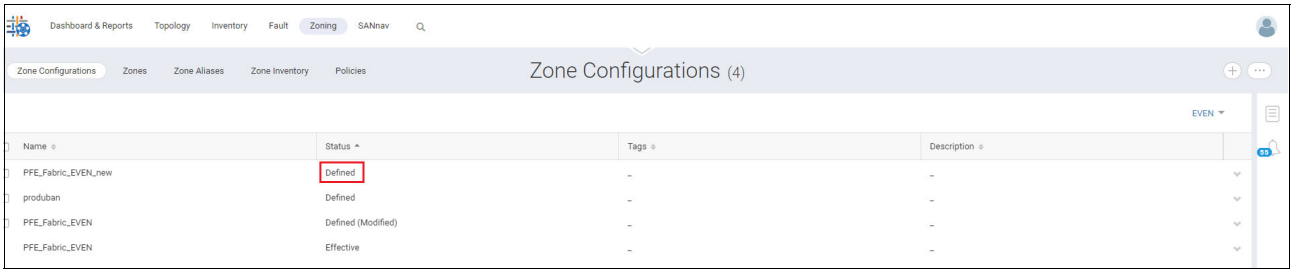


Figure 5-42 Modifying the configuration

3. To modify a zone configuration, drill down to the zone configuration with the `Defined`, `Defined (Copy)`, or `Defined (Modified)` status.
4. To add a zone, click **Add**, select the zone in the Add Zones window, and then click **OK**. To remove a zone, select the zone that you want to remove, and then click **Remove**. The zone is removed from the Zones list.
5. You can save the zone configuration or activate the zone configuration. To save the zone configuration, click **Save**, and then click either **Save** or **Save As** if you want to save the configuration with a different name. The Save Zone Configuration confirmation window opens. Click **OK** to save the changes. You can compare the changes before saving the zone configuration by clicking **Compare**.
6. To activate the zone configuration, select the **Activate** option from the **Actions** menu. The Activate Zone Configuration confirmation window opens. Click **Next** to activate the zone configuration (Figure 5-43 on page 145). For more information, see “Activating a zone configuration” on page 142.

Figure 5-43 Activating a modified configuration

The modified zone configuration can be viewed under the Zone Configurations window.

Adding multiple zones to a zone configuration

Multiple zones can be selected and added to a zone configuration. The Zones window shows active, inactive, or all (both active and inactive) zones. To narrow a result, you can apply a quick filter. By default, the Zones window shows both active and inactive zones. When you want to add multiple zones to a zone configuration, the quick status filter allows you to filter inactive zones, and then add them to the zone configuration. The quick filter persists across the user session or within the user session based on the Persist Last Filter Selection user preferences.

Note: When you migrate from SANnav v2.2.0 to SANnav v2.2.1, the quick filter shows the default value `All`. The quick filter value persists in the user preferences and migrates to later releases of SANnav.

To select and add multiple zones to a zone configuration, compete the following steps:

1. Click **Zoning** in the navigation bar, and then select **Zones** from the **Zones** drop-down menu. The Zones window opens.
2. Select the fabric from the **Select Fabric** drop-down menu, and then click **OK**.

   If a zone is a part of the active zone configuration, the zone is showed with two entries in the Zones window: One is for the active zone, and another one is for the defined copy. Active zones cannot be added to the zone configuration through the **Add to Zone Config** option. The Zones window shows the list of zones for the selected fabric.
3. Select the **Inactive** option from the quick status filter. The Zones window shows the zones that are part of any defined zone configuration or not part of any active zone configuration (stand-alone zones).
4. Click **More (…)** at the upper right of the window, and then select **Bulk Select**. The select options for the zones are showed.

5. Select the zones to add to the existing zone configuration, and then select **Add to Zone Config** from the **Actions** drop-down menu, as shown in Figure 5-44.

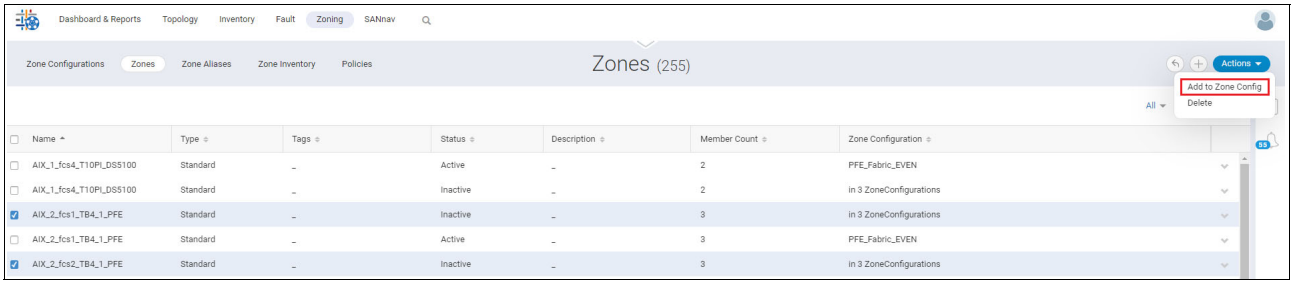


Figure 5-44 Adding multiple zones to the configuration

6. To add a single zone to the zone configuration, click the drop-down arrow next to a zone, and then select the **Add to Zone Config** option, as shown in Figure 5-45.

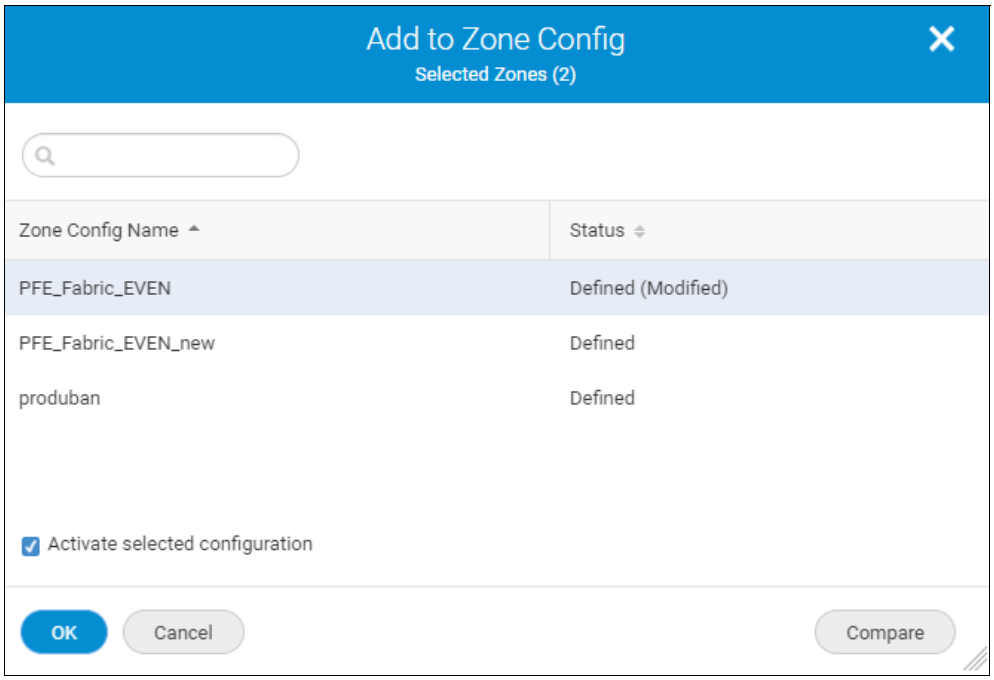


Figure 5-45 Add to Zone Config

7. Select the zone configuration to which you want to add the zones. Select the **Activate selected configuration** checkbox to activate the zone configuration. If you do not select this checkbox, the zones are added to the zone configuration, but the configuration is not activated. To activate a zone configuration, see “Activating a zone configuration” on page 142.

Note: While adding changes to a zone configuration, **Compare** is available to view the changes between the effective zone configuration and the selected zone configuration. The selected zone configuration can be a **Defined (Copy)**, **Defined**, or **Defined (Modified)** copy. For more information about comparing zone configurations, see “Comparing defined with the effective zone configurations” on page 147.

8. Click **OK**. The zones are added to the selected zone configuration.

Comparing defined with the effective zone configurations

The compare zone configuration feature supports comparing a defined zone configuration with the effective zone configuration. The **Compare** feature is available while saving or activating the defined zone configuration.

The differences between effective and defined zone configurations are represented in a tree structure. The newly added, removed, and modified zone entities (zones, zone aliases, and zone members) are showed with clear semantic differences. You can view the differences between an effective and a defined zone only.

The Compare window compares the zone configuration (with the changes that are performed in one or more sessions) that is either selected or opened with the effective zone configuration, and it shows the differences. The differences are showed in a tree structure with zones, zone aliases, and zone members.

The Compare window lists the differences as modified, removed, added zones, or zone members. The added, modified, and removed zoning entities are showed with clear semantic differences:

- The changes are shown in the right pane, which shows the defined configuration.
- The left pane shows the effective configuration of the zone name that is involved in modification or removal.

The Compare and Activate Zone Configuration dialog box is launched automatically when you activate a zone configuration. This feature helps users by avoiding an extra step to invoke **Compare**. This behavior is enabled by default. You can configure this behavior by enabling or disabling the **Show Compare Dialog on Zone Configuration Activation** parameter in the User Preferences window. When this parameter is enabled, the Compare and Activate Zone Configuration dialog box appears automatically when a zone configuration is about to be activated.

Notes:

- When you migrate from SANnav v2.1.x or v2.2.0 to SANnav v2.2.1, the **Show Compare Dialog on Zone Configuration Activation** parameter is enabled by default.
- You can enable or disable the **Show Compare Dialog on Zone Configuration Activation** parameter regardless of the roles to change the user preference option.

To compare configurations between effective and defined (modified) or defined zone configurations, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select **Zone Configurations**. The Zone Configurations window opens.
2. Select the fabric from the **Select Fabric** drop-down menu, and then click **OK**. The recent modification of an effective zone configuration appears as `Defined (Modified)` in the Zone Configurations window. The modified copy of a zone configuration appears as `Defined`. The **Compare** option is visible for all zone configurations in the Zone Configurations list. You can also view the Compare and Activate Zone Configuration dialog box while attempting to activate a zone configuration.

3. You can compare an effective zone configuration with the defined (modified) or defined zone configuration directly from the Zone Configurations window. To compare configurations between the effective and defined (modified) or defined zone configurations, select **Compare** for the defined (modified) or defined zone configuration, as shown in Figure 5-46.

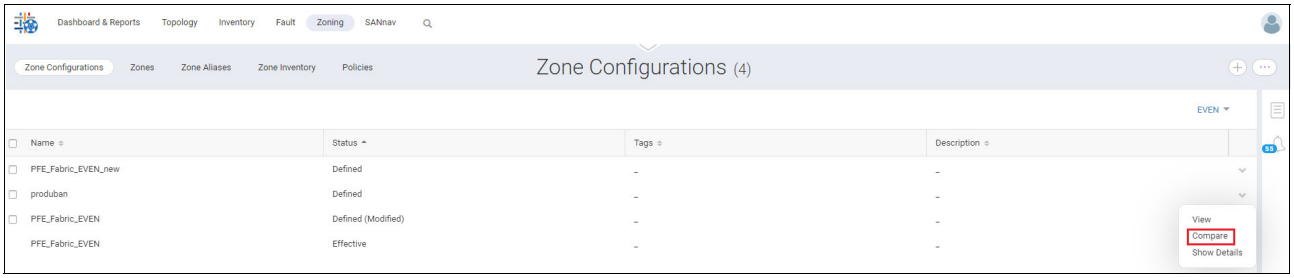


Figure 5-46 Comparing configurations

You can also compare an effective and defined (modified) zone configurations by selecting **Compare** from the effective zone configuration.

4. You can compare and activate a zone configuration by activating a defined (modified) or defined zone configuration. To compare configurations between the effective and defined (modified) or defined zone configurations, drill down to the defined (modified) or defined zone configuration and activate the zone configuration by selecting **Activate** from the **Actions** menu, as shown in Figure 5-47.

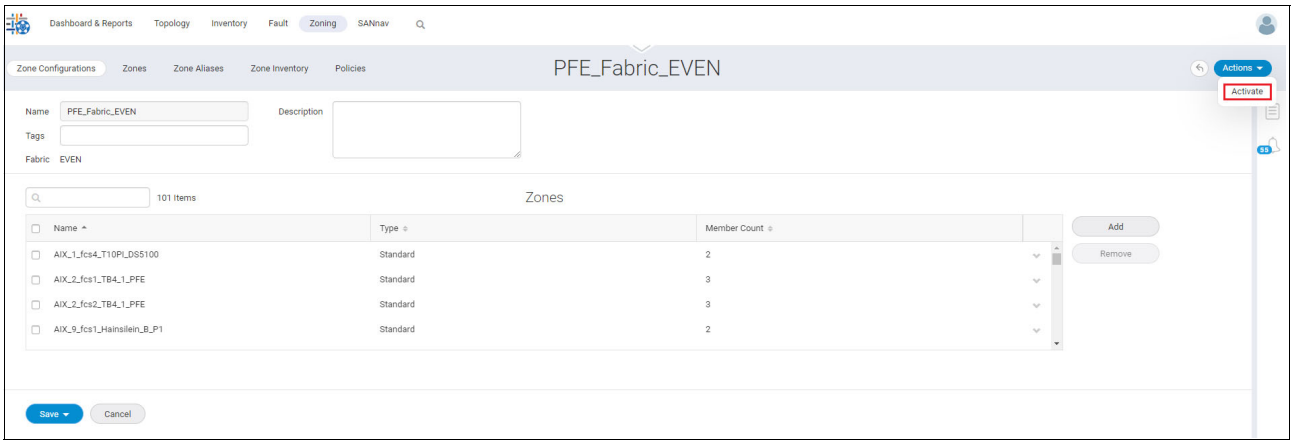


Figure 5-47 Activating a configuration

The Activate Zone Configuration window opens (Figure 5-48 on page 149).

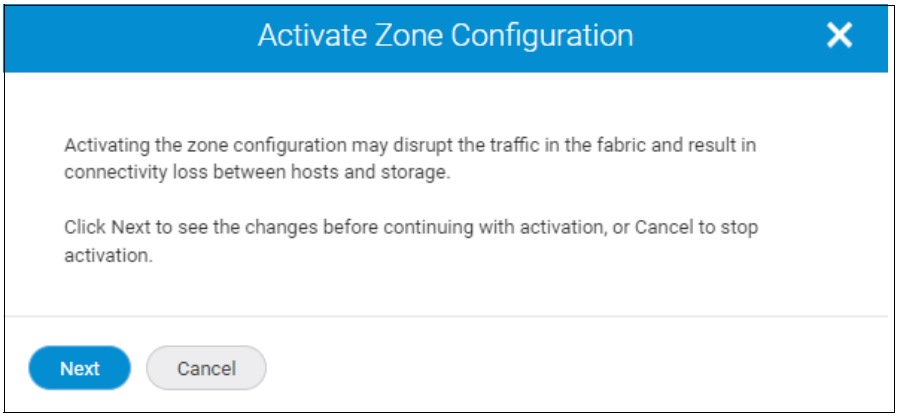


Figure 5-48 Activate Zone Configuration confirmation message

5. Click **Next**.

Notes:

- When a Compare dialog box is launched as part of the activation process based on the user preferences (when the **Show Compare Dialog on Zone Configuration Activation** parameter is enabled) and if there are any changes to the zone database of the fabric, the Compare and Activate Zone Configuration dialog box is launched to refresh the Compare dialog box content.
- While launching the Compare dialog box as part of the activation process, if both zone configurations are identical, the Compare and Activate Zone Configuration dialog box shows a message to continue activating the zone configuration.
- SANnav supports a maximum of 10 open zone configuration comparisons across the SANnav instance.

The Compare and Activate Zone Configuration window opens (Figure 5-49).

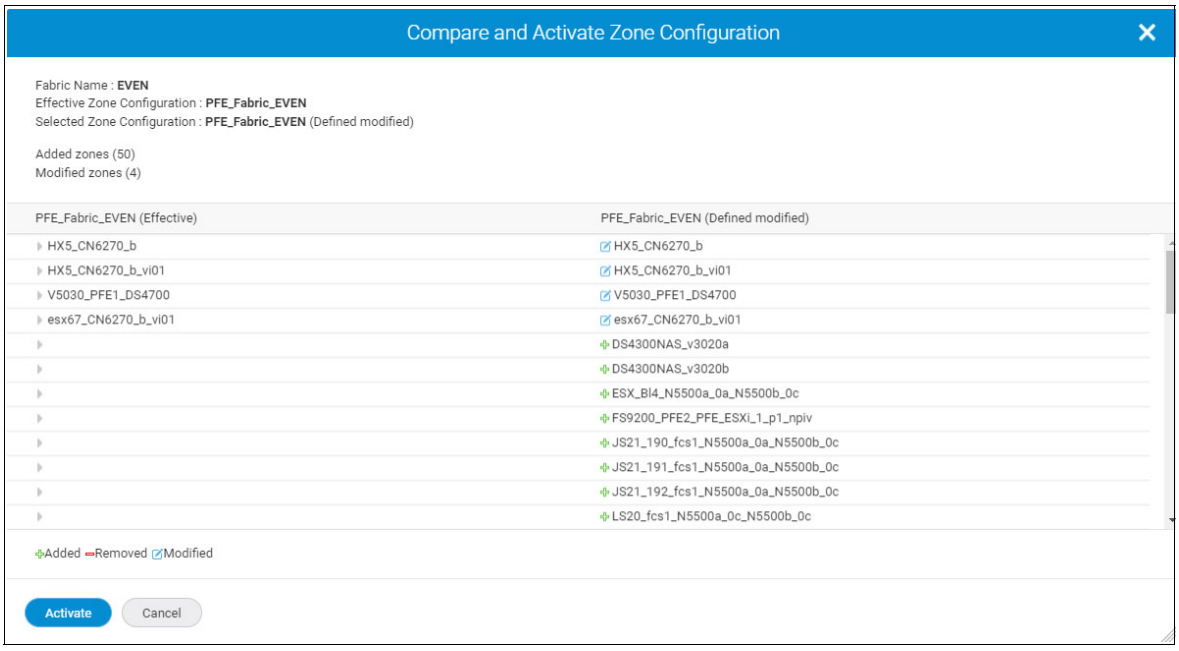


Figure 5-49 Compare and Activate

6. After viewing the changes between the effective and defined zone configurations, click **Activate** to activate the defined zone configuration.

Viewing zone and zone configuration details

You can view the following details in the same window:

- A list of available zone aliases in a zone.
- A list of available alias members in a zone alias.

You can view the details for all zones.

To view the details about zones, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select **Zones** from the **Zones** drop-down menu. The Zones window opens.
2. Select a fabric from the **Select Fabric** option, and then click **OK**. A list of zones for the selected fabric appears.
3. Select the **Show Details** option for an individual zone from the action drop-down menu. The Zone Details window opens and shows the list of zones that are present in the fabric.
4. To view the list of zone aliases that are present in a particular zone, select a zone from the **Zones** list. To view any alias members that are present in the zone alias, select the zone alias name from the **Members** list (Figure 5-50).

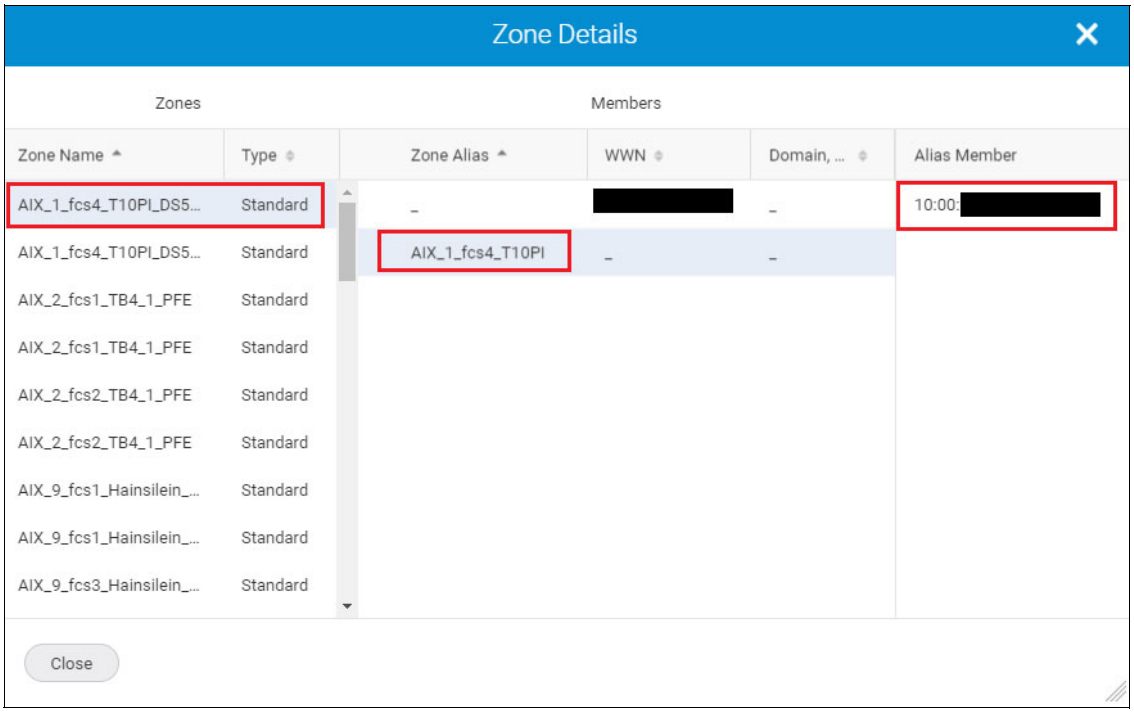


Figure 5-50 Zone details

The list of alias members appears in the Members list.

Note: The principal members in a peer zone are highlighted with the ( ) symbol.

You can view the following details on the same window:

- A list of available zones in a zone configuration
- A list of available zone aliases in a zone
- A list of available alias members in a zone alias

You can view the details for all zone configurations or for a single zone configuration. By using the **Show Details** option, you can view details for existing zones that are part of the zone configuration. It is not applicable for newly created zones or for adding existing zones to the zone configuration.

To view the details about zone configurations, complete the following steps:

1. Click **Zoning** in the navigation bar. The Zone Configurations window opens.
2. Select a fabric from the **Select Fabric** option, and then click **OK**. A list of zone configurations for the selected fabric shows.
3. Select the **Show Details** option from the **Actions** drop-down menu. The Zone Configuration Details window opens and shows the list of configured zones that are present in the fabric.
4. To view the list of zones that are present in a particular zone configuration, select a zone configuration from the **Zone Configurations** list. To view the zone aliases present in a zone, select a zone from the **Zones** list. To view any alias members present in the zone alias, select the zone alias name from the **Members** list.

5.6.6 Creating a zoning report

You can create a report of all zone objects in the discovered fabrics, including unzoned devices. This report is created by using the Zoning widget.

The zoning report consists of two types of tables:

- Zone summary table
- Unzoned devices table

Zone summary table

This table provides complete information about all zone configurations in all discovered fabrics. The zone summary table identifies and lists the dangling zones that do not belong to any zone configuration. The zone summary table includes default columns such as fabric, zone configuration, zone, zone type, status, alias, alias type, member, port role, logged in, vendor, and slot or port number.

Note: You can view the port role and vendor columns in the zone summary table for device ports. For switch ports, these columns are empty.

Unzoned devices table

The unzoned devices table lists all the unzoned and unaliased devices of a fabric. The unzoned device table includes default columns such as device port WWN, device node WWN, port role, alias, host or storage name, connected product, connected product port, logged in, and vendor.

Note: You can view the port role, logged in, and vendor columns in the unzoned devices table for device ports.

The zoning report is based on the fabric filter. You can add a few more columns while generating the report in CSV format.

To view a zoning report, complete the following steps:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Click **+** in the upper right, and then select **Report** → **Select Widgets** from the available options. The Select Widgets window opens (Figure 5-51).

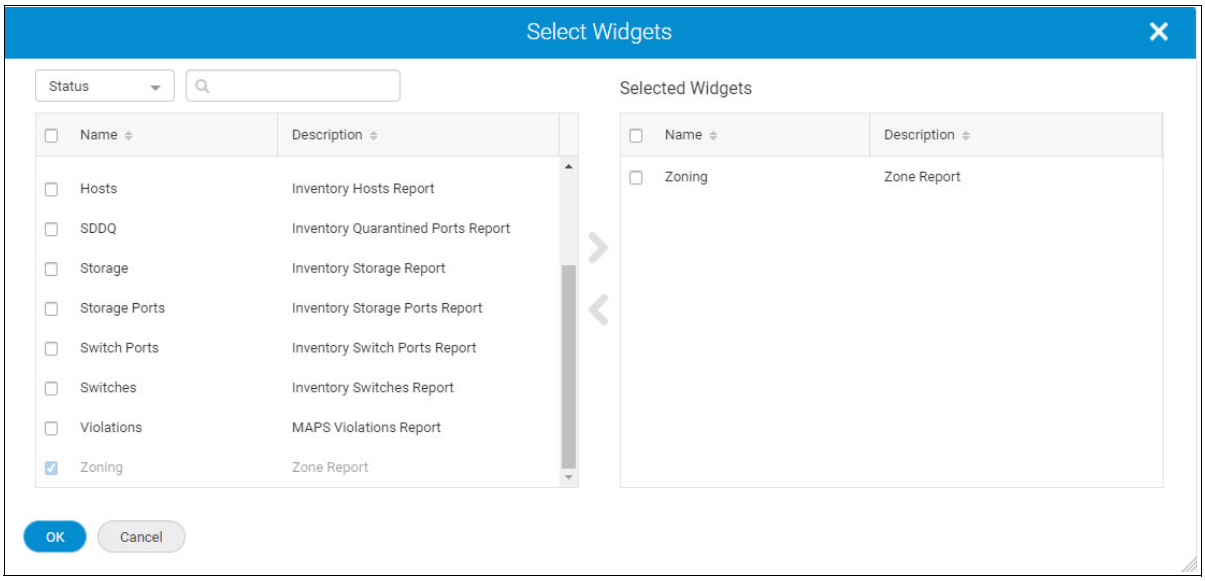


Figure 5-51 Creating a zoning report

3. Select **Status** from the drop-down list, and then select the **Zoning** widget and click the right arrow to move it to the right side of the window. The **Zoning** widget is moved under Selected Widgets (Figure 5-52).

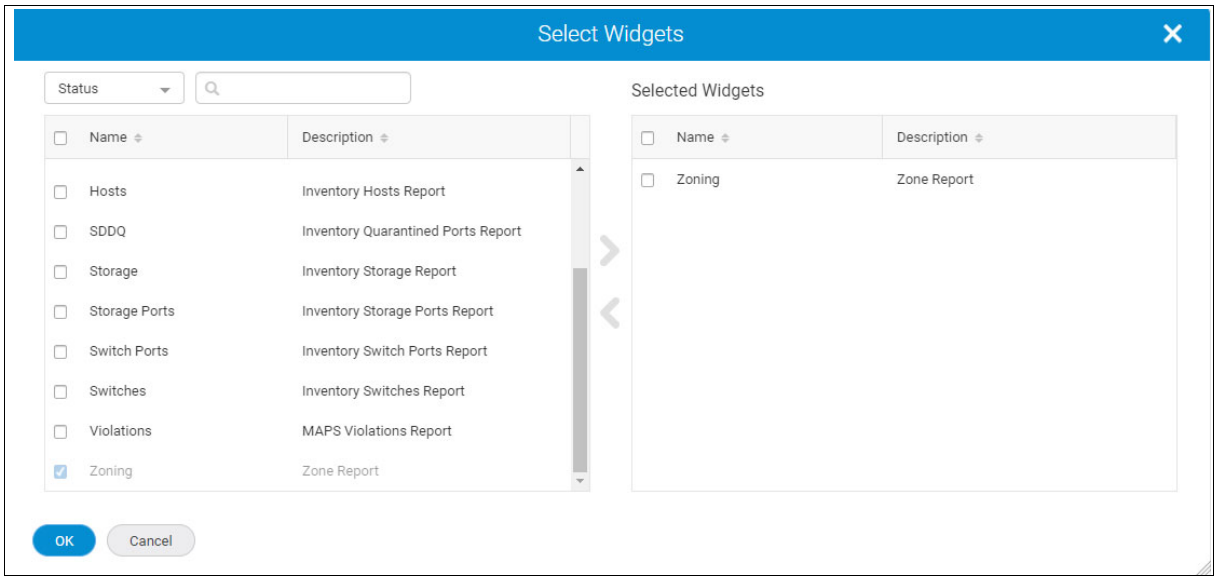


Figure 5-52 Creating a zoning report: Select Widgets

4. Click **OK**. The Create New Report Template window opens.

The Create New Report Template lists the zoned and unzoned device tables. For more information, see 5.9.1, “Creating a report template ” on page 212.

5. Click **Save**.

   To generate your report, go to the Templates window and select **Generate Report** from the action menu. To schedule a report to run later, select **Schedule**. To view the report output, go to the Reports window and export the individual or bulk reports. You can export the data in CSV format.

5.6.7 Configuring the zoning policy

The zoning policy controls device access if zoning is not implemented or if there is no effective zone configuration. The zoning policy has two options:

- **All Access**: All devices within the fabric can communicate with all other devices.
- **No Access**: Devices in the fabric cannot access any other device in the fabric.

The zoning policy applies to the entire fabric, regardless of the switch model. The default setting is **All Access**.

When you disable the zoning configuration in a large fabric with thousands of devices, the name server indicates to all hosts that they can communicate with each other. Each host can receive an enormous list of PIDs and ultimately cause other hosts to run out of memory or crash. To ensure that all devices in a fabric do not see each other during a configuration disable operation, set the default zoning policy to **No Access**.

Note: For switches in large fabrics, the default zone policy must be set to **No Access**. If the default zone policy is **All Access** and you have more than 120 devices in the fabric, you cannot deactivate the active configuration.

To modify the fabric policies, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Policies** tab to view the list of fabrics.
2. Select one or more fabrics from the list.
3. Click the **Actions** drop-down menu and select **Enable (All Access)** or **Disable (No Access)** (Figure 5-53).

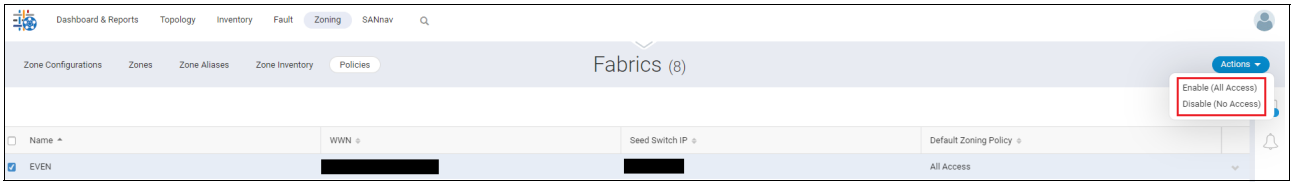


Figure 5-53 Configure Zoning Policy

Alternatively, you can change the policy for a single fabric by selecting **Enable (All Access)** or **Disable (No Access)** from the action menu for that fabric.

Note: When a fabric policy is changed from **No Access** to **All Access** or vice-versa and a fabric-lock occurs, the following error message appears:

```
Failed to save zone. Another transaction from switch in this fabric is in
progress and will take approximately <minutes:seconds> to complete.
```

You can view the error message by clicking **Fault** in the navigation bar and then selecting the **Events** tab.

5.6.8 Zone inventory management

The Zone Inventory window provides a complete list of all zone members across all fabrics and also provides a member-centric view.

You can view the zone members with complete details about the member, such as alias name, zone name, zone configuration name, the fabric, and status of the zone alias. The Zone Inventory list shows one zone member (WWN and Domain, Port Index) per row. When you access the Zone Inventory window, by default the **All Fabrics** option is selected. However, the Zone Inventory list initially is empty, so you must have a search term or filter that is applied to view the member list. The search filter works with the other applied filters. The Zone Inventory list supports sorting by two columns. The quick filters and any other applied filters persist across the user session and within the user session.

The Zone Inventory window shows detailed information about all zone members in the tabular format. Using tags, custom filters, and quick filters, you can search, sort, and filter the information to show exactly the data that you need. SANnav supports applying search, multiple filters, and quick filters simultaneously, as shown in Figure 5-54.

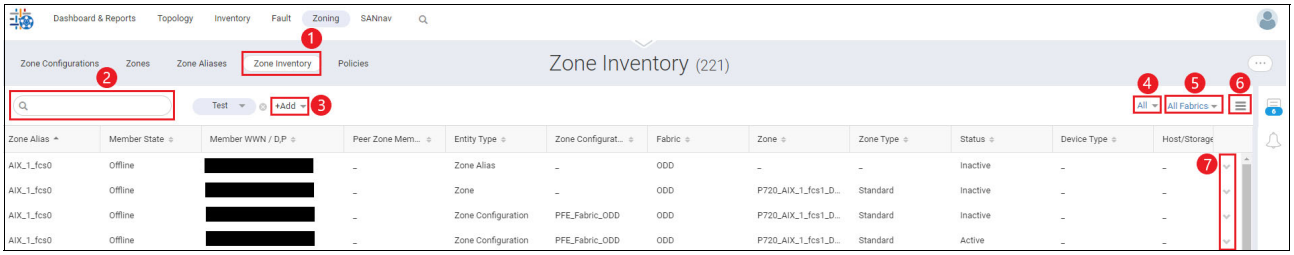


Figure 5-54 Zone Inventory

To use the Zone Inventory function, complete the following steps:

1. Click **Zoning** in the navigation bar to access the Zone Inventory window.
2. Search for the zone member or zone alias to view its details.
3. In the Zone filters view, click **+Add** to add more filter criteria:
   - Status quick filter
   - Fabric quick filter
4. Customize which columns are showed in the table and in which order.
5. Click the action menu to launch the zoning operations.

Exporting zone inventory data

SANnav supports exporting or downloading zone inventory data with the selected columns in the Zone Inventory window as the CSV file. The columns that are showed in the Zone Inventory window after applying quick filters, filters, and search filters are downloaded as a CSV file to your local machine.

To export or download the zone members with the selected columns, complete the following steps:

1. Click **Zoning** in the navigation bar, and then select **Zone Inventory**.
2. You can apply quick filters, filters, or search filters to view zone inventory data. You can also go to the Zone Inventory window from the Zone Summary Widgets window by using the **Filter by this Item** option. You can customize the columns that you want to export to the CSV. You can export all matching zone inventory data to the CSV file, as shown in Figure 5-55.

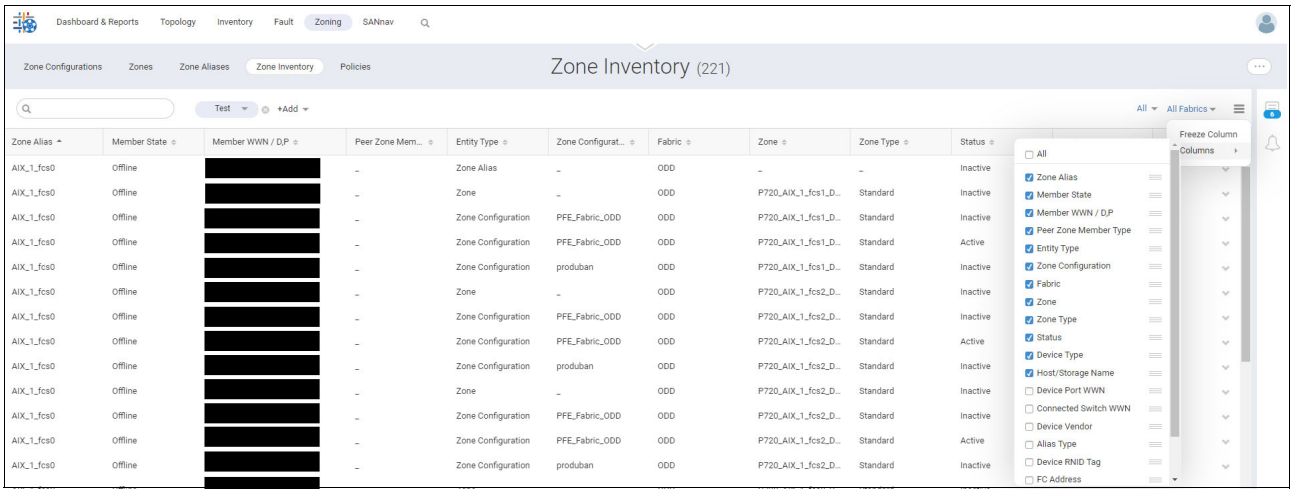


Figure 5-55 Exporting Zone Inventory

3. Click **More (...)** in the upper right of the window, and then select **Export** (Figure 5-56).

Figure 5-56 Exporting Zone Inventory

The zone inventory data is exported as a CSV file to your local machine.

Zone inventory actions

You can initiate various zone configuration operations by using the Zone Inventory window. Using different options in the action menu, you can complete the following operations:

- Remove multiple zone aliases that represent the same WWN member.
- Modify zones with mixed zone members.
- Add zone aliases to one or more zones.
- Add a zone to one or more zone configurations.
- Modify zones by removing, replacing, and adding members to zones.
- Identify zones or zone aliases by zone member, zone alias, zone or configuration name, and rename them in bulk for a clear naming convention.
- Identify unaliased device ports and create zone aliases.
- Identify zones that are not part of any zone configuration.

- Identify and remove or replace offline zone members with other members.
- Add zone members to one or more zones.
- Identify empty zones and remove them in bulk.
- Decommission host or storage ports from a fabric.

5.6.9 Policy-based zone creation

SANnav supports creating zones in bulk from hosts, hosts ports, and storage ports from the Inventory window based on the selected policy.

You can select *N* number of initiators and *M* number of targets to create zones based on the chosen policy type. This feature helps to create multiple zones instead of having all chosen members in a single zone.

Here are the available policy types:

- **I-T** (initiator to target): When you select the I-T policy and three initiators and three targets from a single fabric are connected, nine zones are created. If the initiators and targets are from different fabrics, three zones are created.
- **I-*** (one initiator to multiple targets): When you select the I-* policy and three initiators and three targets from a single fabric are connected, three zones are created. Each zone contains one initiator and three targets. If the initiators and targets are from different fabrics, three zones are created. Each zone contains one initiator and three targets.
- ***-T** (multiple initiators to a single target): When you select the *-T policy and three initiators and three targets from a single fabric are connected, three zones are created. Each zone contains one target and three initiators. If the initiators and targets are from different fabrics, three zones are created. Each zone contains one target and three initiators.

The default policy type is I-T, and the basic zone type is Standard.

SAN administrators can modify the policy type and zone type with the advanced zoning privilege. Users with the simplified zoning privilege can create zones with the I-T policy and standard zone type only. These users can never change these options, and an advanced zoning user cannot change them for them. The number of zones that are created for each fabric depends on the connectivity and the policy that is chosen.

SANnav supports creating zones in multiple fabrics according to the host and storage port connectivity based on the policy. When you select initiator ports that are connected to multiple fabrics (multipathing), SANnav lists all connected storage ports from all those fabrics. When you select **All Fabrics**, all ports belonging to the source selected fabrics are shown, and you can create zones in multiple fabrics by using this option.

By default, the newly created policy-based zones are added to the active zone configuration of the fabric. If the fabric does not have any active zone configuration, SANnav automatically creates an active configuration that is named `PolicyBasedZoneConfig` and adds the newly created zones to it.

Connecting new HBA ports to a fabric by server administrators

Server administrators have a simplified zoning privilege, and they cannot launch a zoning view to create zones. Therefore, server administrators must create zones from the host ports list on the Inventory window.

To connect new HBA ports to a fabric to communicate with designated storage by the server administrator, complete the following steps:

1. Click **Inventory** from the navigation bar, and then select **Host Ports** from the drop-down menu.
2. Select the fabric from the **All Fabrics** drop-down menu. The Host Ports window opens with the list of host ports.
3. Locate the ports for which you want to create zones. Bulk select ports, and then select **Create Zone** from the **Actions** drop-down menu (Figure 5-57).

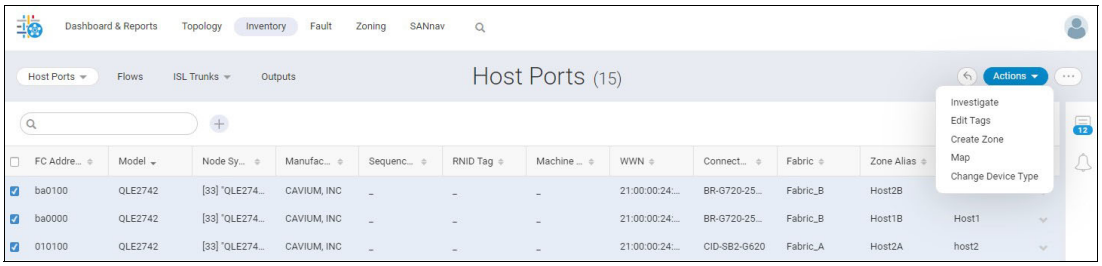


Figure 5-57 Connecting HBA ports to a fabric by server administrators

The Create Zone window opens.

4. Select storage ports from the required fabric, and then add them to the Selected Members table.

Note: By default, SANnav shows the policy type as I-T and the zone type as Standard.

5. Click **Next** to name the zones.
6. Generate zone names automatically or manually.

Server administrators connecting new HBA ports to multiple fabrics (multipathing)

Server administrators have a simplified zoning privilege, so they cannot launch the zoning view to create zones. For multipathing, your host must be connected to more than one fabric. Therefore, server administrators must create zones from the hosts list on the Inventory window.

For a server administrator to connect HBA ports to multiple fabrics to communicate with the designated storage, they must complete the following steps:

1. Click **Inventory** from the navigation bar, and then select **Hosts** from the drop-down menu. The Hosts window opens.
2. Select the host that is connected to multiple fabrics, and then select the **Create Zone** option from the action menu.

Note: To check whether a host is connected to multiple fabrics, drill down to the host and check the Connected Fabric column from the Host Ports table. If the host is connected to multiple fabrics, the Connected Fabric column shows multiple fabrics. The Create Zone window opens.

3. Select storage ports from the required fabric, and then add them to the Selected Members table. You can add ports from multiple fabrics one by one, and then click **Next** to name the zones (Figure 5-58).

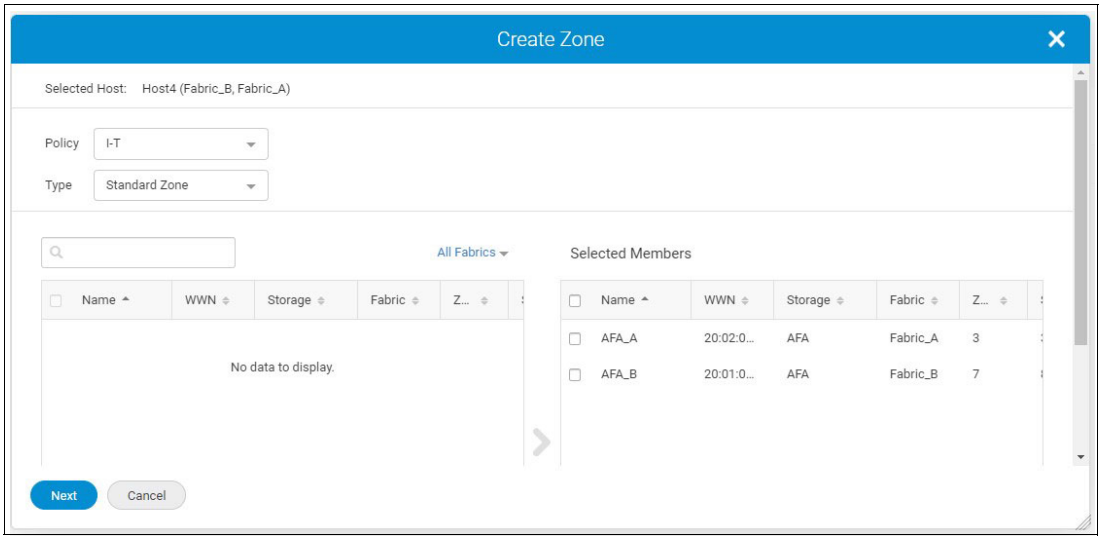


Figure 5-58 A server administrator connecting HBA ports to multiple fabrics (multipathing)

4. Generate zone names automatically or manually. The zones are created in multiple fabrics.

Server administrators connecting new HBA ports from one edge fabric to another edge fabric

Server administrators have a simplified zoning privilege, so they cannot launch the zoning view to create zones.

To connect new HBA ports from one edge or backbone fabric to another edge or backbone fabric, complete the following steps:

1. Click **Inventory** from the navigation bar, and then select **Hosts** from the drop-down menu. The Hosts window opens.
2. Select the edge or backbone fabric from the **All Fabrics** drop-down menu. The Host Ports window opens with the list of host ports.
3. Locate ports for which you want to create zones. Bulk select ports, and then select **Create Zone** from the **Actions** drop-down menu.
4. Select storage ports from another edge or backbone fabric, add them to the **Selected Members** table, and then click **Next** to name the zones.
5. Generate zone names automatically or manually. The new LSAN zones are created in both fabrics. The Create Zone window summarizes the updates.

Administrators connecting new HBA ports to a fabric without launching the zoning view

An administrator can connect new HBA ports to a fabric without launching the zoning view. Server administrators cannot perform this operation without the advanced zoning privilege.

For an administrator to connect new HBA ports to a fabric, they must complete the following steps:

1. Click **Inventory** from the navigation bar, and then select **Host Ports** or **Storage Ports** from the drop-down menu.
2. Select the fabric from the **All Fabrics** drop-down menu. The Host Ports or Storage Ports window opens with the list of host or storage ports.
3. Locate ports for which you want to create zones. Bulk select ports, and then select **Create Zone** from the **Actions** drop-down menu. The Create Zone window opens.
4. Select the policy type and zone type.
5. Select storage ports from the required fabric, add them to the **Selected Members** table, and then click **Next** to name zones (Figure 5-59).

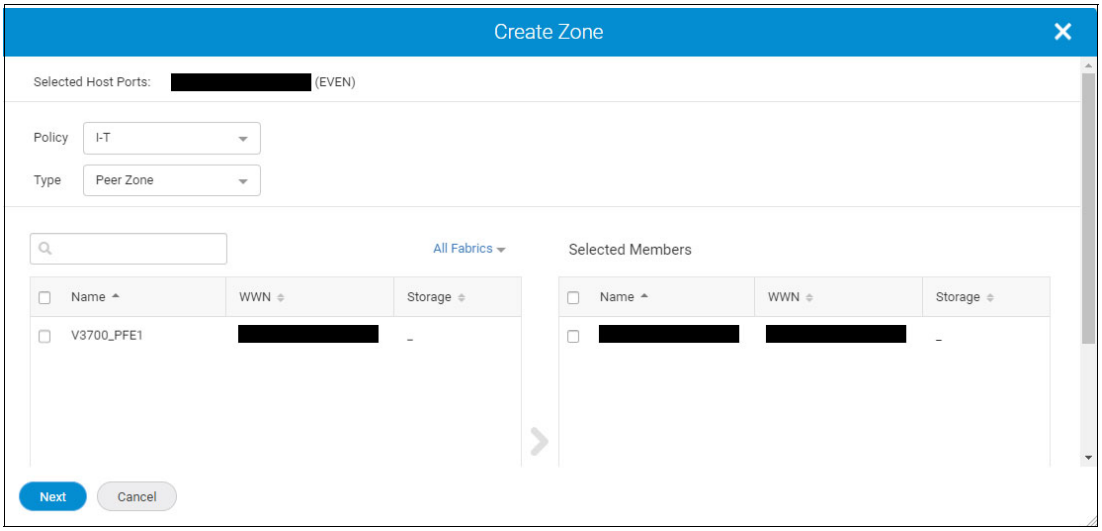


Figure 5-59 Administrators connecting new HBA ports to a fabric without launching the zoning view

6. Generate zone names automatically or manually. The Create Zone window summarizes the newly created zones. By default, the newly created policy-based zones are added to the active zone configuration of the fabric. If the fabric does not have an active zone configuration, SANnav automatically creates an active configuration that is named `PolicyBasedZoneConfig` and adds the newly created zones to it.

5.7 Dashboards

SANnav dashboards give you a functional, seamless, and customizable view of your SAN environments so that you can monitor and troubleshoot them effectively and efficiently.

Some of the key capabilities of dashboards include the following ones:

- Live monitoring of network health and performance
- Standard dashboards
- Ability to build custom dashboard templates for static and dynamic views
- Widgets to monitor switch and port status and error and performance statistics
- Ability to export dashboard widgets to a CSV, PDF, or HTML file
- Ability to customize content by using filters, fabric, and date range

SANnav provides the following dashboards:

- Health Summary
- Network Port Traffic Conditions
- Extension Dashboard

You also can create your own custom dashboards by using system-defined product status and performance widgets. You can share the dashboards with all users and can export them to other SANnav instances.

One of the dashboards is designated as the default dashboard. The default dashboard is the default landing view when you log in to SANnav. The Health Summary dashboard is the default dashboard after installing SANnav. You can select another standard or customized dashboard as the default.

5.7.1 Changing the default dashboard

When you log in to SANnav for the first time, the default landing view is the Health Summary dashboard. You can choose a different dashboard for the default landing view.

You must have Dashboards and Reports privileges with read permission.

Changing the default dashboard can be helpful when you are working repeatedly with a dashboard and you want it to show as the default view until you change it.

The default dashboard is on a per-user basis. Each user can have a personal default dashboard.

To change the default dashboard, complete the following steps:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Select Dashboard** at the upper right of the window.
2. Click the **star** icon next to the dashboard that you want to designate as the default dashboard, and click **OK**.

The dashboard with a blue-colored star now shows in the dashboard view and serves as the default view the next time that you log in.

5.7.2 Health Summary dashboard

The Health Summary dashboard provides an overall view of network health from various perspectives: fabrics, switches, hosts, and storage. You start with an overview picture of network health and then drill down to investigate specific problems (Figure 5-60).

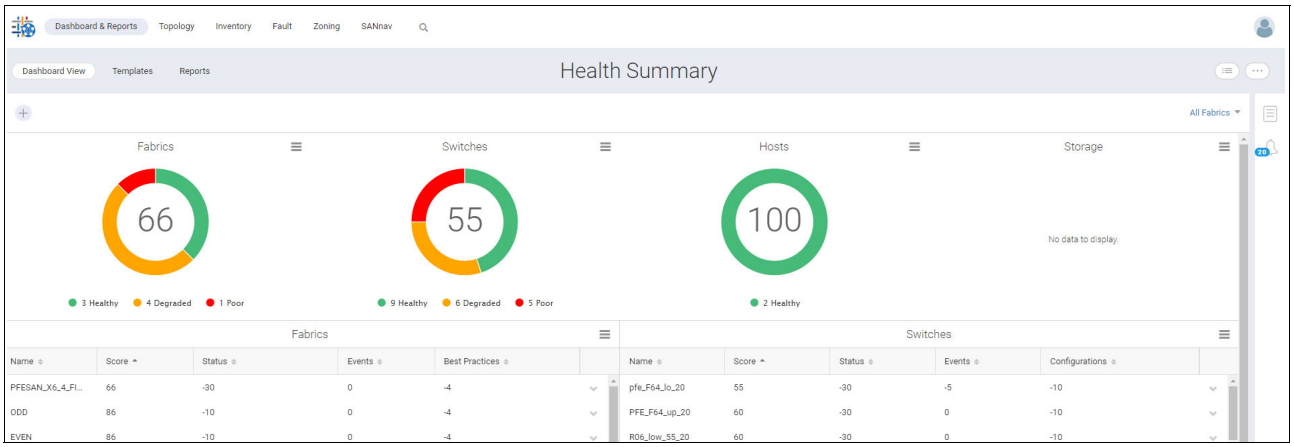


Figure 5-60 Health Summary dashboard

The Health Summary dashboard consists of eight widgets for Fabrics, Switches, Hosts, and Storage in the following layout:

- Four graphical widgets
- Four tabular widgets

For the graphical widgets, the number in the center of each circle is the health score of the least healthy member in that category. For example, if you have 100 switches, of which 99 have a health score of 100 and 1 has a health score of 40, then 40 is showed in the center of the switch circle. In Figure 5-60, the least healthy switch has a score of 55, and the least healthy fabric has a score of 66.

The overall health is determined by the health score:

- If the score is greater than 90, the health is Healthy.
- If the score is 71 - 90, the heath is Degraded.
- If the score is 70 or less, the health is Poor.

The health score is computed based on various factors, such as status, events, and best-practice violations. You can customize how the health score is computed.

The tabular widgets show details about the health score of each member. Click the down arrow at the right of each table entry to show actions that you can take, such as viewing inventory details, showing properties, or (for switches) opening in Web Tools.

By default, all objects in your area of responsibility (AOR) are showed. Using the filter bar, you can create filters and change the network scope if you want to narrow the view. In addition, you can use special tags to exclude objects from the dashboard.

The Health Summary dashboard is automatically updated every 15 minutes when viewed as a dynamic dashboard (from the Dashboard View).

The Health Summary dashboard is one of the predefined dashboards in SANnav, so you cannot modify it to add or delete widgets. However, you can save this dashboard as a custom template or use these widgets in custom dashboards.

5.7.3 Customizing the health score computation for managed entities

SANnav Management Portal computes a health score for fabrics, switches, hosts, and storage. The ideal health score is 100, although certain factors might cause this score to decrease.

You can customize which factors are considered for the health score and the number of points that are deducted for each violation. You also can select whether to include acknowledged events in the health score computation.

To customize the health score computation for managed entities, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** → **Health Score Computation**.
2. Click one of the health-factor lists to show detailed information about factors that contribute to reductions in the health score.

   Figure 5-61 shows how the health score for a fabric is computed.

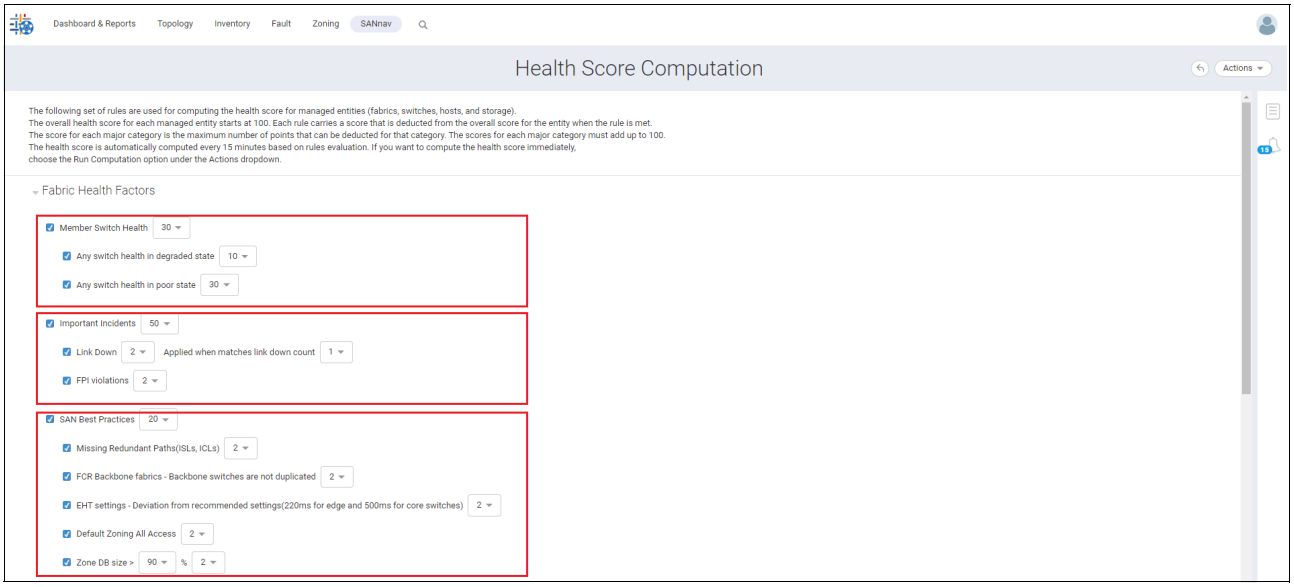


Figure 5-61 Health score computation

The overall fabric health score is determined by three major categories:

- Member Switch
- Health Important Incidents
- SAN Best Practices

The rules under each major category show the number of points that is deducted from the health score if the condition is met. For example, if any switch in the fabric has degraded health, 10 points are deducted from the fabric health score. If any switch in the fabric has poor health, then 30 points are deducted.

The number next to each major category is the maximum number of points that can be deducted for that category. For example, if a fabric contains a switch with degraded health (a 10-point deduction) and a switch with poor health (a 30-point deduction), only 30 points are deducted because the maximum points that can be deducted for the Member Switch Health category is 30.

3. Select or clear the major categories and rules that you want to include or exclude from health score consideration.
4. For each included major category, enter the maximum number of points that can be deducted for that category. The number of points for all included major categories must add up to 100.
5. Under each included major category, enter the number of points to be deducted for each included rule. The number of points for any individual rule cannot exceed the maximum points for the parent category.
6. Select the **Ignore acknowledged events** checkbox at the bottom of the window if you do not want acknowledged events to be considered for the health score. Clearing this checkbox means that acknowledged events are included in the health score computation.

   For the following health factors, score reduction continues to occur regardless of whether the checkbox is selected:

   – Link Down (fabric health factor)
   – COMPASS Config drifts (switch health factor)
7. Click **Save** when you are finished making changes.

At any time, you can select **Actions** → **Restore Default Settings** to go back to the original settings.

The next time that the health score is computed, the Health Summary dashboard reflects the new computations. The health score is computed approximately every 15 minutes. You can force the computation by selecting **Actions** → **Run Computation**.

5.7.4 Excluding entities from the health score computation

You can exclude objects from the health score computation by assigning the special tag `SMP_HSD_IGNORE` to those objects.

For example, you might not want multiple paths between hosts and tape devices. However, by default, points are deducted from the health score for missing redundant paths between host and storage devices. In this case, you can tag the tape storage devices so that multipath connectivity between hosts and the tape devices is not considered in the health score computation.

This example explains how to use the `SMP_HSD_IGNORE` tag to exclude storage ports that are connected to tape devices.

The `SMP_HSD_IGNORE` tag is not case-sensitive, and it can be used with other tags. For example, you can have a tag field with `"tag1,SMP_hsd_ignore,tag2"`.

To tag tape storage devices for exclusion from the health score computation, complete the following steps:

1. Click **Inventory** in the navigation bar, and then select the type of entity that you want to tag (Fabrics, Switches, Hosts, or Storage). For this example, select **Storage**.
2. Click **More** (**…**) in the upper right of the window, and click **Bulk Select**.

3. Select the items that you want to exclude from the health score computation, click the **Actions** drop-down menu, and click **Edit Tags**. For this example, select the tape devices.
4. In the **Edit Tags** dialog box, enter the `SMP_HSD_IGNORE` tag in the Add Tags field, and click **OK**.
5. To refresh the dashboard, complete the following steps:
   a. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** → **Health Score Computation**.
   b. Select **Actions** → **Run Computation** in the upper right to refresh the dashboard.
6. Click **Dashboards & Reports** in the navigation bar to view the updated dashboard. The objects with the `SMP_HSD_IGNORE` tag are excluded from the dashboard.

5.7.5 Refreshing the health score for managed entities

The Health Summary dashboard automatically updates every 15 minutes. You also can update the health score on demand by completing the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring** → **Health Score Computation**.
2. Select **Actions** → **Run Computation** (Figure 5-62).

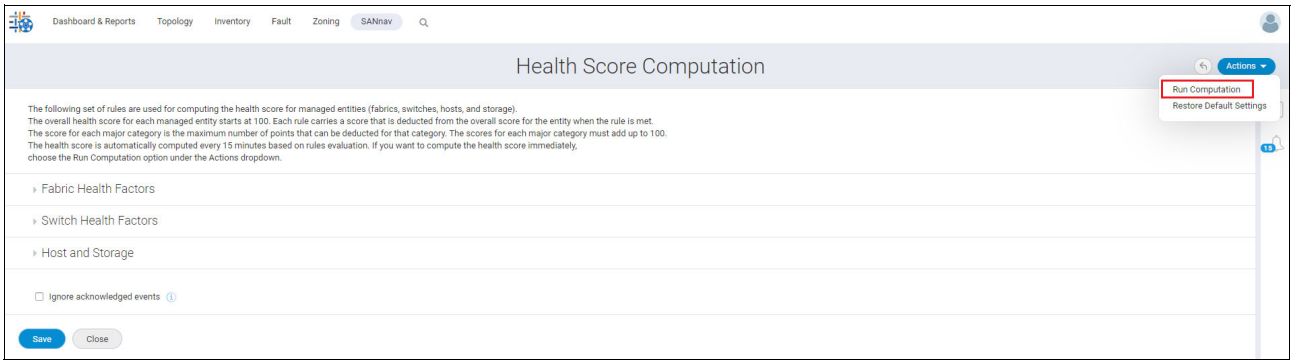


Figure 5-62 Run computation

The computation might take some time to complete. The health score is recomputed and updated in the Health Summary dashboard.

5.7.6 Monitoring the SAN health and status daily

When you check the overall health of the SAN, if you notice problem areas, you can drill down to get more information by completing the following steps:

1. Log in to SANnav Management Portal and click **Dashboard & Reports** in the navigation bar. The default dashboard opens.
2. If the Health Summary dashboard is not the default dashboard, click the **Select Dashboard** icon at the upper right of the window, click **Health Summary** in the table, and click **OK**. (Figure 5-63 on page 165).

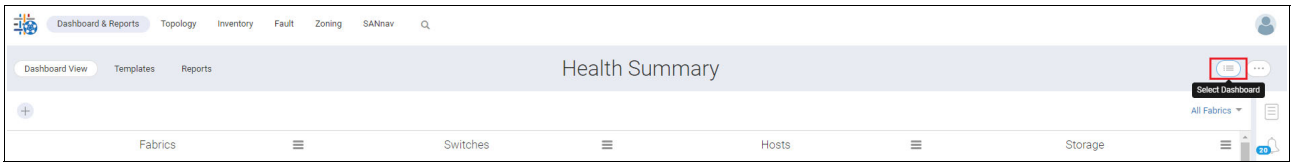


Figure 5-63 Selecting a dashboard

3. In the Health Summary dashboard, click the red or orange areas of the widgets to see a list of items with a poor or degraded score (Figure 5-64).

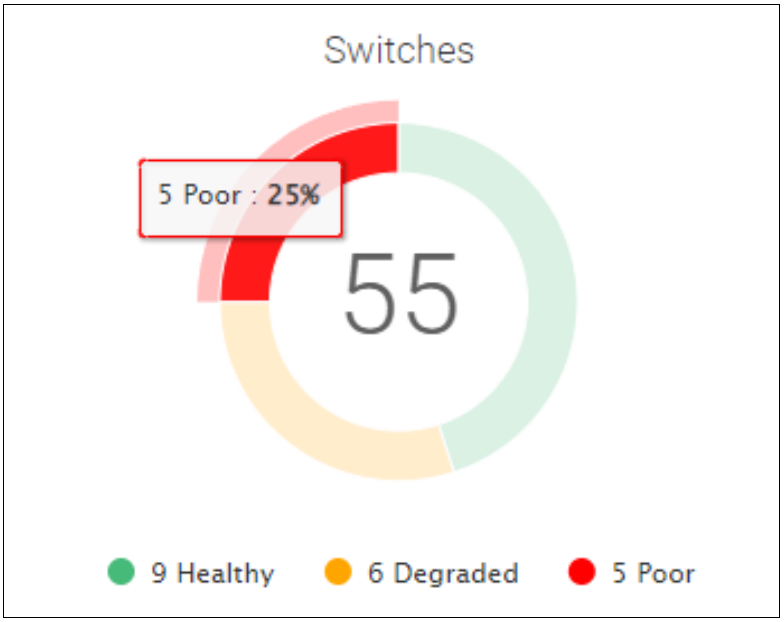


Figure 5-64 Health Summary dashboard: Poor score

A table shows the objects with the associated score, and shows how many points were deducted for each category. This table shows the same information as the table widgets in the dashboard, except that you see only the entries with the associated score. For example, Figure 5-65 shows only the switches with poor health.

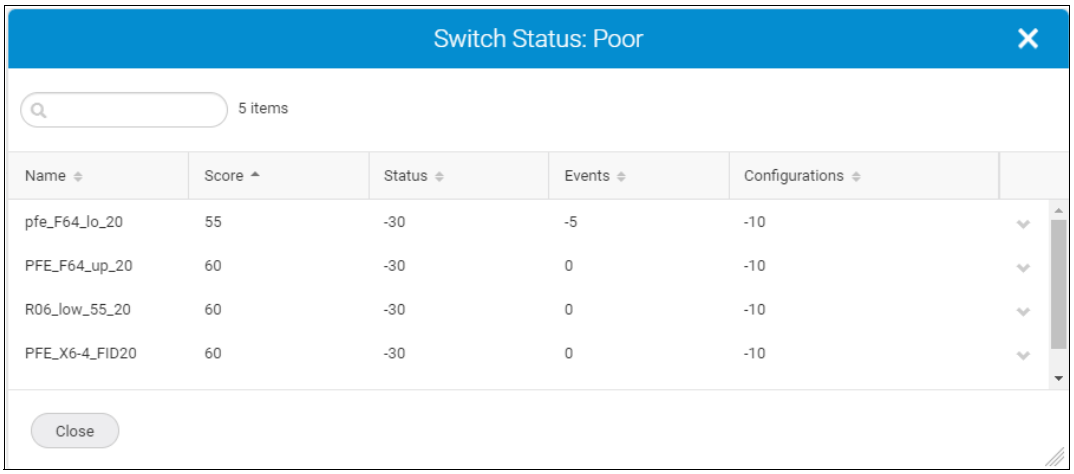


Figure 5-65 Switch Status: Poor

For the first switch in this example, 30 points were deducted for switch status factors, 5 points were deducted for events factors, and 10 points were deducted for configuration factors.

4. Click the down arrow to the right of an entry (the action menu) and click **Show Details** to see the causes for the score deductions and recommendations for fixing.

   The recommendations provide actions that you can take to restore the status to Healthy. The action menu is available both in the dialog box and in the tabular widgets of the Health Summary dashboard (Figure 5-66).

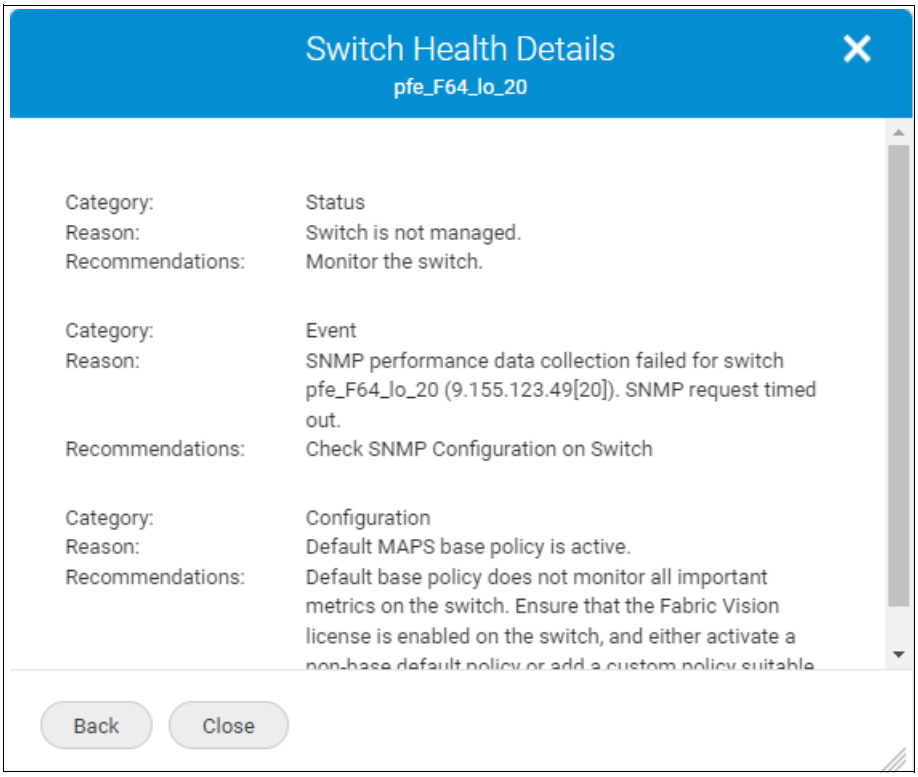


Figure 5-66 Switch Health Details

5. Depending on the causes for the health score deductions, select other options from the action menu to drill down for more details (Figure 5-67).

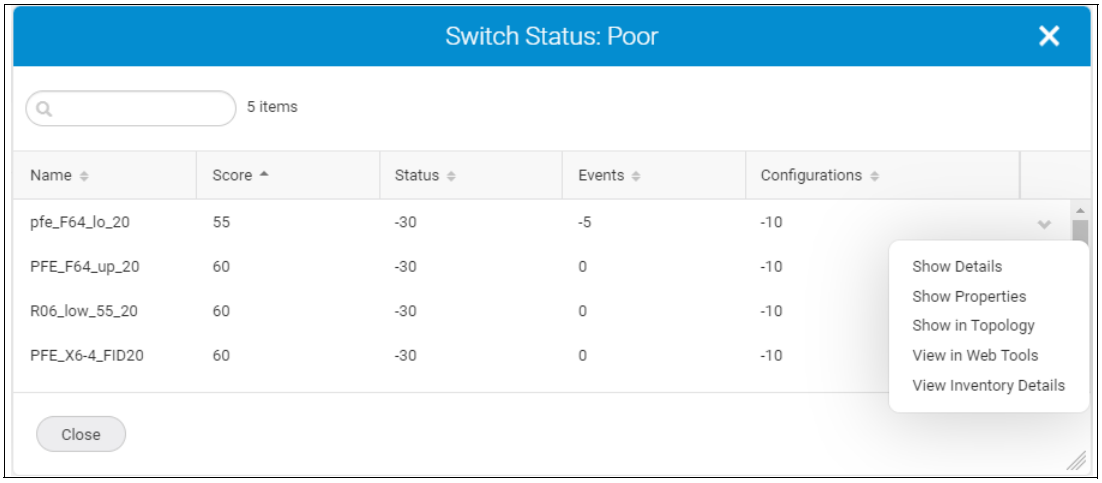


Figure 5-67 Poor action menu

For example, select **View Inventory Details** to look at port optics, set maintenance mode, or disable the switch. The **View in Web Tools** option is available only for switches.

5.7.7 Network Port Traffic Conditions dashboard

The Network Port Traffic Conditions dashboard provides instant visibility into various network traffic conditions across managed fabrics. The dashboard identifies mildly, moderately, or severely congested F_Ports, E_Ports, and EX_Ports across the entire SAN environment, and it shows factors that are contributing to the congestion to help you troubleshoot its cause.

The Network Port Traffic Conditions dashboard is supported on Gen 6 or later platforms operating with FOS 8.2.1 or later with MAPS enabled.

This dashboard provides four widgets that show the top E_Ports, EX_Ports, and F_Ports that are congested or oversubscribed over time. The counts are computed and the graphs are refreshed once every minute, and the counts are showed for the last 30 minutes, 1 hour, or 2 hours. A fifth widget lists the quarantined ports.

Note: For FOS versions earlier than 9.0.0, only congestion data is showed. The Top Oversubscribed Ports and Quarantined Ports widgets are empty.

Figure 5-68 shows the dashboard.

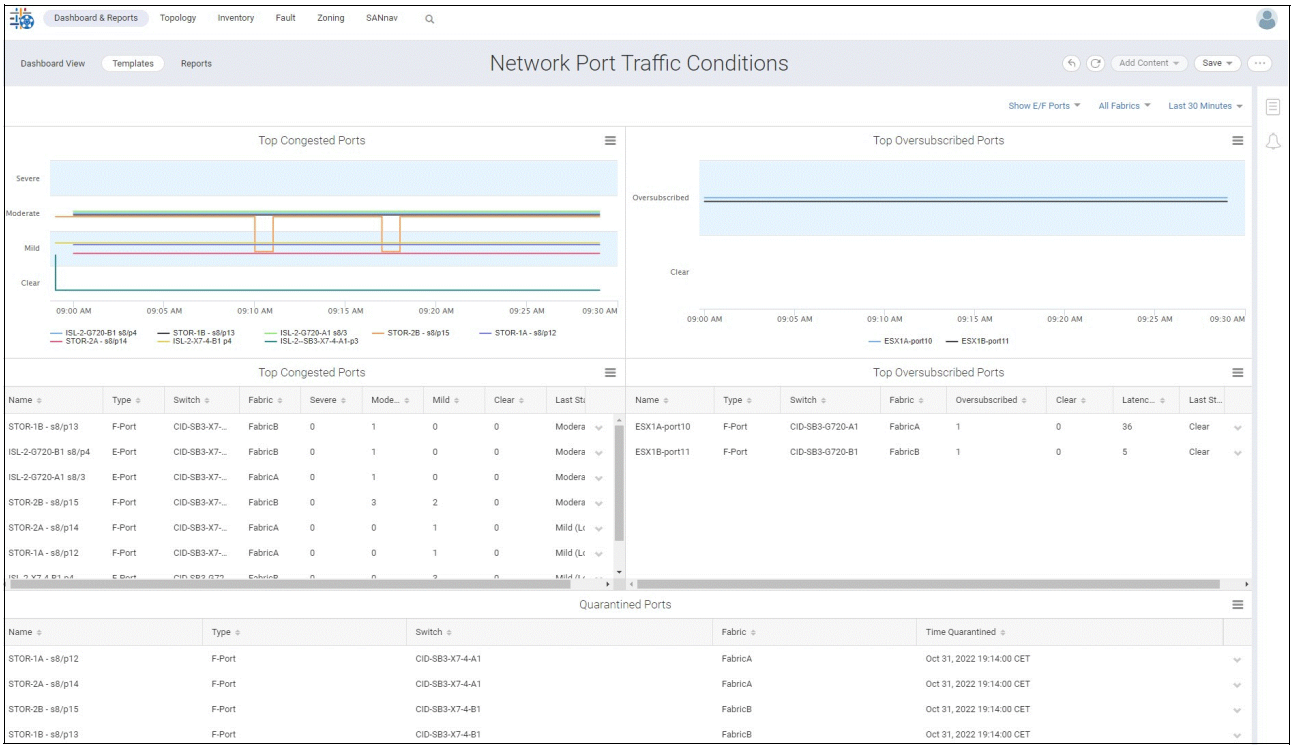


Figure 5-68 Network Port Traffic Conditions dashboard

In the graphical widgets, each port appears as a differently colored line graph. The current time interval that is configured for monitoring ports appears on the **Date Range** drop-down menu at the upper right of the window.

To modify the show, use the following features:

- Click the **Show E/F Ports** drop-down menu at the upper right of the dashboard to show data for specific port types only.
- Customize the network scope and date range by using the drop-down lists on the right side of the filter bar.

5.7.8 Top congested ports and top oversubscribed ports

Congestion is a network traffic condition that occurs when frames enter a fabric faster than they exit the fabric. As a result, frames build up, or congest, in switch ports while waiting for transmission. This causes traffic moving through the fabric to slow down or become “congested”. Congestion can occur on F_Ports, E_Ports, and EX_Ports. Back pressure from a congested port in the fabric can cause traffic to slow down on upstream interswitch links (ISLs) and inter-chassis links (ICLs).

Oversubscription is identified by queue latency on upstream ports and high-bandwidth utilization at a downstream port. Congestion from oversubscription is typically caused by a bandwidth mismatch between the source and destination ports, such as a speed mismatch when a 16G device is sending to a 4G device.

The Top Congested Ports and Top Oversubscribed Ports widgets show the top 10 congested and oversubscribed ports for the network scope and date range. To see this data, complete the following steps:

1. In the charts, click the hamburger icon to launch Troubleshooting Mode or to export the chart as an HTML file.
2. Click ports in the legend below each graph to hide or show the corresponding lines in the graph. For example, in Figure 5-69, the graph lines for port8_4 and port15_4 are hidden.

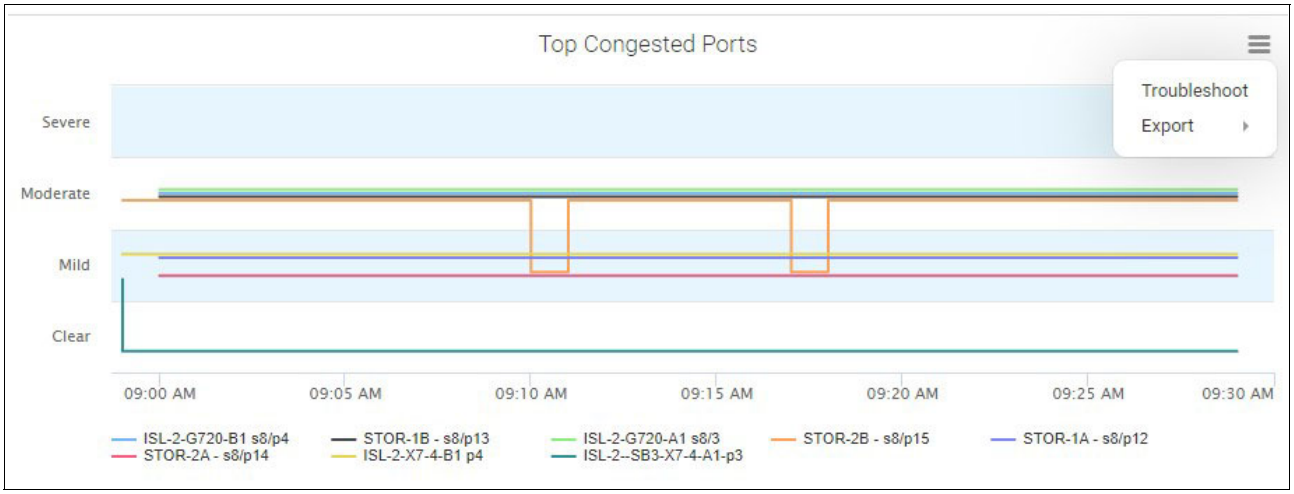


Figure 5-69 Top congested ports

  - In the Top Congested Ports table, the Severe, Moderate, Mild, and Clear columns indicate the number of times that the port went into each congestion state for the date range.
  - In the Top Oversubscribed Ports table, the Oversubscribed and Clear columns indicate the number of times that the port went into each state for the date range.

3. In the tables, click the action menu in the rightmost column to launch Investigation Mode, show port properties, or launch the Topology window for the port. For the congested ports, you can also show the FPI and port health violations from MAPS, as shown in Figure 5-70.

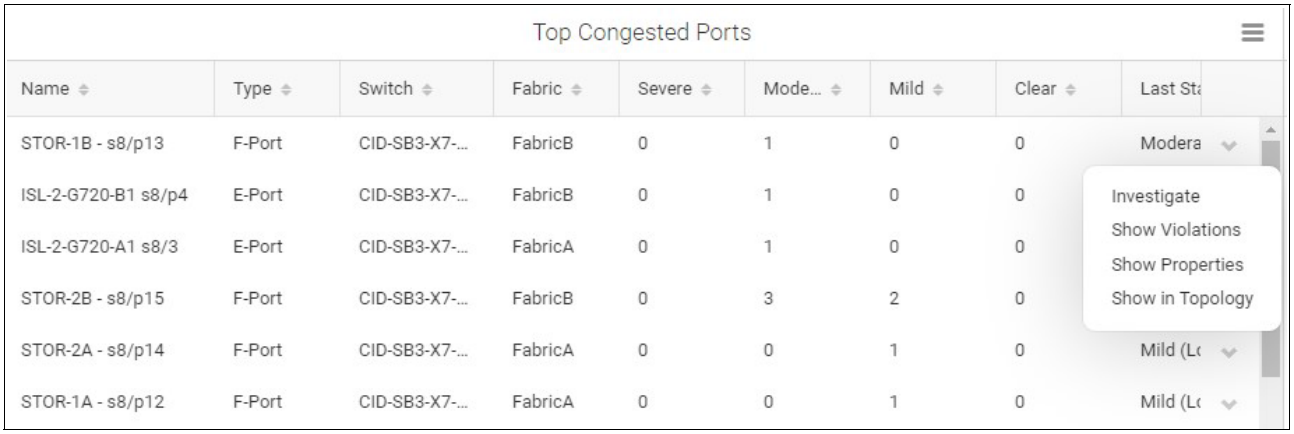


Figure 5-70 Top congested ports: Investigation Mode

5.7.9 Quarantined ports

Quarantined ports are ports that are quarantined by the MAPS Slow-Drain Device Quarantine (SDDQ) feature. The date range does not apply to the Quarantined Ports widget.

Click the action menu in the rightmost column to launch Investigation Mode and show the port properties.

5.7.10 Analyzing congested ports

In SANnav Management Portal, if the Network Port Traffic Conditions dashboard indicates congested or oversubscribed ports, you can use Troubleshooting Mode and Investigation Mode to get more details about these ports.

5.7.11 Troubleshooting Mode

The Troubleshooting Mode window is an expanded view of the Network Port Traffic Conditions dashboard. To show the Troubleshooting Mode window, click the hamburger icon that is at the upper right of the charts in the Network Port Traffic Conditions dashboard, and select **Troubleshoot**.

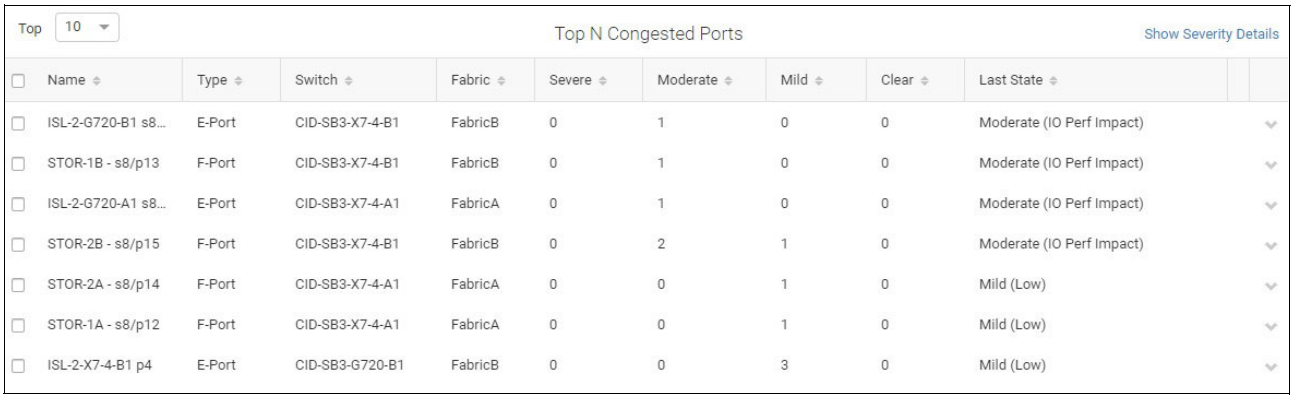
The network scope and date range indicators at the upper right of the window show the values that were specified in the Network Port Traffic Conditions dashboard when Troubleshooting Mode was entered.

Click the top drop-down menu above the table to select more ports to show.

For congested ports, the Severe, Moderate, and Mild columns show the number of ports that exhibit severe, moderate, and mild severity congestion states. These states are based on the MAPS congestion severity states. For more information, see Table 5-2 on page 172.

Click **Show Severity Details** to show the MAPS congestion severity states in the table. (This option is not available for oversubscribed ports.) In this view of the table, a value for Frame Loss or I/O Perf Impact that is greater than zero for a port can indicate a credit-stalled device.

A credit-stalled device is a misbehaving device that stops returning R_RDY signals (buffer credits) promptly to the switch, which causes the switch to stop sending frames to the device. Credit-stalled devices can be identified by credit latency or frame loss at a port. In the case of frame loss, the credit stall is long enough to cause queue latencies greater than 220 ms to 500 ms, as shown in Figure 5-71.


Top 10

Top N Congested Ports

Show Severity Details

Name	Type	Switch	Fabric	Severe	Moderate	Mild	Clear	Last State
ISL-2-G720-B1 s8...	E-Port	CID-SB3-X7-4-B1	FabricB	0	1	0	0	Moderate (IO Perf Impact)
STOR-1B - s8/p13	F-Port	CID-SB3-X7-4-B1	FabricB	0	1	0	0	Moderate (IO Perf Impact)
ISL-2-G720-A1 s8...	E-Port	CID-SB3-X7-4-A1	FabricA	0	1	0	0	Moderate (IO Perf Impact)
STOR-2B - s8/p15	F-Port	CID-SB3-X7-4-B1	FabricB	0	2	1	0	Moderate (IO Perf Impact)
STOR-2A - s8/p14	F-Port	CID-SB3-X7-4-A1	FabricA	0	0	1	0	Mild (Low)
STOR-1A - s8/p12	F-Port	CID-SB3-X7-4-A1	FabricA	0	0	1	0	Mild (Low)
ISL-2-X7-4-B1 p4	E-Port	CID-SB3-G720-B1	FabricB	0	0	3	0	Mild (Low)

Figure 5-71 Troubleshooting Mode congested ports

For oversubscribed ports, the `Latency` column indicates the average time that a frame is in the port transmit queue before being transmitted. Increasing latency at an ISL or ICL port is an indication of downstream congestion that is caused by oversubscription or a credit-stalled device.

5.7.12 Investigation Mode

To perform more investigation, click the down arrow at the end of a port row, and then select **Investigate** to show the Investigation Mode window for the port (Figure 5-72 on page 171). On this window, the congestion measures that are causing problems are preselected. You can show detailed congestion metrics in configurable time ranges of up to 2 hours with 1-minute granularity.

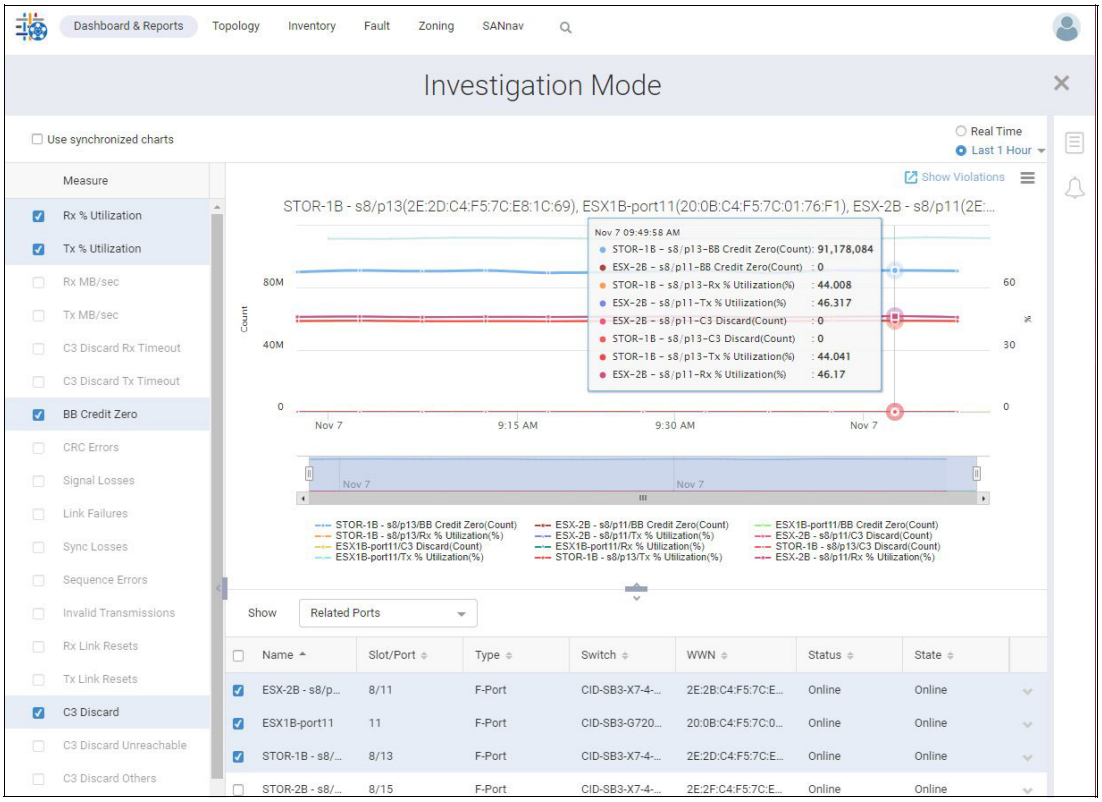


Figure 5-72 Investigation Mode

Table 5-1 shows the congestion measures in Investigation Mode.

Table 5-1 Congestion measures in Investigation Mode

Measure	Description
Rx % Utilization	The average percentage of link capacity that is used when receiving traffic. High-bandwidth utilization can indicate a source of oversubscription that can lead to congestion.
Tx % Utilization	The average percentage of link capacity that is used when transmitting traffic. High-bandwidth utilization can indicate a source of oversubscription that can lead to congestion.
IBM C3® Discard Rx Timeout	The number of Class 3 (C3) frame receive timeouts. Class 3 receive timeout errors (C3RXTO) on a port trigger a Frame Loss state for the port. Receive timeouts on an F_Port indicate that frames that are received on the port are being discarded because of back pressure from upstream ports (ISLs or other devices).
C3 Discard Tx Timeout	The number of C3 frame transmit timeouts. C3 transmit timeouts on an F_Port indicate that the F_Port is the source of congestion and causing back pressure. FPI, a MAPS feature, uses instances of C3 frame timeouts and instances of when transmit buffer-to-buffer credits are at zero to detect credit latency and F_Ports that are connected to credit-stalled devices. C3RXTOs on a port trigger a Frame Loss state for the port.
BB Credit Zero	The number of times BB Credit was at zero for the port. Incrementing counts of BB Credit Zero indicate credit latency. BB Credit Zero counts are incremented when the transmit credit value is at zero for a specific period and there is a frame waiting in the queue of the port or virtual channel for transmission. The frame cannot be transmitted when the credit value is at zero. Credit latency at a device port is an indication of a credit-stalled device. Credit latency at an ISL port is an indication of downstream congestion that is caused by oversubscription or a credit-stalled device.

In SANnav Management Portal, the line graphs in the Network Port Traffic Conditions dashboard and Troubleshooting Mode window show the number of ports that exhibit severe, moderate, and mild severity congested states during selectable time intervals. These states are based on the congestion states and metrics that are used by FPI, a Brocade MAPS feature to monitor congestion.

Table 5-2 compares the severity states that are identified in the dashboard with congestion states and metrics that are used to determine these states for the MAPS congestion dashboard and MAPS alerts.

Table 5-2 Congestion severity states

Congestion severity states in dashboard	MAPS congestion severity states	Metrics used to determine MAPS severity states
Severe	Frame Loss	This state is the highest congestion severity state. In this state, MAPS FPI generates a frame loss alert for the port. A Frame Loss state indicates a severe level of latency, which means frame timeouts either occurred or are likely to occur.
Moderate	I/O Perf Impact	This state is the second highest congestion severity state. In this state, MAPS FPI generates a performance impact alert for the port. This state can occur if the port does not have credit for a substantial period or if frames are transmitted with delay. A port or device in this state can negatively impact overall network performance.
Mild	Medium	A port is in a medium congestion severity state if any or both of the following conditions are met: ► Transmit Queue Latency (TQL) is 5 or more milliseconds but less than 10 milliseconds. ► Credit zero statistics indicate a latency of 100 or more milliseconds, but less than 700 milliseconds in 1 second.
	Low	A port is in a low congestion severity state if any or both of the following conditions are met: ► If the TQL is 3 or more milliseconds but less than 5 milliseconds. ► If the credit zero statistics indicate a latency of 50 or more milliseconds, but less than 100 milliseconds in 1 second.
	Info	A port is in an informative congestion severity state if any or both of the following conditions are met: ► If the TQL is 1 or more milliseconds but less than 3 milliseconds. ► If the credit zero statistics indicate a latency of 10 or more milliseconds but less than 50 milliseconds in 1 second.

For more information about how MAPS congested states are determined for a port, see the *Brocade Fabric OS MAPS User Guide, 9.1.x*.

5.7.13 Extension dashboard

To launch and use the Extension dashboard, complete the following steps:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Dashboard View** in the subnavigation bar.
2. Click **Select Dashboard** in the upper right of the window, select **Extension Dashboard**, and click **OK**, as shown in Figure 5-73 on page 173.

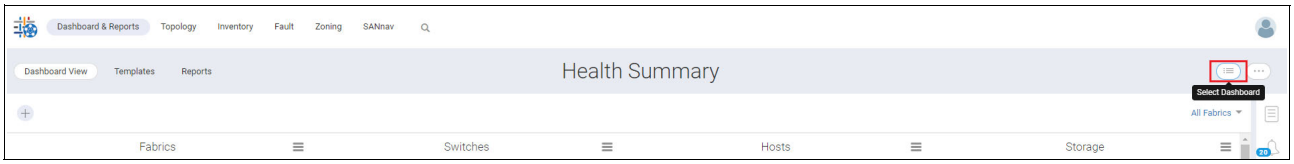


Figure 5-73 Selecting the Extension dashboard

The Extension dashboard opens, as shown in Figure 5-74. The dashboard consists of six widgets: two showing extension tunnel data, and four showing circuit data.

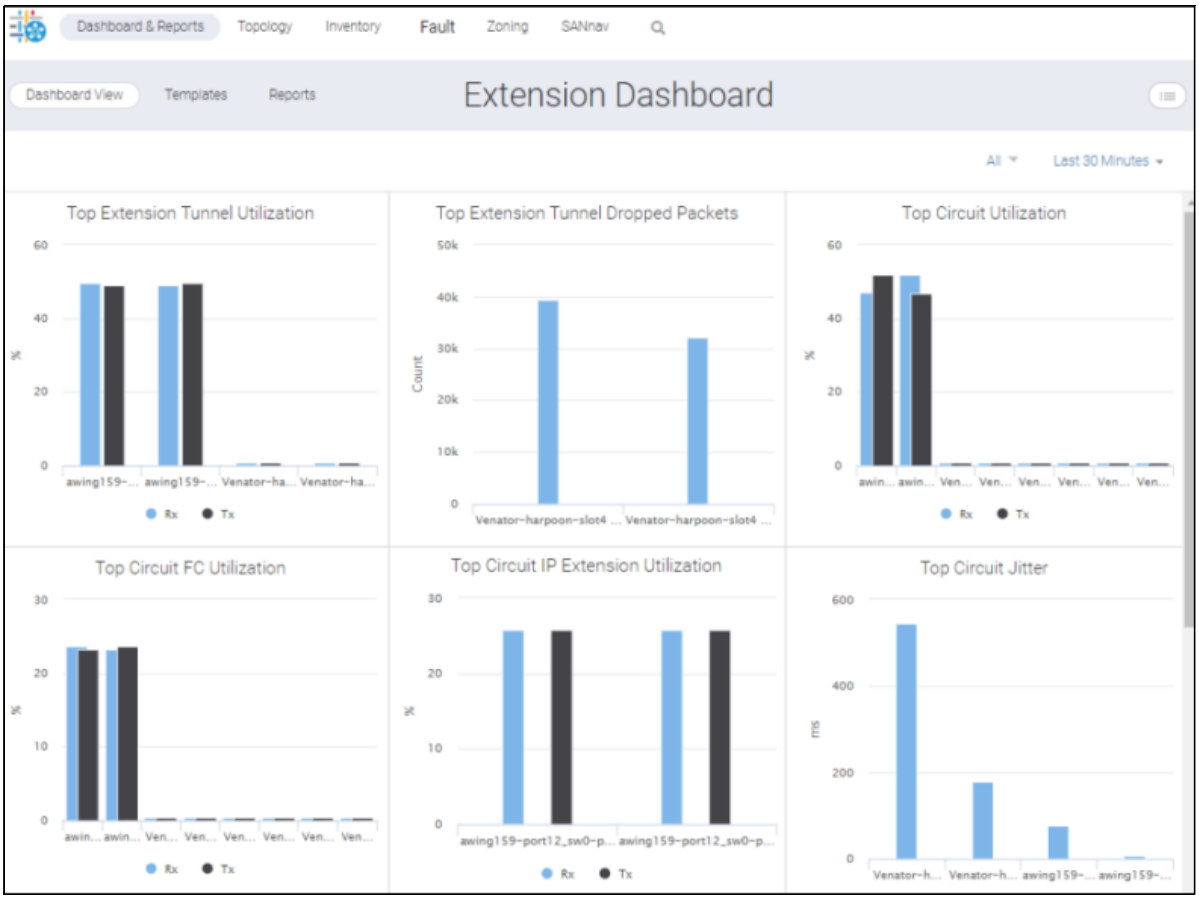


Figure 5-74 Extension dashboard

3. If you want to examine tunnel or circuit utilization, click a bar in one of the utilization widgets, and then select **Investigate** from the list, as shown in Figure 5-75.

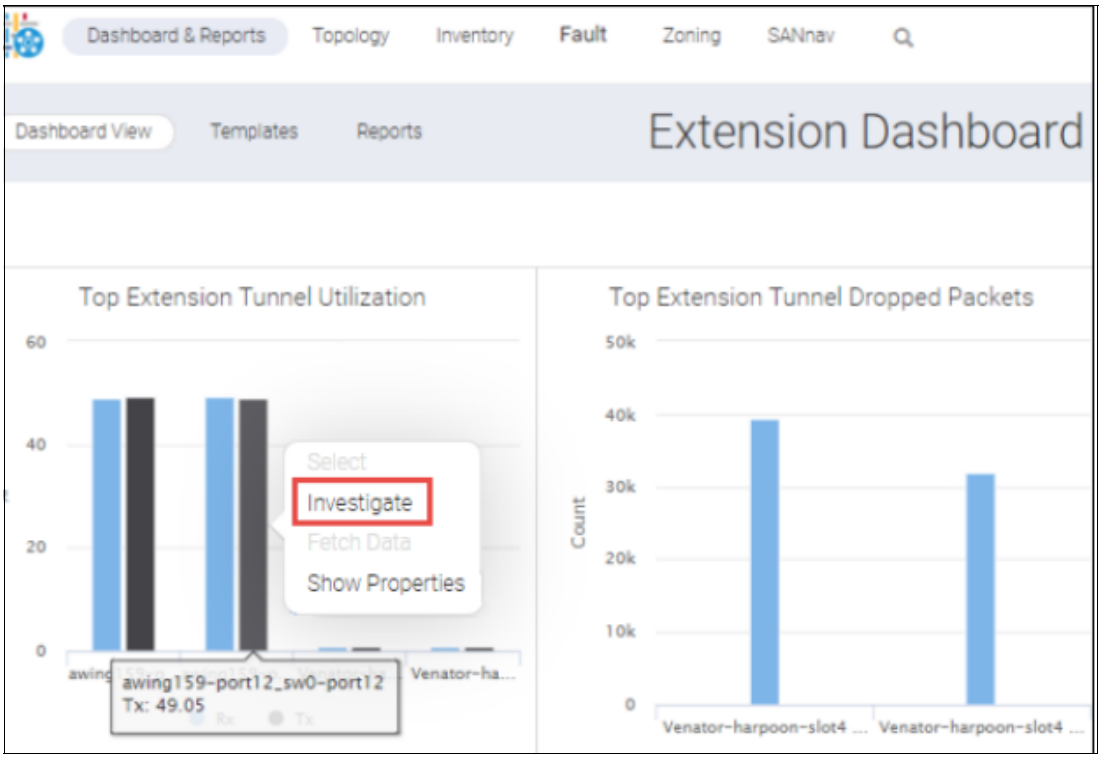


Figure 5-75 Extension dashboard: Investigate

4. Using Investigation Mode, you can see trends over time. Figure 5-76 on page 175 shows the Investigation Mode dialog box for a tunnel. Click the **X** in the upper right of the window to return to the dashboard view, as shown in Figure 5-76 on page 175.

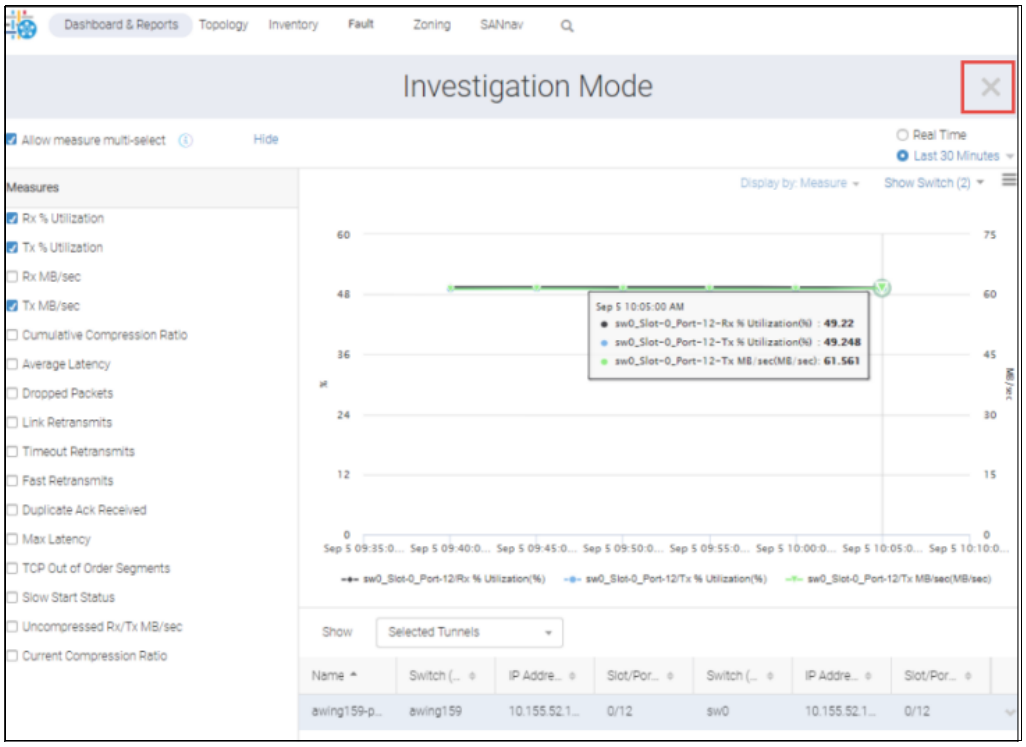


Figure 5-76 Investigation Mode dialog box for a tunnel

5. If you want to show the properties of a tunnel or circuit, click a bar in one of the graphs, and then select **Show Properties** from the list.

   A list appears with details about the tunnel or circuit. Figure 5-77 shows the properties of a tunnel.

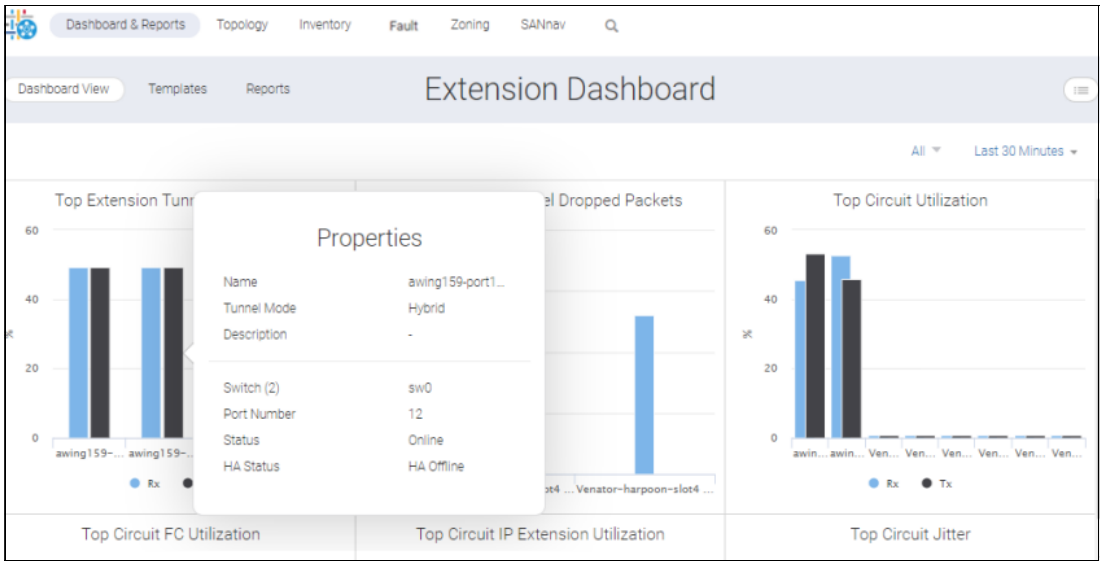


Figure 5-77 Extension Dashboard: Show Properties

6. To change the network scope and time range, click the drop-down lists in the upper right of the dashboard window. The extension widgets show data for the tunnels and circuits that belong to the fabrics in the selected network scope and for the selected time range.

5.7.14 Topology visualization

Using SANnav Management Portal, you can easily view and navigate a visual representation of the elements in your SAN topology based on a selected context. This visual representation enables you to focus on the information in the topology view instead of a complex network of devices and connections.

The Topology window shows graphical representations of the fabrics. For example, after you discover a fabric, you might want to view the topology to see a pictorial representation of the connected switches and devices.

You can show a topology for the following contexts:

- Fabric context: Shows all switches in the fabric and in other directly connected fabrics.
- Switch context: Shows all fabrics, switches, and devices that are directly connected to the selected switch.
- Switch port context: Shows all entities that are connected to the selected switch port.
- Host or storage context: Shows the connectivity to edge switches, fabrics, and other devices that are zoned with the selected device.
- Host port or storage port context: Shows edge switches, fabrics, and other device ports that are zoned with the selected device port.
- Zone context: Shows all zone members, including involved fabrics.

Note: If an icon on the topology window is “grayed-out”, it means that the associated object is disabled.

The topology shows information that is related to discovered fabrics only. For this reason, for FC Routing, you should discover all fabrics (backbone and edge fabrics) in the same instance of SANnav Management Portal.

Topology views are a snapshot in time, and they are not automatically updated. You can update the topology view by clicking the refresh icon in the upper right of the window. Also, if you navigate away from the Topology window, when you return to the window, the view is updated with the latest data, as shown in Figure 5-78.

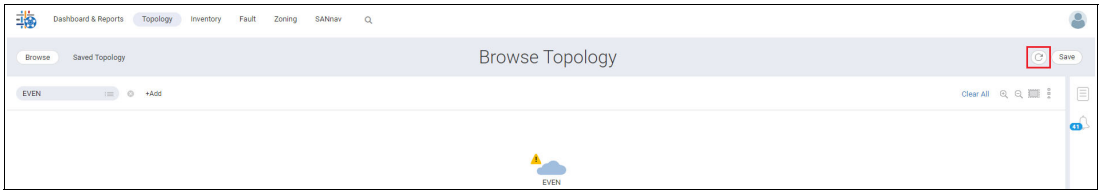


Figure 5-78 Refresh icon on the Topology window

You can save a topology view for easy access in the future. Saving a topology saves only the current context and does not save the navigated contexts. Saved topologies cannot be shared with other users.

Understanding topology icons

Click the **Legend View** icon in the upper right of the Topology window to show explanations of the graphics that are used in the topology, as shown in Figure 5-79.

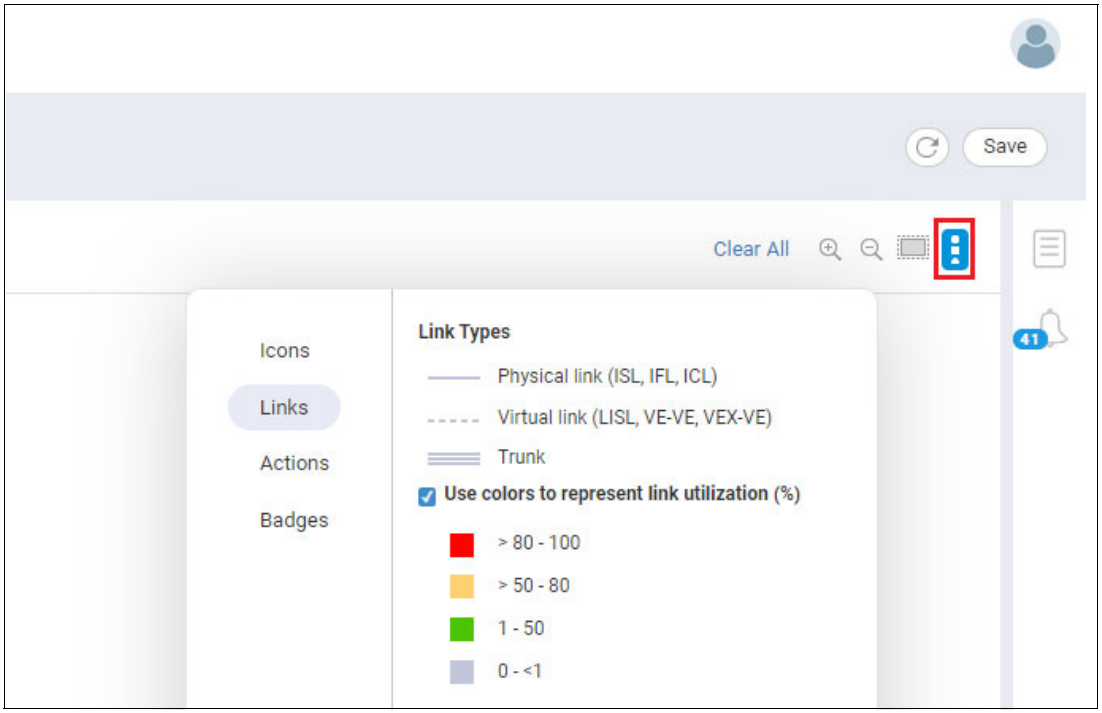


Figure 5-79 Topology legend view

In the legend dialog box, click the links on the left to show icons, links, actions, and badges. For links, you can turn off link utilization colors for your current session.

Adjusting the appearance of the topology view

If necessary, you can adjust the appearance of the topology by completing the following steps:

1. Click any of the icons and drag it to a new location.
2. Click the background and drag the entire topology to reposition it in the window.
3. Use the scroll button on the mouse or the zoom buttons in the upper right of the window to resize the topology view.
4. Click **Reset View** in the upper right to recenter and resize the topology to fit in the view, as shown in Figure 5-80.

Figure 5-80 Reset View

5. Click **Clear All** to remove all contexts and start over.

Viewing direct connectivity between objects

Click an icon in the topology to highlight the devices that are directly connected to it.

For example, Figure 5-81 shows a fabric. Clicking a device in the fabric, in this case, a host highlights all devices that are directly connected to that host and disables the other devices. Clicking the same device again or clicking anywhere in the canvas restores the original view.

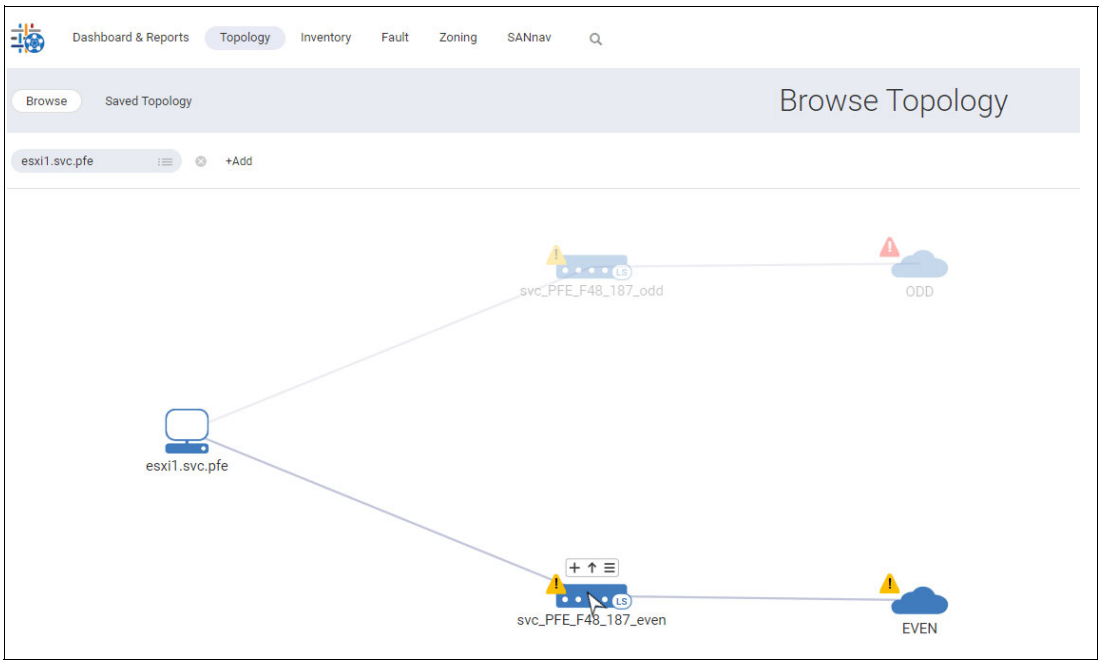


Figure 5-81 Direct connectivity

5.7.15 Viewing the fabric topology

After you discover a fabric in SANnav Management Portal, you might want to view a pictorial representation of the fabric, including the switches, ports, and connected devices.

You can launch a topology view in several ways, including from the action menu on the Inventory window and from the Health Summary dashboard.

To launch the topology view from the Topology window by adding a context, complete the following steps:

1. Click **Topology** in the navigation bar, and then click **+** to add a context (Figure 5-82).

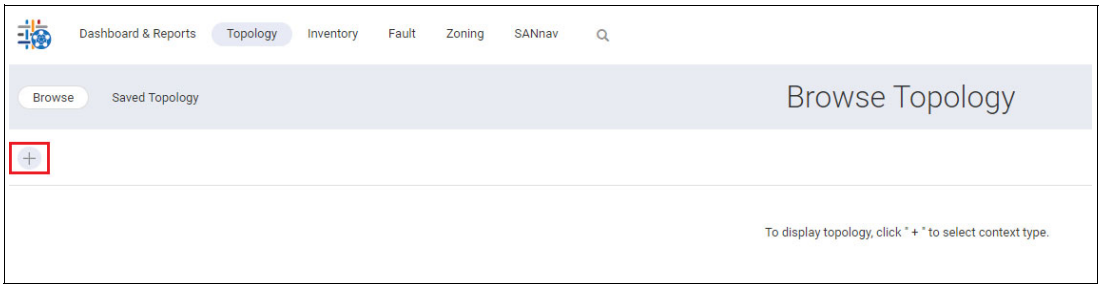


Figure 5-82 Viewing a topology

2. In the Add Context Type dialog box, select the **Fabric** context, and then click **OK**.

3. In the Fabric context field, click the menu icon to select a fabric, or type the fabric name directly into the context field. SANnav provides suggestions as you type (Figure 5-83).

Figure 5-83 Viewing the fabric topology

The Browse Topology window shows a pictorial view of the fabric. This view is the fabric context, so the topology shows all switches in the fabric. Note the fabric name that is shown in the context navigation pane at the top of the window. This fabric has four switches (Figure 5-84).

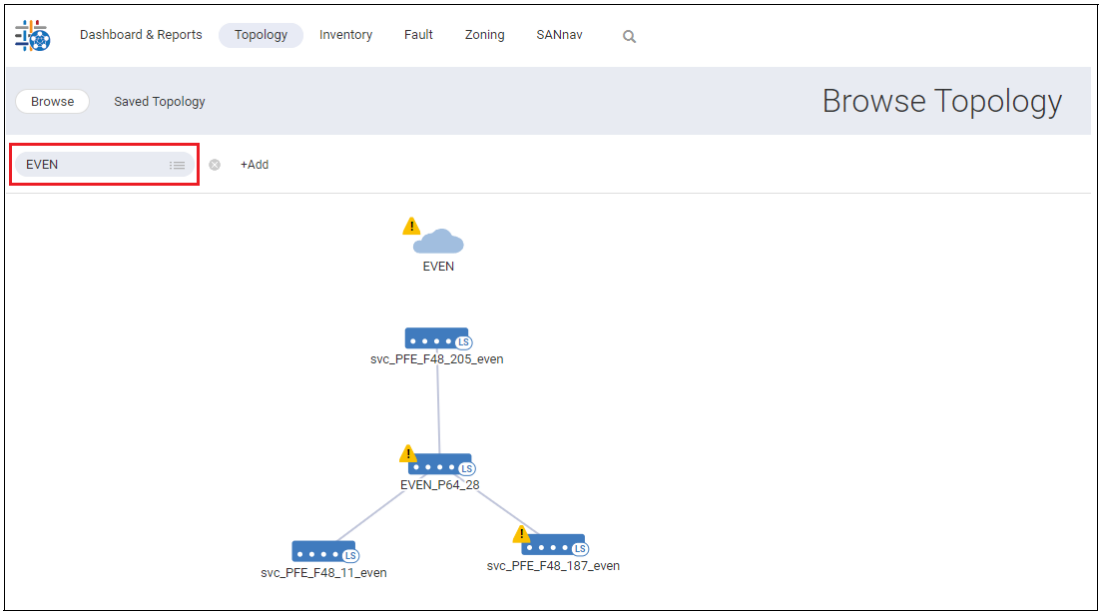


Figure 5-84 EVEN fabric

4. Hover your cursor over each switch and click **+** to show the online ports (Figure 5-85).

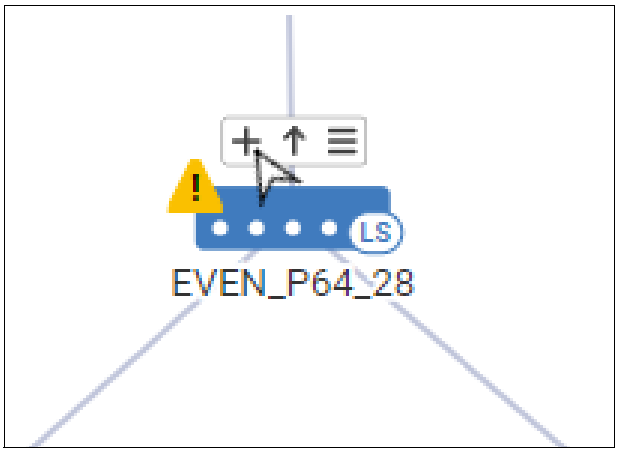


Figure 5-85 Showing the online ports

The topology now shows the online ports and the connections between them. (Virtual ports are not shown.) Notice that some switches are connected with trunk links (ISL, IFL, or F_Port trunks) (Figure 5-86).

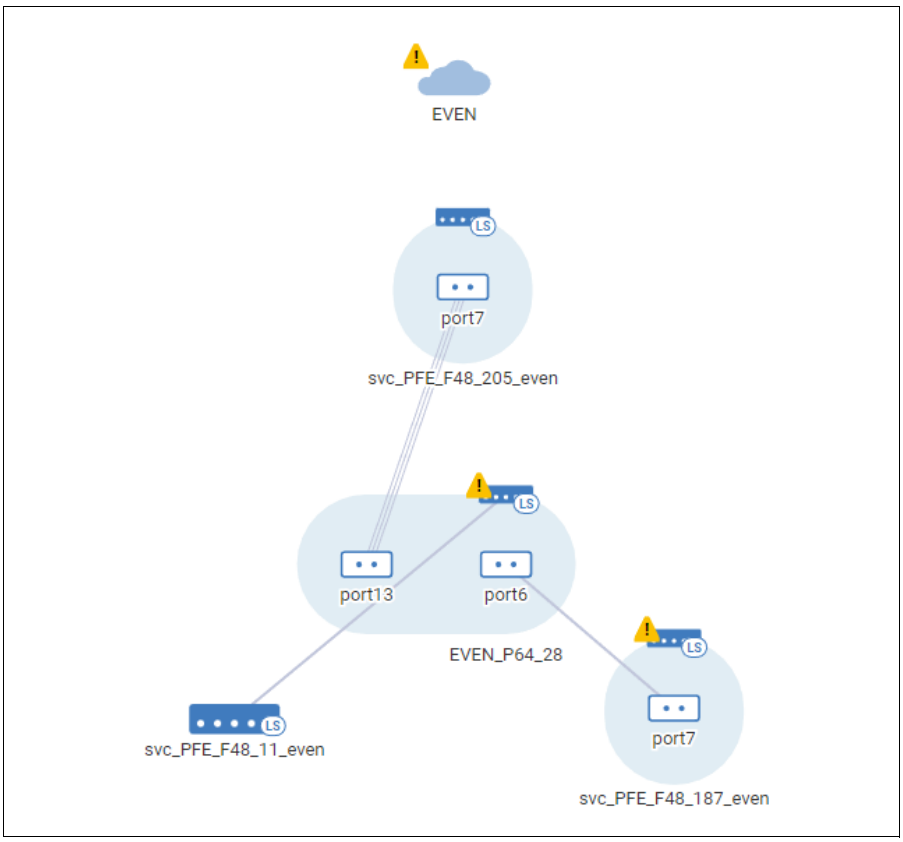


Figure 5-86 Fabric online ports

Note: If the number of ports that are connected to a switch is greater than 15, SANnav shows the ports in a tabular view.

Hover your cursor over a port icon, click the hamburger icon, and select any of the menu options. For example, if you select **Show Trunk Links**, a window opens and shows the trunk links in a tabular format. Selecting **Investigate** opens Investigate Mode for the port or trunk (Figure 5-87).

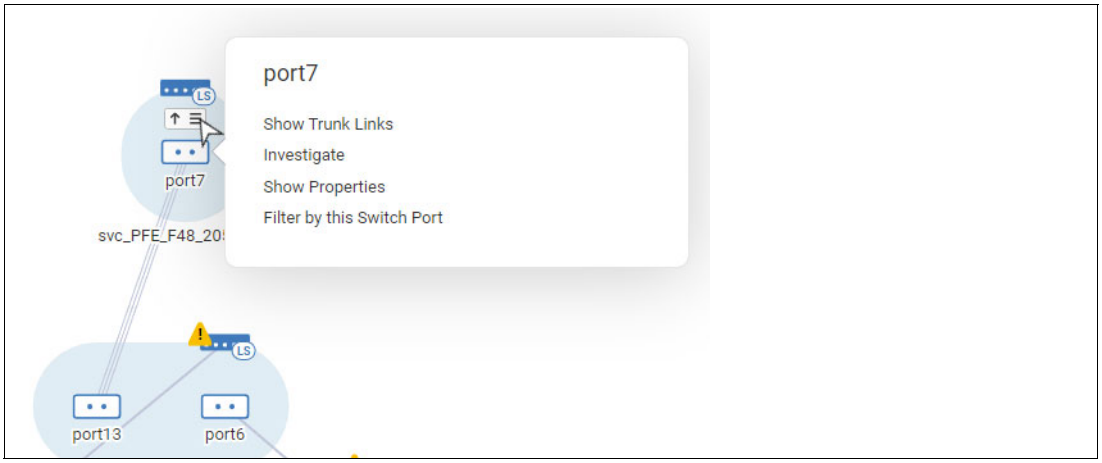


Figure 5-87 Investigate Mode

5. Hover your cursor over the fabric icon or a switch icon, click the hamburger icon, and select any of the menu options (Figure 5-88).

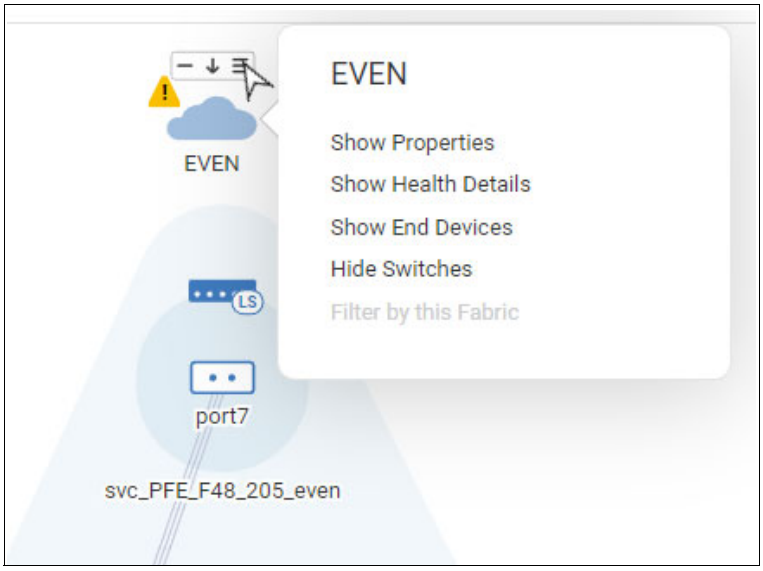


Figure 5-88 Hover your cursor over the fabric icon

6. Hover your cursor over one of the switches and click the up arrow to change to the switch context.

   Clicking the up arrow adds a context to the context navigation pane, which is “up” or at the top of the topology window.

Now, the topology is in the switch context and shows all switches and devices that are directly connected to the selected switch. Notice that the context navigation pane now contains two contexts (Figure 5-89).

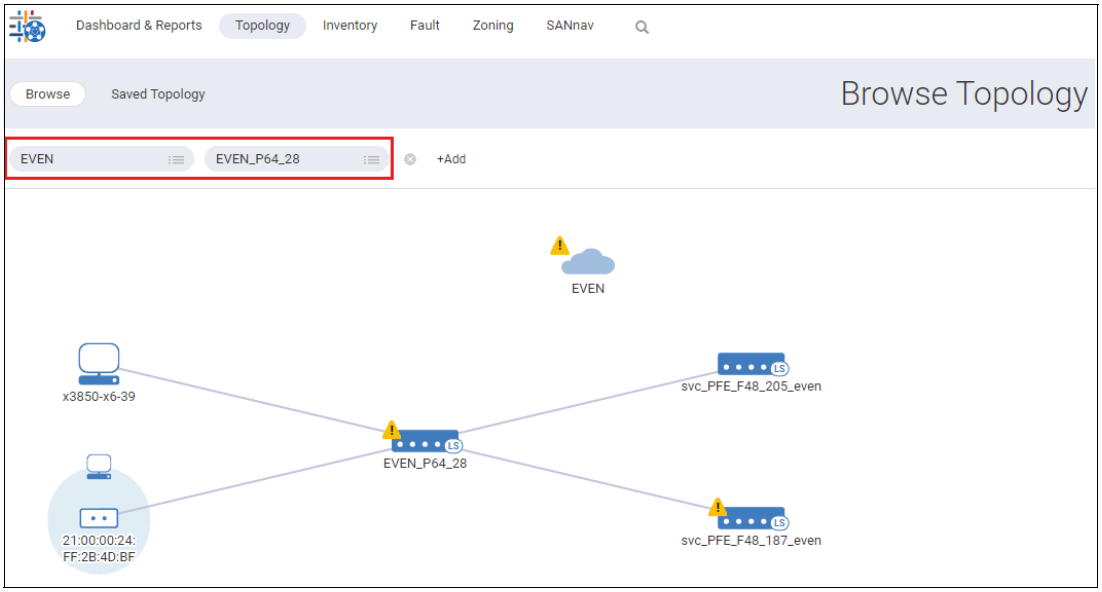


Figure 5-89 Context navigation pane

You can keep adding contexts by hovering your cursor over an object and clicking the up arrow or by clicking **+Add** in the context navigation pane to add a context type that is relevant to the current contexts.

Note: If the browser is refreshed, only the latest chosen context is showed, and the other contexts are deleted.

To go back to the previous context, click the **X** in the context navigation pane, or hover your cursor over the selected object and click the down arrow.

7. Click **Save** in the upper right of the window if you want to save the topology. You can access the saved topology later from the **Saved Topology** tab.

5.7.16 Showing all devices in a fabric

The SANnav Management Portal Topology feature allows you to quickly see a graphical representation of all end devices that are attached to your fabric. To do so, complete the following steps:

1. Click **Topology** in the navigation bar.
2. Click **+**, select **Fabric** for the context type, and click **OK**.
3. Click the **Menu** icon to select a fabric or type the fabric name directly into the context field (Figure 5-90 on page 183).

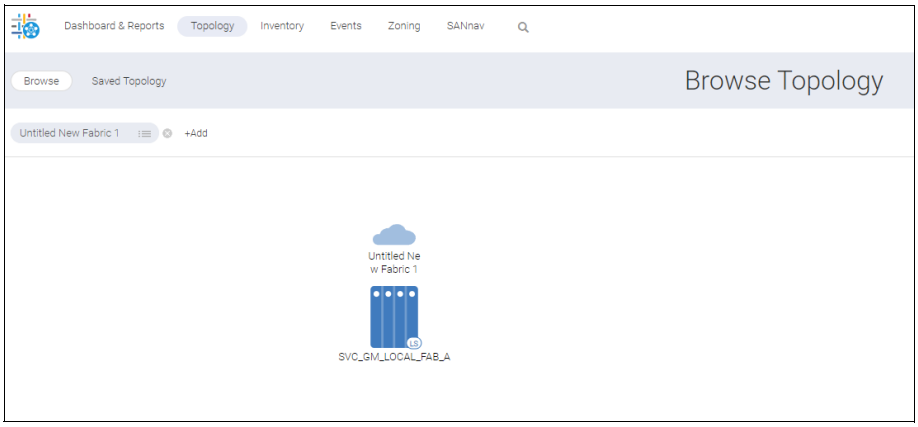


Figure 5-90 Untitled fabric 1 topology

4. Hover your cursor over the fabric icon, click the hamburger icon, and select **Show End Devices (**Figure 5-91).

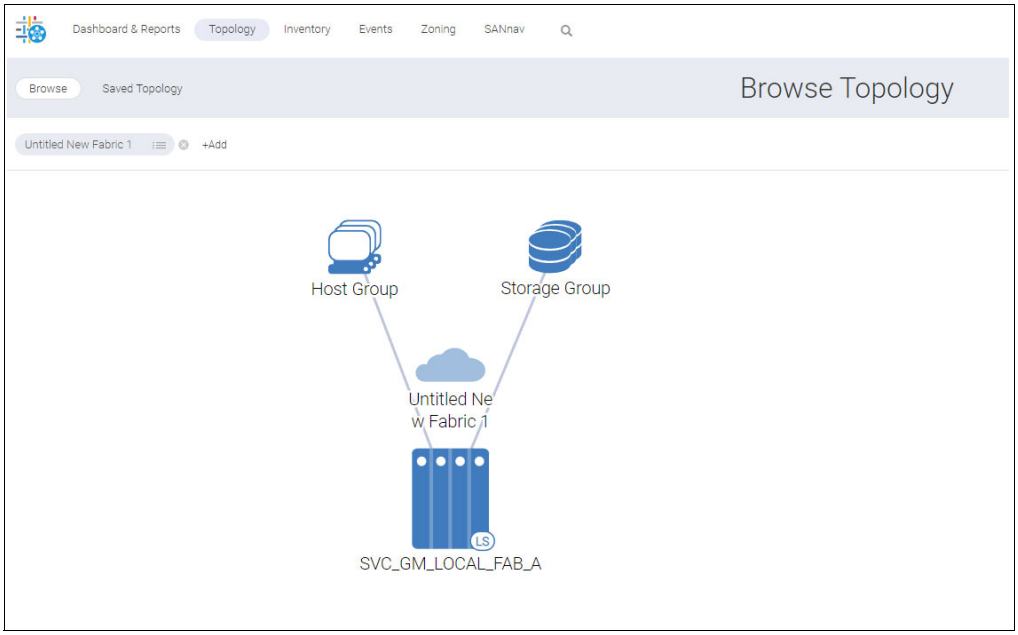


Figure 5-91 All end devices topology

If a switch has more than five connected end devices of the same type, the devices are shown in the topology as a group.

5. To show the objects in a host or storage group individually in the topology, complete the following steps:

   a. Hover your cursor over the group icon, click the hamburger icon, and then select **Show Storage** (or **Show Hosts**) (Figure 5-92).

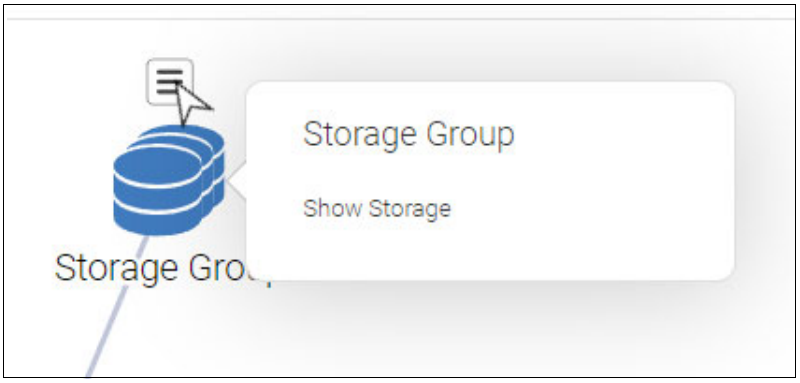


Figure 5-92 Show Storage

   A list of the devices in that group shows.

   b. Select the devices that you want to show individually in the topology and click **OK**. The selected items are removed from the host group and are shown individually in the topology (Figure 5-93).

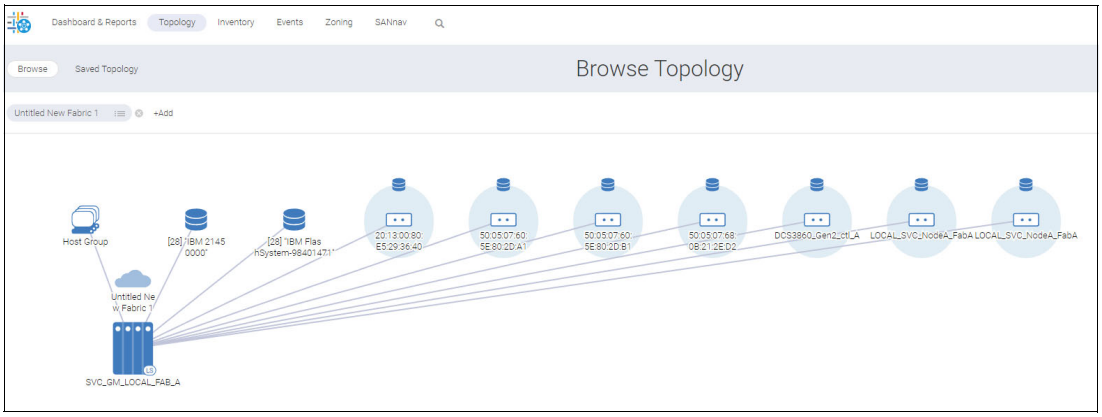


Figure 5-93 Showing individual storage

If the number of items remaining in the group is five or less, the group closes and all remaining items are shown individually in the topology.

For Fibre Channel over Ethernet (FCoE) devices that are connected through a link aggregation group (LAG), a virtual link type is shown. Link utilization colors are not shown for links connecting a LAG.

5.7.17 Viewing connectivity between hosts and storage

Using the SANnav Management Portal Topology feature, you can view hosts and storage and all paths between them.

To access the topology through the dashboard starting from a host, complete the following steps. You can also start from a storage device.

1. Go to the Health Summary dashboard, click the down arrow next to a host (or storage device) to open the action menu, and click **Show in Topology**.

   Although you can start from the Inventory window or the Topology window, this step shows how to start from the Health Summary dashboard and select the item that you want to view (Figure 5-94).

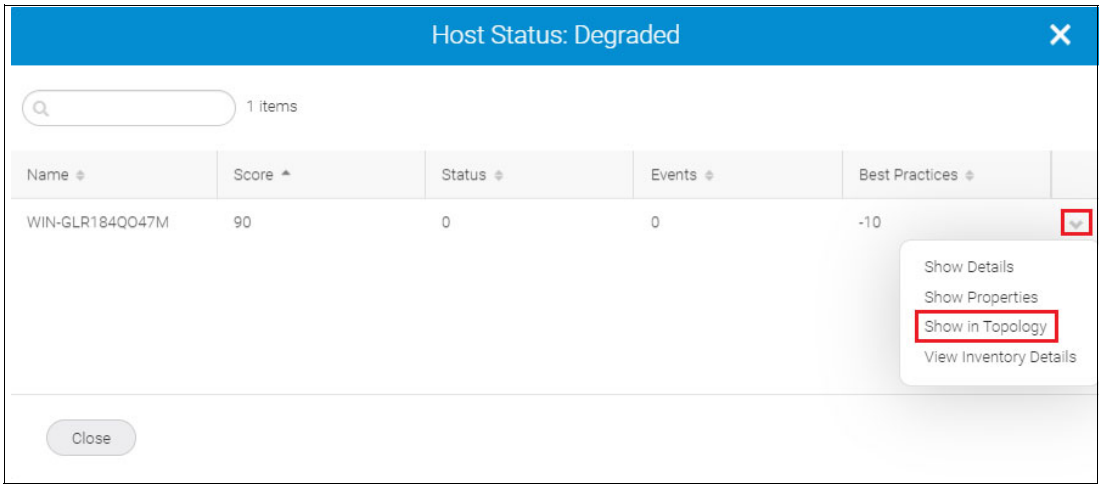


Figure 5-94 Show in Topology

2. The Browse Topology window shows a pictorial view of the fabric from the context of the chosen storage. The hostname is shown in the context navigation pane. You can see the host, along with all paths to the storage devices that the host connects to (Figure 5-95).

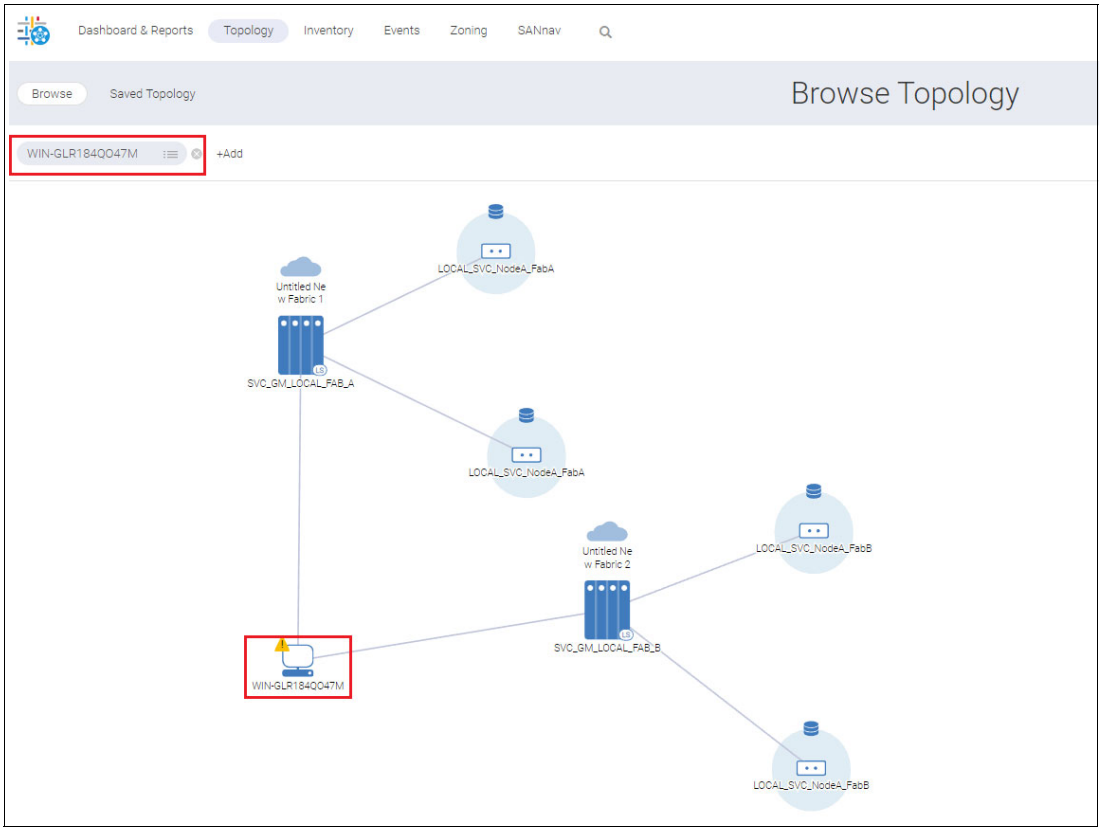


Figure 5-95 Showing the host in a topology

3. To see the host ports, hover your cursor over the host icon, and click **+** (Figure 5-96 on page 187).

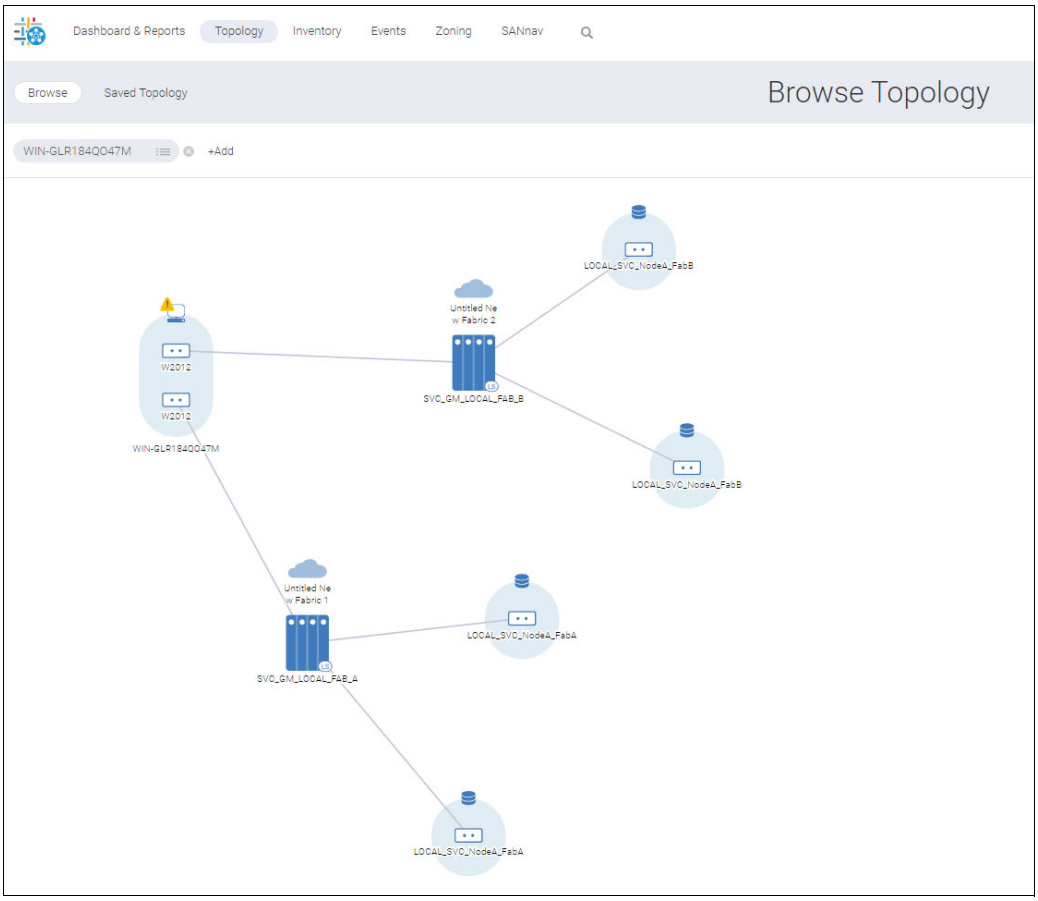


Figure 5-96 See host ports

Some of the icons might have yellow or red warning symbols, which indicate degraded or poor health. For more information about these warnings, hover your cursor over the icon, click the icon, and select **Show Health Details**.

Only the physical ports are showed. You can drill down even further and show the virtual (N_Port ID Virtualization (NPIV)) ports that are associated with the host or storage ports. Hover your cursor over a host or storage port icon, click the hamburger icon, and select **Show Virtual Ports** to show the associated virtual ports in a tabular format.

Note: If the host contains only NPIV ports, they are not shown in the host context. If those NPIV ports are zoned, they are shown in the storage context on the host side.

5.7.18 Viewing link utilization

The Topology window in SANnav Management Portal provides a visual indication of when a link is over 50% utilization and over 80% utilization, so you can easily see which links are busy.

When you view the topology, the link color indicates the percent utilization of the link:

- Green = 1% - 50% utilization
- Yellow = More than 50% - 80% utilization
- Red = More than 80% utilization
- Gray = Less than 1% utilization, or the link is not used or not monitored for utilization (default color)

The utilization of a port link is determined by the higher of the transmitted (Tx) and received (Rx) frames. For example, if the Tx utilization is 60% and the Rx utilization is 40%, the link color is yellow to reflect the higher utilization.

The utilization of a switch link is determined by the highest of all the port links. For example, if the switch link is red, at least one of the port links is red. Expand the switch to see the individual port links.

You can turn off the link colors by selecting an option in the Links section of the Legend View. If you turn off the link colors, all links (monitored and unmonitored) are showed as gray. The link color option persists only for the current user session.

Link utilization is not shown between a switch icon and a fabric icon. If you want to see that link utilization, you must expand the fabric (Figure 5-97).

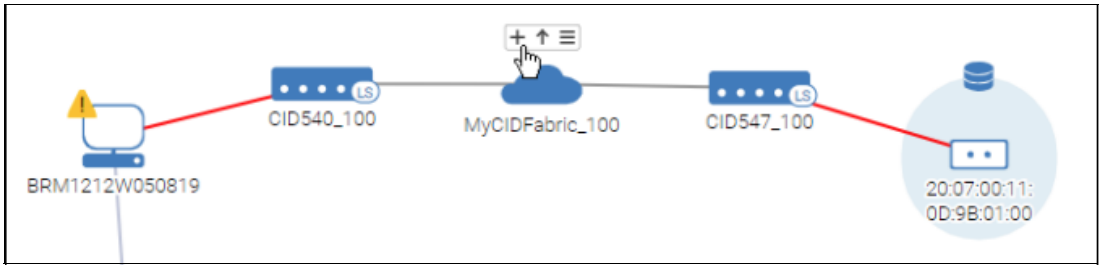


Figure 5-97 Link utilization

When the fabric is expanded, the link utilization color and details icon are available (Figure 5-98).

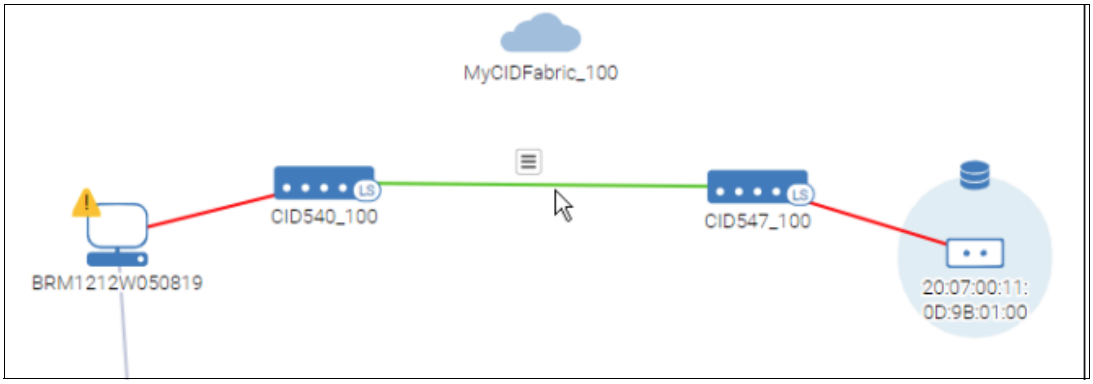


Figure 5-98 Expanding the fabric

To view links and link utilization, complete the following steps:

1. Click **Topology** in the navigation bar, and then click **+** to add a context.
2. In the Add Context Type dialog box, select a context, and click **OK**. For this example, select the **Fabric** context.

3. In the Fabric context field, click the **Menu** icon to select a fabric, or type the fabric name directly into the context field. The Browse Topology window (Figure 5-99) shows a pictorial view of the fabric. This fabric has two switches, and the link between them is red, which means the link utilization is over 80%.

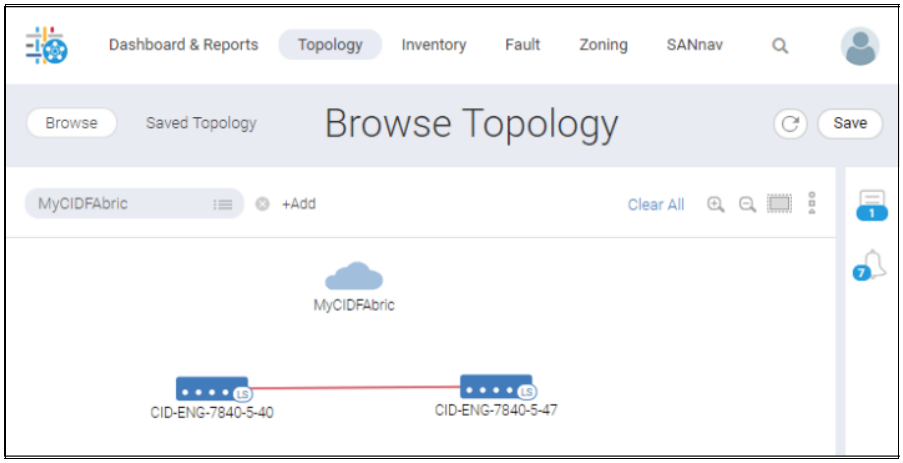


Figure 5-99 Browse Topology

4. Hover your cursor over the link, click the hamburger icon, and then select **Show Details** to show information about each of the ports in the link (Figure 5-100).

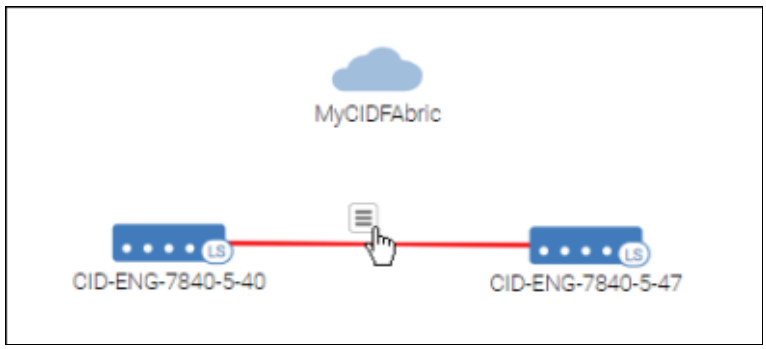


Figure 5-100 Selecting Show Details to show information about each of the ports in the link

Notice the Rx and Tx utilization. For two ports, the utilization is over 80% (Figure 5-101).

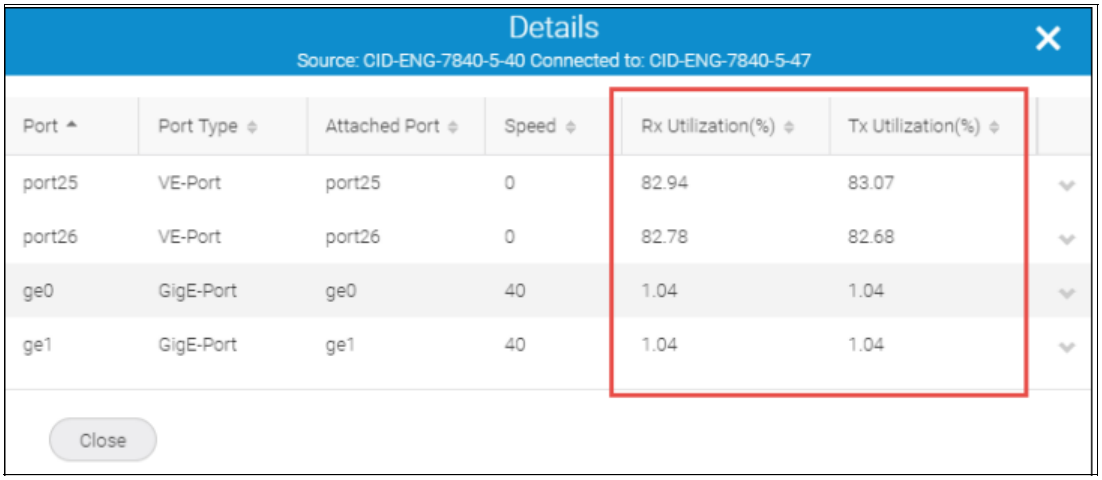


Figure 5-101 Rx and Tx utilization

5. Hover your cursor over a switch icon and click **+** to expand the switch and show the ports that make up the link.

   If the switch has more than 15 online ports, expanding the switch shows information in a tabular view.

   The switch in this example has three port links, two of which are over 80% utilization. Even though one of the links is at or below 50% utilization, the overall utilization state of the switch link is the same as the highest utilization of all the port links.

6. Hover your cursor over one of the port links, click the hamburger icon, and then select **Show Properties** to show information about that specific port link.

   The Show Properties option is not available for GigE group port links.

7. If the link is a trunk, hover your cursor over the port icon at one end of the link, click the hamburger icon, and then select **Show Trunk Links** to view details about the trunk (Figure 5-102).

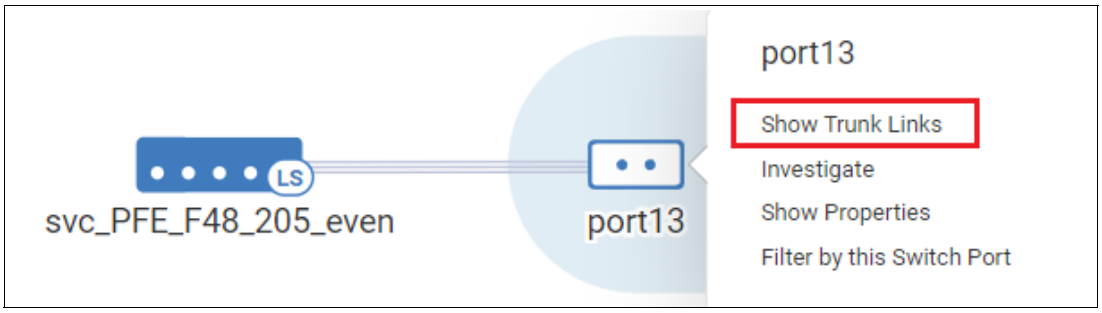


Figure 5-102 Show Trunk Links

If you find links with high utilization, you can open Investigate mode to look at the link usage pattern over time. Hover your cursor over the switch port, click the hamburger icon, and then select **Investigate** to open Investigate mode.

For links with consistently high utilization, you might consider adding more links, creating trunks, or configuring your network to provide alternative paths for the traffic.

5.7.19 Viewing a zone topology

In SANnav Management Portal, viewing a zone topology shows all ports that are members of the zone.

You can view the topology for zones in the active zone configuration only.

To view a zone topology starting from the Topology window, complete the following steps. You also can launch the Topology window from the effective zone configuration details window by selecting **Show in Topology** from the **Zone** action menu.

1. Click **Topology** in the navigation bar.
2. Click **+**, select **Zone** for the context type, and then click **OK**.
3. Click the **Menu** icon to select a fabric and then select one or more zones. Alternatively, you can type the zone name directly into the context field (Figure 5-103).

Figure 5-103 Zone topology

The Browse Topology window shows a pictorial view of the zone, showing connectivity between all zone members (Figure 5-104).

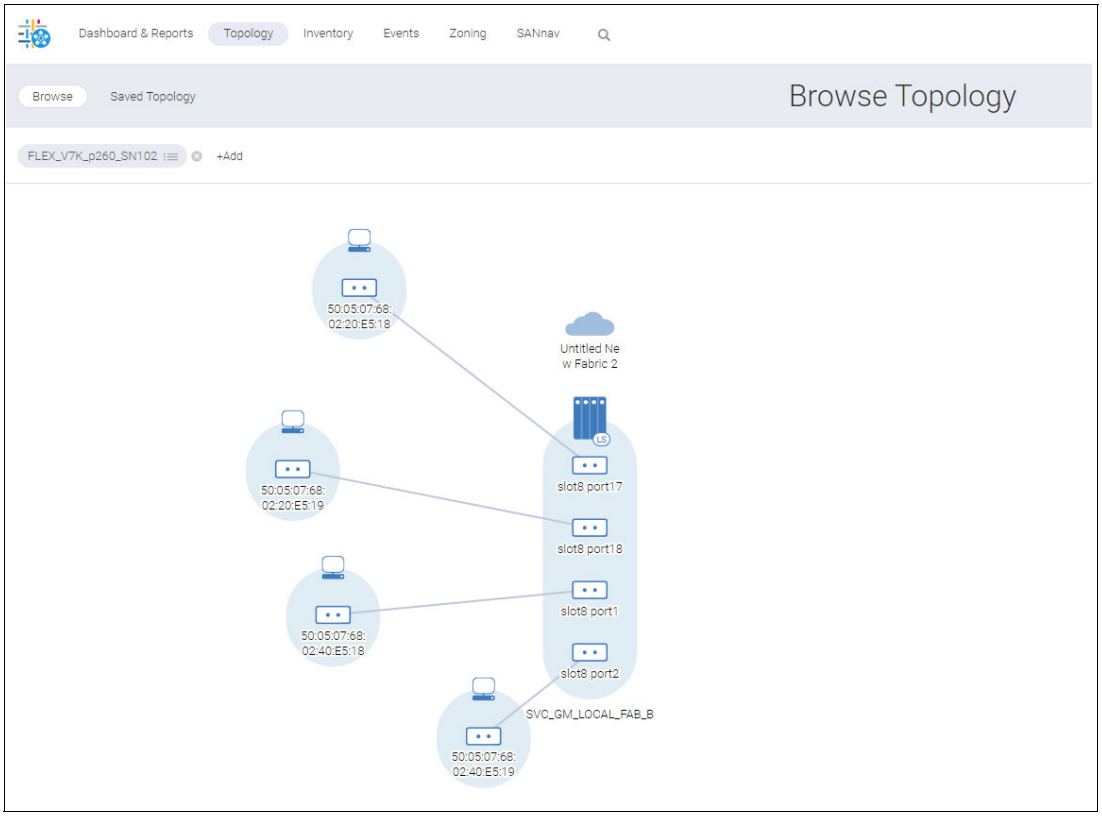


Figure 5-104 Flex zone

4. You can click the **Menu** icon to add zones or remove zones from the context. If more than one zone is selected, the context field shows the number of zones selected (Figure 5-105).

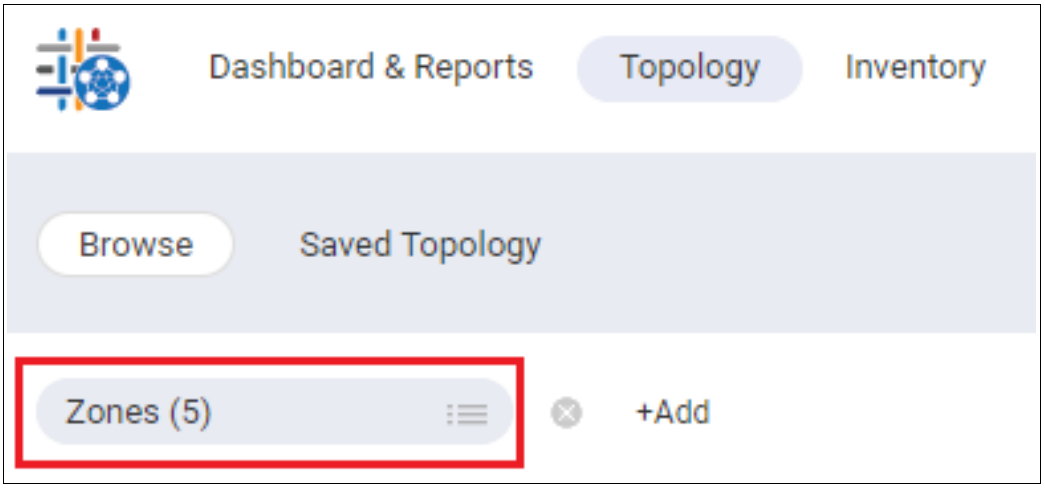


Figure 5-105 Multiple zones

5.7.20 Viewing saved topologies

You can view topologies that you previously saved in SANnav Management Portal.

You can view only the topologies that you created and saved. You cannot view topologies that were created by others. Saved topologies cannot be shared with other users.

When you view a saved topology, the latest content is showed, which is not necessarily the content at the time that the topology was saved. New entities are shown that might not have been present in the saved topology, and entities that no longer exist are not showed.

Note: If the saved topology context (fabric, switch, switch port, and so on) is unmonitored or removed from SANnav, attempting to view the saved topology results in an error message. If that entity is monitored or added back to SANnav, the error still occurs. In this case, you must delete the saved topology and save it again for this entity.

To view saved topologies, complete the following steps:

1. Click **Topology** in the navigation bar, and then click **Saved Topology**. A list of your saved topologies shows.
2. Locate the topology that you want to view and select **Show in Browse** from the action menu in the rightmost column (Figure 5-106).

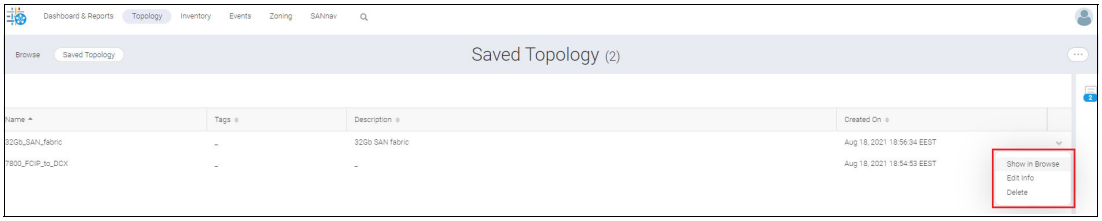


Figure 5-106 Saved topology

The topology shows in the Browse window.

You can perform the same operations on the saved topology as on a standard (unsaved) topology, such as showing ports, showing link properties, and adding contexts.

3. If you want to save your changes, click **Save**.

   Alternatively, if you want to leave without saving your changes, click **Clear All** (Figure 5-107).

Figure 5-107 Editing the topology

4. To rename a topology, select **Edit Info** from the action menu in the rightmost column on the Saved Topology window.
5. To delete a topology, select **Delete** from the action menu in the rightmost column on the Saved Topology window. You can also use bulk edit to delete multiple topologies concurrently.

5.7.21 MAPS violations

A violation is an alert that is sent by MAPS if the triggering condition persists every time that a rule is checked.

Here is the list of MAPS violations widgets:

- Initiator Port Health Violations
- ISL Port Health Violations
- Port Health Violations
- Target Port Health Violations
- Out of Range Violations

Note: The FICON Management Service violation is not supported by MAPS in SANnav.

Viewing MAPS violations

You can view MAPS violations in the Violations window. Violations are filtered based on severity, network scope, and date range. Available violation severities are All, Critical, Error, Warning, and Info.

To view the MAPS violations, complete the following steps:

1. Click **Fault** in the navigation bar, and then select the **Violations** tab. The Violations window opens.
2. Click the arrow next to a rule to view the violation details (Figure 5-108).

Figure 5-108 MAPS violation

For more information about violations, see 5.10, “Fault Management” on page 219.

Troubleshooting MAPS violations

You can troubleshoot the MAPS event violations by taking recommended actions. For more information about recommended actions, see 5.10.6, “Managing event policies ” on page 241.

5.8 Investigation Mode

SANnav Investigation Mode enables you to view performance measures for selected chassis, switch ports, extension tunnels, extension circuits, and trunks.

5.8.1 Launching Investigation Mode

You can launch Investigation Mode in several ways. To launch Investigation Mode, select the **Investigate** option from dashboard widgets, tables, or dialog boxes. You can investigate a single element or multiple elements (of the same type). This section describes how to select the elements that you want to investigate and launch Investigation Mode. Section 5.8.3, “Using Investigation Mode ” on page 199describes what happens after you click **Investigate**.

Invoking Investigation Mode from a dashboard widget

On the Dashboard View window, several widgets include the **Investigate** option. Figure 5-109 shows how you can investigate a switch port by clicking the graph in the Top Port BB Credit Zero widget. You can also select **Investigate All**, which investigates all ports that are shown in the widget.

Figure 5-109 shows how you can investigate a switch port by clicking the action menu in the Port Details window of the Port Distribution widget.

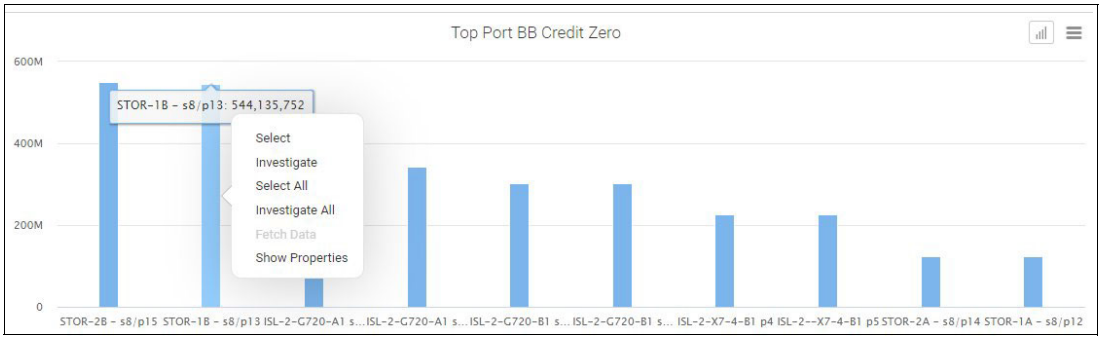


Figure 5-109 Launching Investigation Mode from a dashboard widget

Invoking Investigation Mode from an inventory list

From the Inventory window, click **Investigate** from the action menu for chassis and switch ports. Clicking **Investigate** from the action menu for hosts, host ports, storage, and storage ports launches Investigation Mode for the F_Port of the connected switch.

The bulk select option is available if you want to investigate multiple items (Figure 5-110).

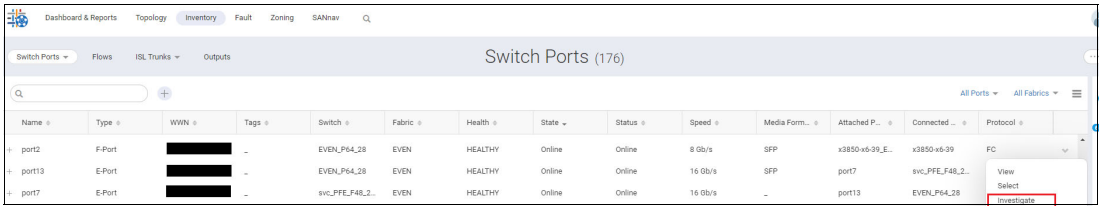


Figure 5-110 Launching Investigation Mode from the Inventory window

For switch ports, you can also launch Investigation Mode from the Switch Details window.

For trunks and extension tunnels, select one of the options from the **ISL Trunks** drop-down menu in the subnavigation bar. Then, select **Investigate** from the action menu for the selected trunk or tunnel (Figure 5-111).

Figure 5-111 Launching Investigation Mode for trunks or extension tunnels

To launch Investigation Mode for each of the ISL ports in a trunk, first select **Show Links** from the action menu for a selected trunk, and then click **Investigate** from the ISL Links dialog box (Figure 5-112).

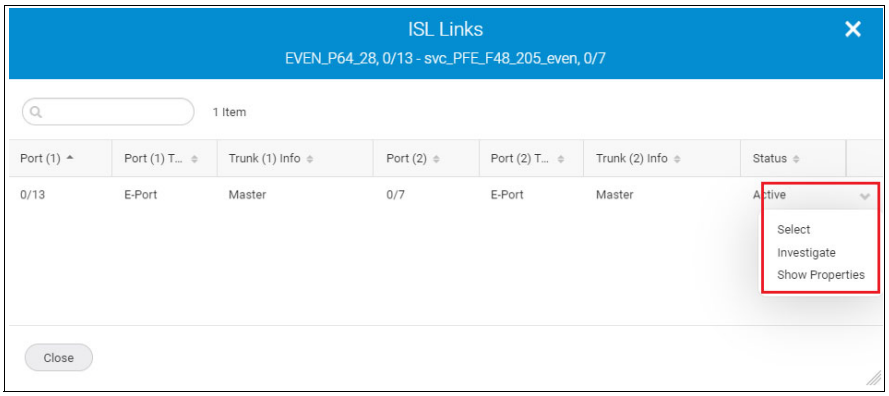


Figure 5-112 Launching Investigation Mode for link ports

After you launch Investigate Mode for a tunnel, you can launch Investigate Mode for the circuits that are associated with that tunnel by clicking **Investigate Circuits** from the details table (Figure 5-113).

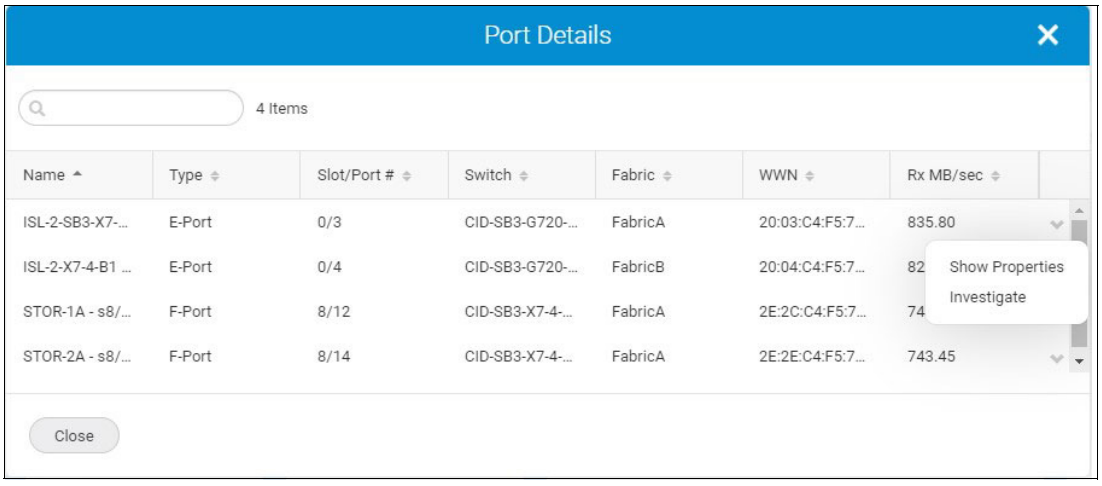


Figure 5-113 Launching Investigation Mode from a dashboard widget

Invoking Investigation Mode from the sidebar

From the Inventory windows, you can select items that you are interested in investigating and add them to the sidebar. The sidebar is a subset of the inventory items and contains only the items that you want to investigate. From the sidebar, you can select items to investigate and easily reinvestigate them later without having to locate them again from the Inventory windows.

Invoking Investigation Mode for high-granularity data

If a port or extension tunnel is scheduled for high-granularity data collection, you can launch Investigation Mode from the Outputs window in Inventory. Select **Port Data Collection** or **Tunnel Data Collection** and click **Investigate** from the action menu for the port or tunnel that you want to investigate.

5.8.2 Collecting items in the sidebar for Investigation Mode

For items that you frequently investigate, you can select them and put them in the SANnav sidebar. The sidebar allows you to easily reinvestigate items without having to locate and reselect them from the Inventory window.

To collect items in the sidebar for Investigation Mode, complete the following steps:

1. Click **Inventory** in the navigation bar.
2. Locate the type of items that you want to investigate.
3. Select **Chassis** or **Switch Ports** from the leftmost drop-down list in the subnavigation bar.
4. Select **ISL Trunks**, **IFL Trunks**, **F Port Trunks**, or **Extension Tunnels** from the next drop-down list. You cannot add circuits to the sidebar (Figure 5-114).

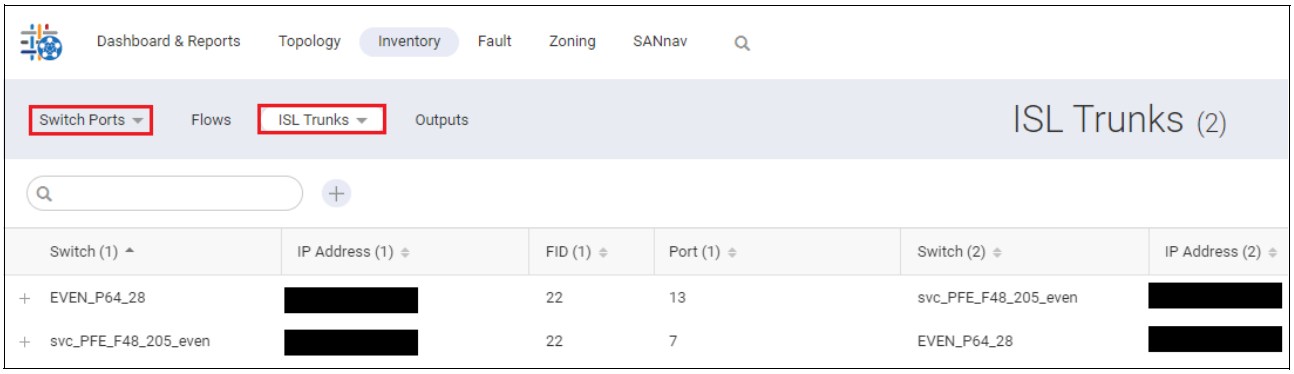


Figure 5-114 Collecting items in the sidebar for Investigation Mode

5. Click **+** at the left of every row for each item that you want to add to the sidebar. As you click the icons, the **+** changes to a **–** symbol, and the sidebar icon increments the count of selected items (Figure 5-115).

Figure 5-115 Collecting items in the sidebar

6. Click the sidebar icon to expand the sidebar.
7. In the sidebar, select the type of item that you want to investigate from the drop-down menu (Figure 5-116).

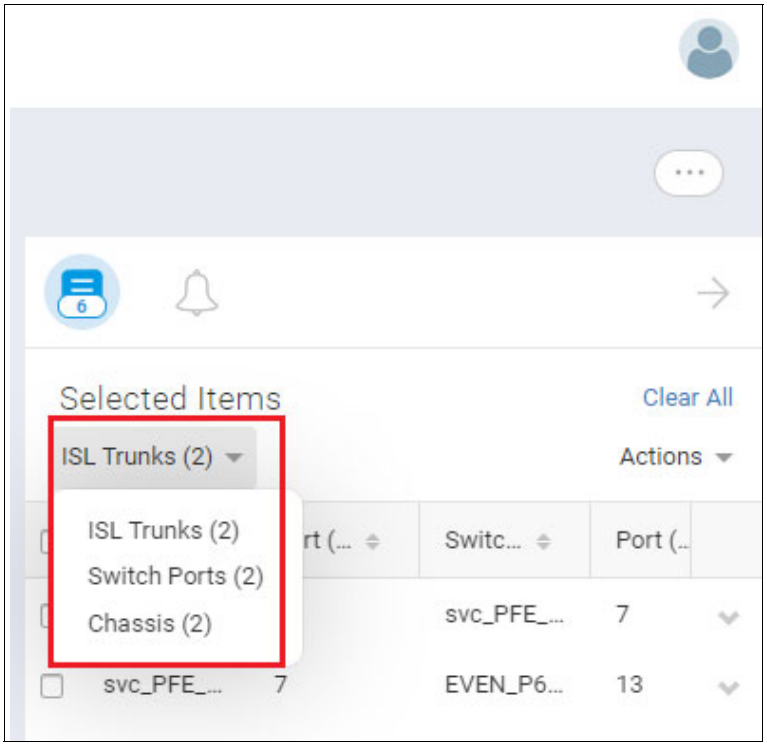


Figure 5-116 Selecting types from the sidebar

8. Select the items that you want to investigate and select **Actions** → **Investigate**. If you select multiple ports, they must all be of the same type (Figure 5-117 on page 199).

Note: Clicking **Clear All** deletes all items from the sidebar. If you want to clear select items, you must clear each checkbox individually.

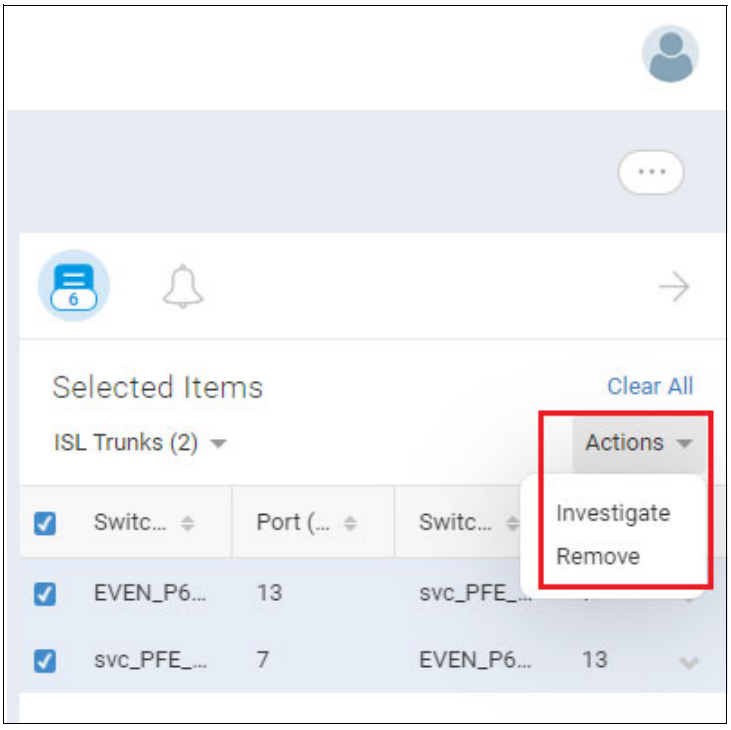


Figure 5-117 Sidebar select action

The Investigation Mode window opens.

5.8.3 Using Investigation Mode

SANnav Investigation Mode shows graphs of historic and real-time performance metrics for one or more switches, ports, tunnels, and circuits.

Investigation Mode launches when you click **Investigate** from the Inventory window, from dashboard widgets, or from the sidebar.

The Investigation Mode window consists of three parts: a Measures pane, a Details table for the selected entities (ports, switches, trunks, tunnels, or circuits), and a graph area. Select measures and entities that you want to investigate, and the resultant graph opens in the graph area (Figure 5-118).

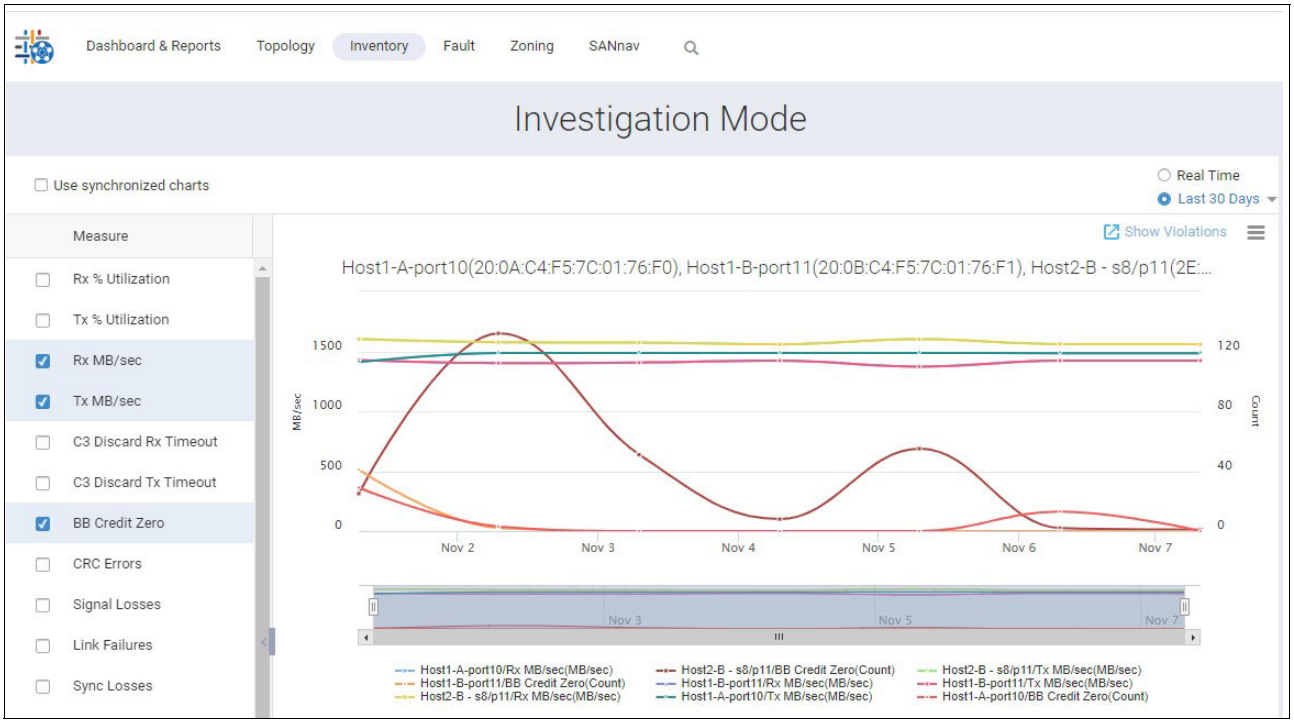


Figure 5-118 Using Investigation Mode

- Measures pane: Contains a list of measures that are available for the selected entities.
- Details table: Shows the entities that are selected for investigation.
- Graph area: Shows a different colored line for each selected measure-entity pair.

Measures pane

The list of available measures depends on the type of entity that is selected. For example, switches have different measures than ports, and Give ports have different measures than F_Ports and E_Ports.

Select the measures that you want to monitor. You can select up to six measures to monitor for a single entity. You can select up to four measures for multiple entities.

Select **Allow Zoom and Fetch** to view data points at a higher level of granularity. If this box is checked, you can select only a single measure.

After you select the measures, you can click **Hide** to hide the Measures pane and allow more space for the graph.

Notes:

- For switches, the CPU and memory utilization percentage measures are for the logical switch, not for the chassis.
- For switch ports, scroll to the bottom of the Measures pane to select port health, congestion, and port utilization violations. These violations measures are disabled when viewing the graphs in real-time mode.

Details table

The details table shows the items that were chosen for investigation.

Select items in the table to show in the graph area. You can select up to six items to show in the graph area.

You can show more items in the table by choosing the **All**, **Related**, or **Selected** options from the **Show** drop-down list:

- For switches, selecting the **All Products** option shows all switches across all fabrics that are discovered in SANnav.
- For E_Ports, selecting the **Related Ports** option shows the connected E_Ports on the other switch. For F_Ports, the **Related Ports** option shows all ports that are zoned to this port, based on active zones.
- For all other ports, tunnels, and circuits, selecting the **All** option shows all ports, tunnels, or circuits in the switch. If you originally selected items from different switches, all ports, tunnels, or circuits from each of the switches are showed.

The **Selected** option shows only the items that were originally chosen for investigation.

For ports, you can also select flows to investigate, if any are configured. For more information about investigating flows, see *Brocade SANnav Management Portal Flow Management User Guide, v2.2.1.x*.

Graph area

A graph plot depends on the measures that are selected. The graph area shows one line for each entity or measure pair.

Note: If the graph area is empty, either measures are not selected, or there might not be data to show for this combination of measure and port.

Historic and real-time data

By default, the graphs show historic data from the last 30 minutes. You can change this value by selecting the date range drop-down menu in the upper right of the graph area.

The graphs update periodically depending on the granularity of the selected date range:

- For date ranges of Last 30 Minutes, Last 1 Hour, and Last 2 Hours, the data shows in 5-minute intervals.
- For date ranges of Last 1 Day, Last 3 Days, and Last 1 Week, the data shows in 1-hour intervals.
- For a date range of Last 30 Days, the data shows in 1-day intervals.
- For custom date ranges, the data is showed once, and the graphs do not update.

In addition to viewing historic data, you can select **Real Time** to view “live” performance data, which is updated in 10-second intervals. If you are investigating switches, the **Real Time** option is not available.

Data points

Hover your cursor over a data point in the graph to see more details in a tooltip box.

Some data points might be missing, which might be due to an SNMP timeout or to performance data collection being disabled.

The graph in Figure 5-119 plots TX% utilization on two ports. Hovering your cursor over a data point in one line gives details for all data points for that same period. Note the missing data points, which are indicated by the red rectangle, which occurred earlier in the date range.

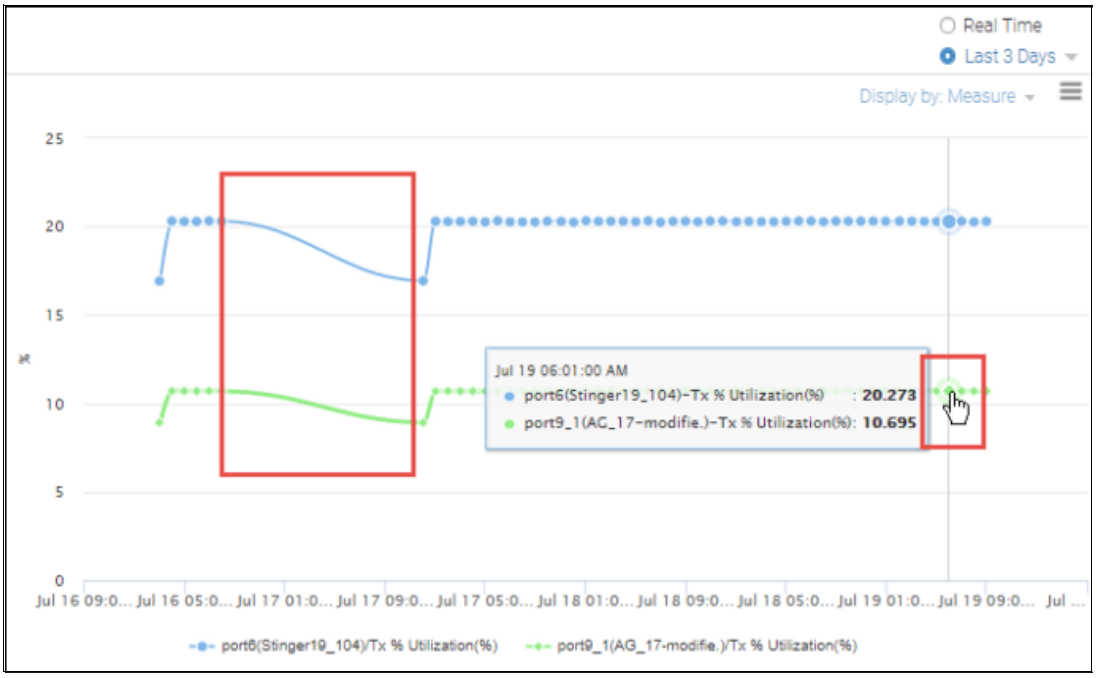


Figure 5-119 TX% utilization on two ports.

Zooming in on data

To zoom in on an area of the graph, drag out a rectangular area in the graph with your mouse pointer (Figure 5-120 on page 203).

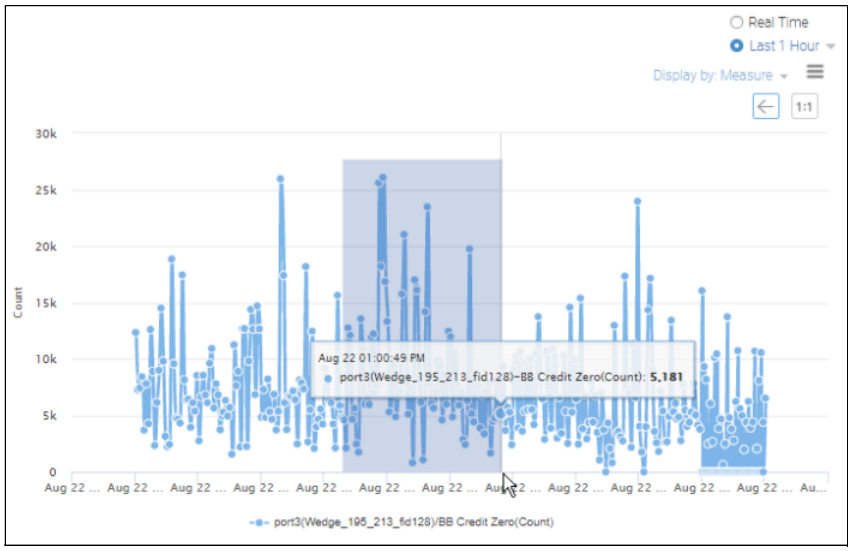


Figure 5-120 Highlighting part of a graph to zoom in

The graph is redrawn with the selected area magnified. Click **Back** in the upper right to return to the previous view (Figure 5-121).

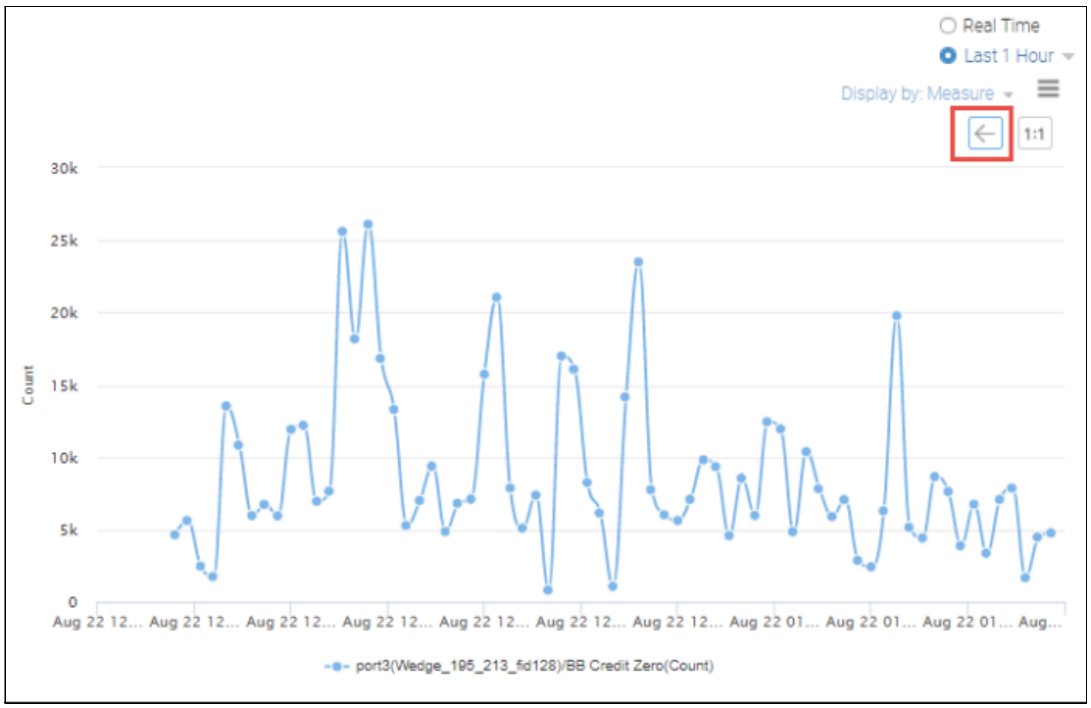


Figure 5-121 The graph is redrawn with the selected area magnified

Zoom and Fetch for higher granularity

For switch ports, you can obtain (“fetch”) a higher level of granularity for a data point with Zoom and Fetch. Click a data point in the graph, and then click **Zoom and Fetch** **(**Figure 5-122).

Note: You must select **Allow Zoom and Fetch** in the Measures pane to enable this capability.

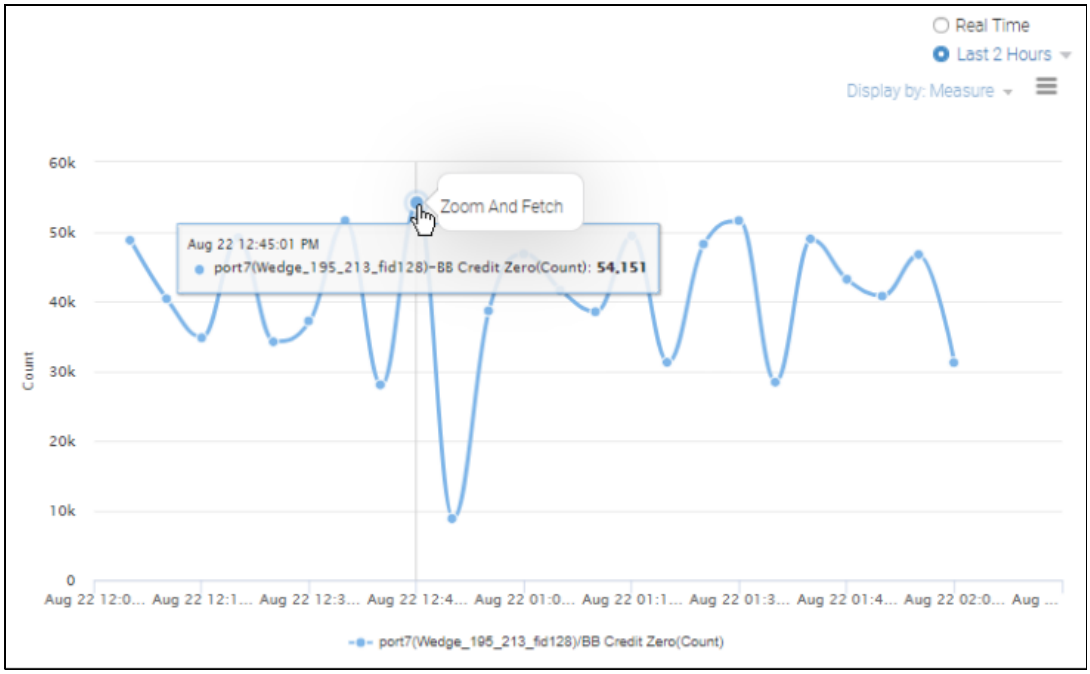


Figure 5-122 Selecting Zoom and Fetch

The graph shows at a higher granularity. Each successive application of Zoom and Fetch shows a greater level of granularity. For example, Zoom and Fetch that is applied to 1-day granularity shows data at 1-hour granularity. Applying Zoom and Fetch to 1-hour granularity shows data at 5-minute granularity.

Note: Zoom and Fetch is applicable only to FC switch ports of types E, F, EX, N, and SIM, and it is applicable only in a graph with one port and one measure. Zoom and Fetch is not available in real-time mode or if multiple ports or multiple measures are selected.

Graph legend

Below each graph is a legend, which lists the entity, measure, and unit of measurement for each line in the graph. You can click items in the legend to hide or show the corresponding lines in the graph.

Figure 5-123 on page 205 shows CPU utilization percentage for four switches. Two of the switches were cleared in the legend, so only two lines show in the graph.

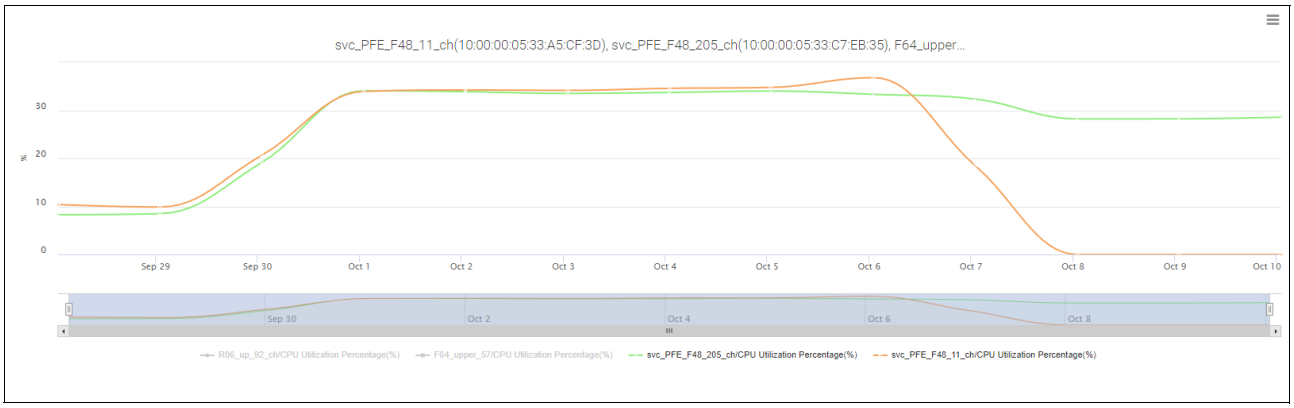


Figure 5-123 CPU utilization percentage for four switches

Types of graphs

The graph area can show different types of graphs:

- One entity and multiple measures
- Multiple entities and one measure
- Multiple entities and multiple measures

You can show one entity and up to six measures or one measure and up to six entities in a single graph.

If you show multiple entities and multiple measures, multiple graphs are generated. SANnav shows up to four graphs, and each graph is limited to four measures and four entities. The graphs can be showed by entity or by measure, depending on the value in the **Show by** drop-down menu (Figure 5-124).

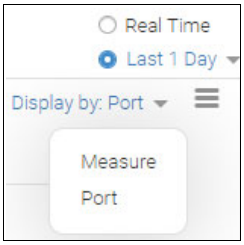


Figure 5-124 Show by drop-down menu

When multiple graphs are showed, you can move the slider bar at the upper left of the graph area to compress the graphs so that you can view more on a single window (Figure 5-125).

Note: When you compress the graphs, the legend below them disappears.

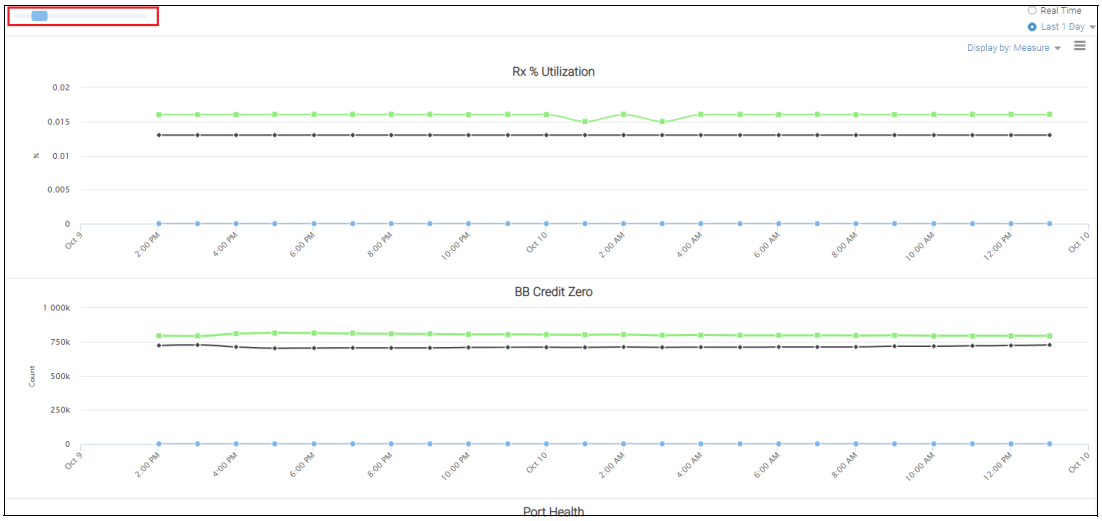


Figure 5-125 Compressing graphs

Exporting the graph

To export a static copy of the graph, click the hamburger icon in the upper right of the graph and select **Export**. An HTML file showing the graph is downloaded to your local machine.

Investigating trunks

SANnav Management Portal supports launching Investigation Mode for ISL trunks, IFL trunks, and F_Port trunks.

When investigating ISL trunks, you can plot a graph for either or both ends of the trunk. For IFL trunks, you can investigate only the backbone switch end of the trunk. For F_Port trunks, you can investigate only the non-Access Gateway switch end of the trunk.

For ISL trunks, select one of the options in the **Show Switches** drop-down list in the upper right of the graph area (Figure 5-126 on page 207):

- **Show Switches (1 & 2)** selects both ends of the trunk.
- **Show Switch (1)** selects the source end of the trunk.
- **Show Switch (2)** selects the target end of the trunk.

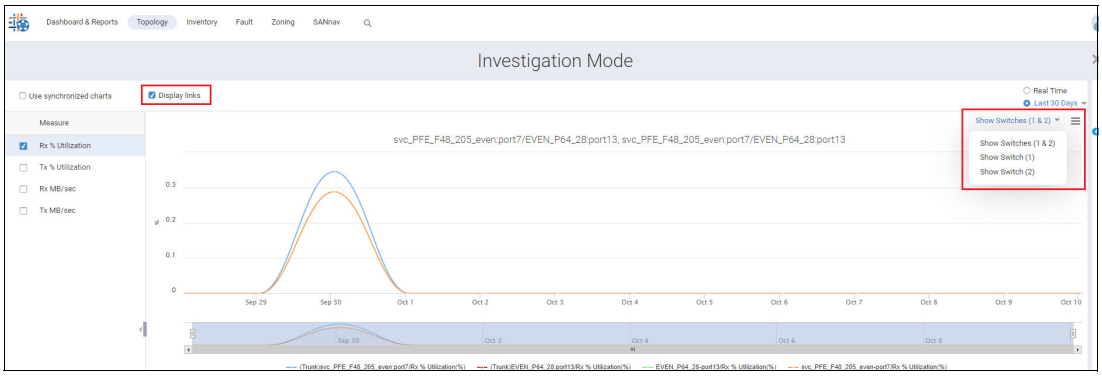


Figure 5-126 Investigating trunks.

To investigate links that are associated with trunk objects, select the **Show links** checkbox in the upper left of the graph area, as shown in Figure 5-126.

The **Show links** checkbox is enabled only if one measure and one trunk are selected.

In SANnav Management Portal, you can view switch port health, port congestion, and port utilization violations separately from the other switch port measures. You cannot show the violations in real-time mode.

To see the violations, complete the following steps:

1. Scroll to the bottom of the Measures pane and select the violations that you want to see, as shown in Figure 5-127.

   The violations measures are available only for switch ports. You can select violations measures regardless of the number of measures or ports that are selected.

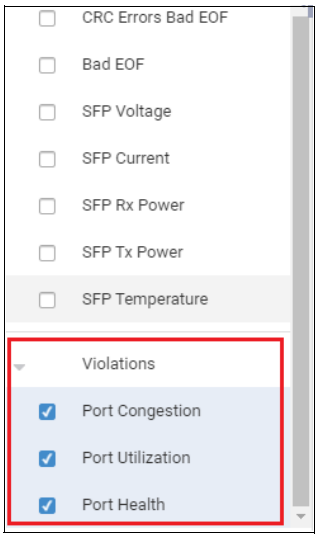


Figure 5-127 Investigating switch port violations

2. Click **Show Violations** in the upper left of the graph area. A dialog box opens and shows the violations as a series of bar graphs (Figure 5-128).

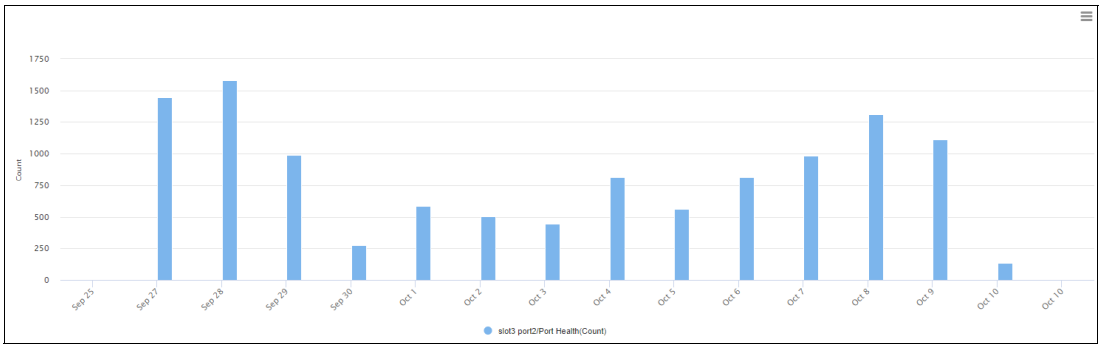


Figure 5-128 Show Violations

3. Hover your cursor over a bar to see details in a tooltip.
4. Click a bar to view violation details in table format (Figure 5-129).

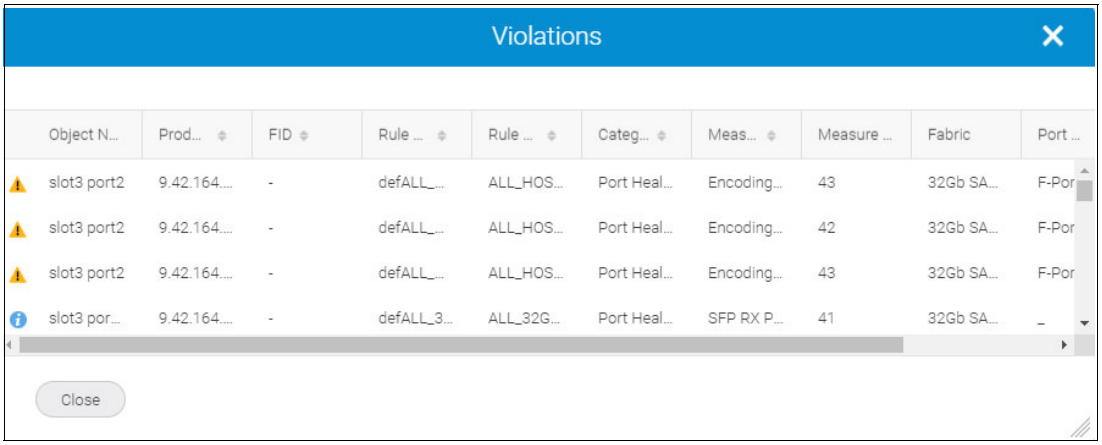


Figure 5-129 Violations details table

5. Click **Close** to close the dialog box.

5.8.4 Collecting high-granularity data

By default, SANnav Management Portal collects performance data at 5-minute intervals. SANnav can optionally collect and show performance metrics at 2-second intervals (for switch ports) or 5-second intervals (for extension tunnels and circuits).

- FOS 8.2.1b or later is required to support 2-second granularity for switch ports.
- FOS 9.0.0 or later is required to support 5-second granularity for extension tunnels and circuits.

To capture metrics at these intervals, you must schedule high-granularity data collection. High-granularity data collection is supported only on switches that support data streaming.

Scheduling high-granularity data collection

To capture high-granularity performance metrics, you must set up a schedule for the data collection in SANnav Management Portal.

Before you can schedule high-granularity data collection, you must have the following access: *Performance privilege with read/write permission*.

Unlike other scheduling in SANnav, you specify only a start time. You cannot specify an end time. The data collection continues for 3 days from the start time unless you stop it. The collected data is retained for 14 days, unless you delete it.

The maximum number of ports that can be scheduled for data collection is 100. The maximum number of extension tunnels is 10.

SANnav collects high-granularity data only on E_Ports, EX_Ports, F_Ports, N_Ports, SIM ports, extension tunnels, and extension circuits.

For extension tunnels and circuits, if one side of the tunnel is an unsupported platform, data is collected only for the side with the supported platform.

Note: After you set high-granularity data collection for a port or tunnel, you cannot set high-granularity data collection on the same port or tunnel until the previous collection is completed or stopped.

To schedule high-granularity data collection, complete the following steps:

1. Click **Inventory** in the navigation bar, and then select **Switch Ports** or **Extension Tunnels** from the drop-down list.
2. Select the ports or tunnels on which you want to collect high-granularity data.
3. To select a single port or tunnel, click the down arrow in the rightmost column and select **Schedule** from the action menu. Alternatively for ports, you can use the bulk select option to schedule multiple ports at the same time.
4. Click **More** and click **Bulk Select**.

Note: Although you can schedule a maximum of 100 ports for data collection, the maximum limit for scheduling ports at one time through the Bulk Select function is 20.

   A column of checkboxes shows on the leftmost side of the table.

5. Select the checkboxes for the ports on which you want to collect data, and then select **Actions** → **Schedule** in the upper right of the window.

6. Select the start date and time for the data collection (Figure 5-130).

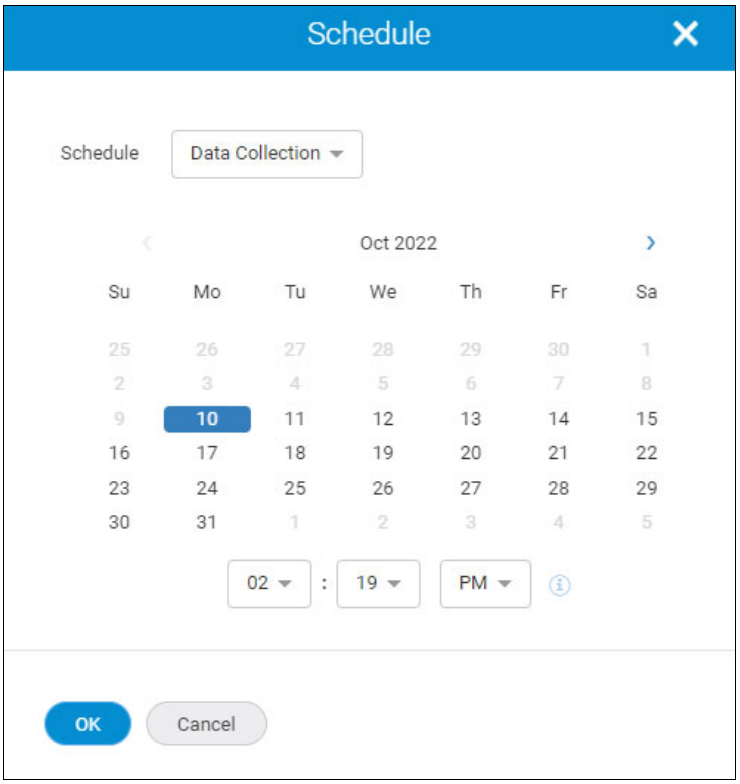


Figure 5-130 Selecting the start date and time for data collection

7. Click **OK**.

   Within 5 minutes of the specified start time, SANnav Management Portal collects metrics for the specified port or tunnel at high granularity. Collection of high-granularity metrics continues for 3 days. SANnav retains the collected data for 14 days.

8. Click the **Outputs** tab and select **Port Data Collection** or **Tunnel Data Collection** to view the scheduled collections.

   A separate output collection is generated for each port or tunnel (Figure 5-131).

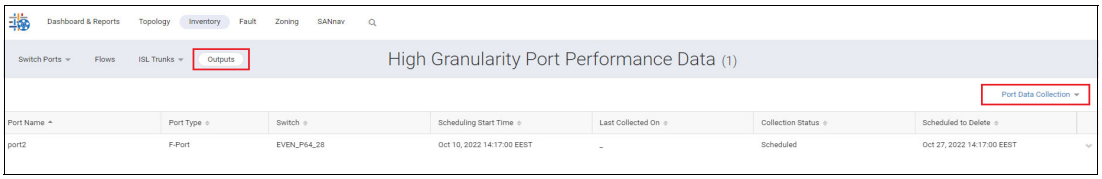


Figure 5-131 Outputs port data collection

9. To stop data collection or to delete a collection, click the down arrow to the right of the table entry and select **Stop Collection** or **Delete**.

   If you stop the data collection and then want to collect data again on the same port or tunnel, you must create another schedule. To investigate scheduled ports, use the navigator bar to zoom in to 2-second granularity for 2 hours.

Viewing high-granularity performance data

After you schedule high-granularity data collection in SANnav Management Portal, you can view the data after the collection completes or while the collection is in progress by completing the following steps:

1. Click **Inventory** in the navigation bar, and then click the **Outputs** tab.
2. Select **Port Data Collection** or **Tunnel Data Collection** to view the scheduled collections. The Collection Status column can have the following values:
   - Scheduled: High-granularity data collection is scheduled but has not yet started.
   - In Progress: Data collection is in progress for three days.
   - Completed: Data collection for three days is completed.
   - Paused: The Kafka connection is broken.
   - Stopped: Data collection was stopped by the user.

   The Last Collected On column shows the last time data collection occurred. This column is updated every 5 minutes. If the Last Collected On field has a value, that is, it is not blank, you can launch Investigation Mode to view the high-granularity data (Figure 5-132).

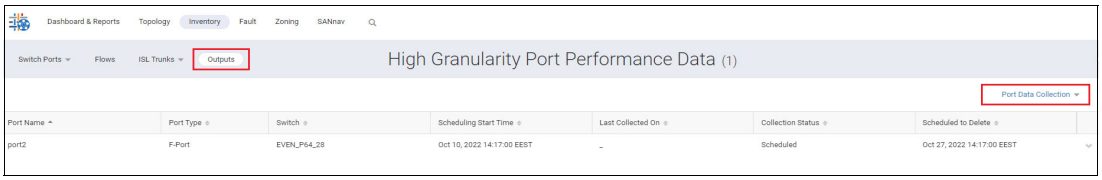


Figure 5-132 Outputs port data collection

3. Click **Investigate** from the action menu to the right of a table entry.

   Clicking **Investigate** launches Investigation Mode with a non-synchronized chart. The time range is based on the high-granularity data that was collected in this schedule. By default, the window loads with 1-hour granularity for the entire 3-day data collection period. If the data collection period was less than 1 day, then the granularity is 5 minutes. If the data collection period was less than 2 hours, then the granularity is 2 seconds (for FC ports) or 5 seconds (for extension tunnels and circuits).
4. Select a measure that you want to monitor.

   To view high-granularity data, you must click only a single measure.
5. To export the high-granularity data, click the hamburger icon in the upper right of the graph, select **Export**, and select whether to export the graph as an HTML or CSV file.

5.9 Reports

SANnav Management Portal implements a highly flexible reporting infrastructure that enables you to generate custom reports of your SAN environment based on your need.

You can generate reports on demand or schedule them to generate at daily, weekly, or monthly time intervals.

You can view the report output in SANnav, and you can export the output. Reports are generated in PDF, HTML, and CSV formats, which you can export to a compressed file.

In addition to exporting reports, you can also export report templates and then import the templates into another SANnav instance. In this way, you can share report templates across all SANnav instances.

5.9.1 Creating a report template

When you want to generate reports in SANnav Management Portal, first create a report template. The report template specifies the widgets to go in the report and the network scope, date range, and specific filters.

Complete the following steps:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.

   The Templates window lists all dashboard and reports templates.

2. Click **+** on the right side of the subnavigation bar and select **Report** → **Select Widgets** (Figure 5-133).

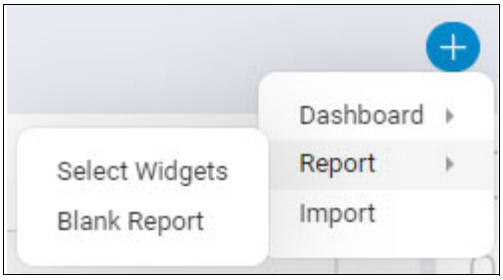


Figure 5-133 Creating a report

3. Select the widgets that you want in your report and click the right arrow to move them to the Selected Widgets list.

Tip: For the best performance, select no more than 16 widgets per report template.

You can select from two categories of widgets: Status and Performance.

The order of the widgets in the Selected Widgets list is the order that they are showed in the report.

If you select several widgets at once and then click the right arrow to move them to the Selected Widgets list, the widget sequence is maintained. You cannot resort the widgets after the move.

If you want the widgets in a particular order, select each widget separately, and then click the right arrow before selecting the next widget (Figure 5-134 on page 213).

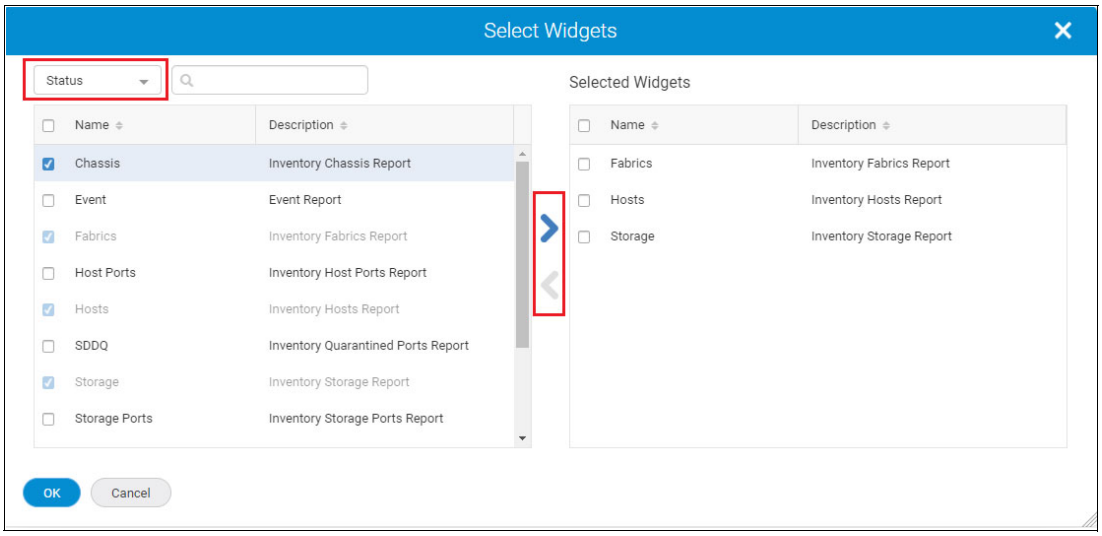


Figure 5-134 Report: Select Widgets

4. Click **OK** when you are finished adding widgets.

   The template shows placeholders for each widget.

5. Add filters to the report template by clicking **+** on the left side of the filter bar. These filters apply to all widgets in the template. The generated report contains data for only those objects that meet the filter requirements.

Notes:

- Filters are not applicable to circuit or extension widgets.
- Although there is no restriction on the number of filters that can be added or applied as part of the report template, a best practice is two parameter conditions within a filter and two filters within a report.

6. Customize the network scope and date range by using the drop-down lists on the right side of the filter bar (Figure 5-135).

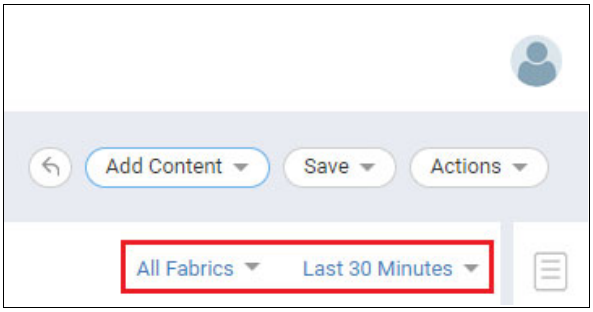


Figure 5-135 Customizing the scope

7. Customize the widgets (Figure 5-136).

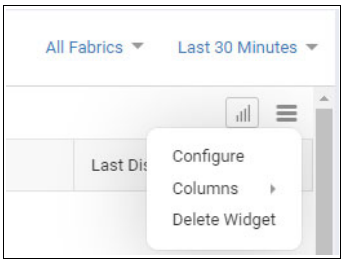


Figure 5-136 Customizing widgets

8. Click the hamburger icon for each widget to do the following tasks:
   a. Change the name of the widget in the report by using the **Configure** option.
   b. Add or delete columns for tabular widgets.
   c. Delete the widget from the report.

   You cannot rearrange the widgets in the report, but you can add widgets to the top and bottom of the report by selecting **Add Content** → **Add Widgets** in the subnavigation bar.
9. Customize the widget content, if applicable.

   Some of the widgets provide or require more customization. For time series widgets, you must specify filters to filter the data based on average value or number of occurrences.

Note: If you do not specify filters for time series widgets, the generated report contains zeros for these widgets.

For example, Figure 5-137 shows how you can generate a time series report if the Rx utilization of a port reaches or exceeds 95% at least 10 times.

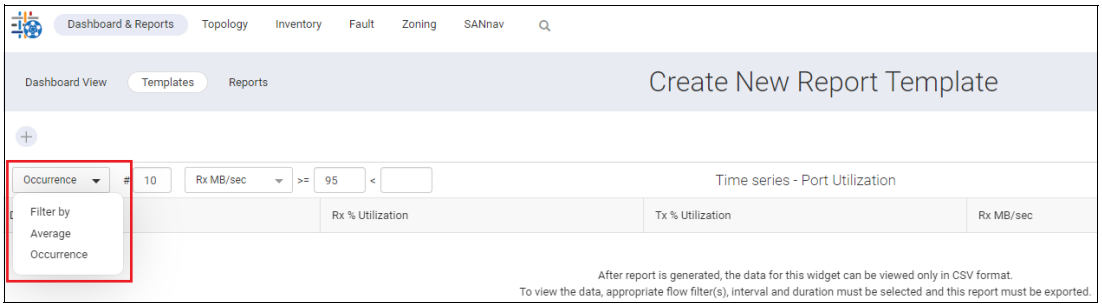


Figure 5-137 Time Series Rx Util

Other widgets might provide more customization options. For example, some of the top utilization widgets require that you select a measure and a utilization percentage (Figure 5-138 on page 215).

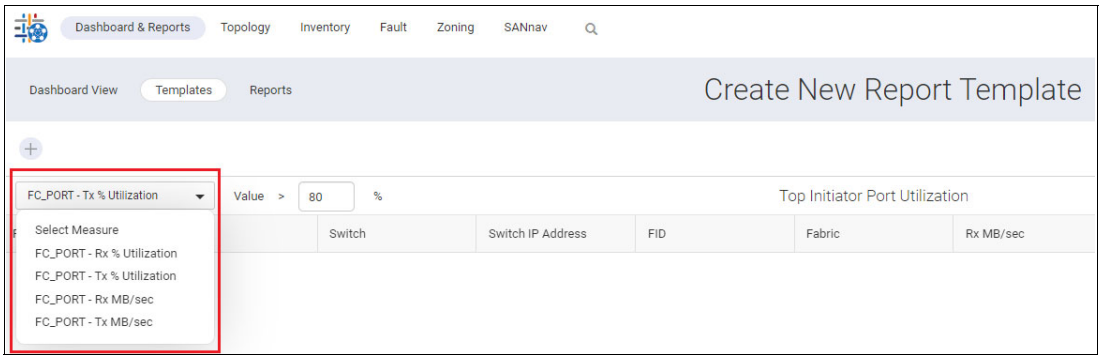


Figure 5-138 Top Init Tx Util

10. Select either **Save** → **Save** or **Save** → **Save As** to save the report template (Figure 5-139).

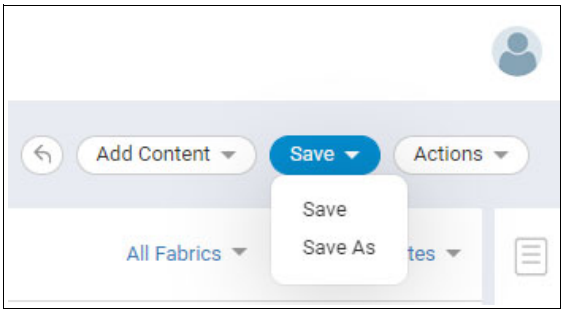


Figure 5-139 Saving the template

When you save the template, you must supply a name for the template, optional tags, and a description. The template name can contain alphanumeric and special characters except for the following special characters:

`/ \ : * ? % " < > | '`

5.9.2 Editing a report template

After you create a report in SANnav, you might want to change it or create another, similar report. You can edit the template and replace it or save it as a new template. To do so, complete the following steps:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar. The Templates window lists all dashboard and reports templates.
2. To edit the template name, tags, description, and sharing, find the report template that you want to modify, and from the action menu on the right side of the table, select **Edit Info** (Figure 5-140).

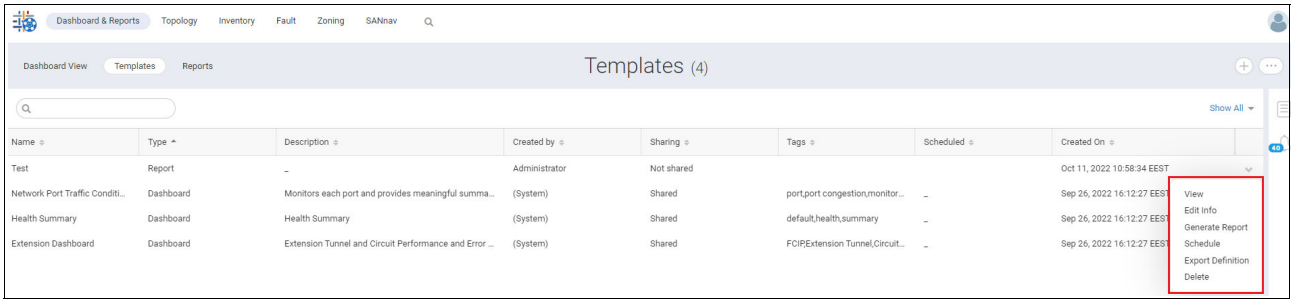


Figure 5-140 Editing the report

The Edit Info dialog box allows you to change the template name, tags, and description. From here, you can also designate whether the template may be shared with other SANnav administrators.

3. To edit the template, from the action menu, click **View** to show the template layout.
4. Add widgets and save the template (Figure 5-141).

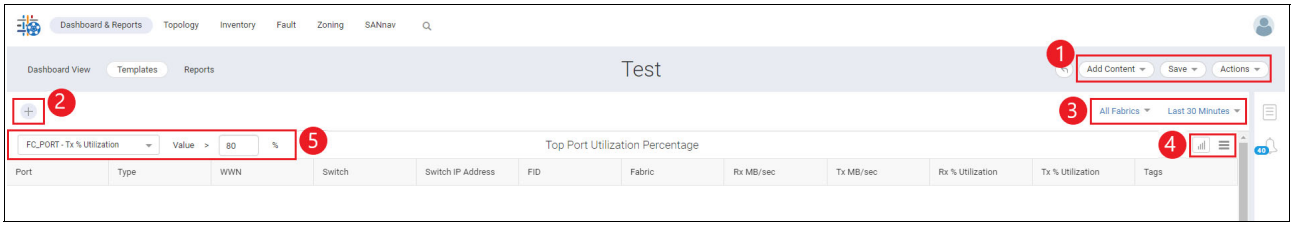


Figure 5-141 Edit from view

Note: In Figure 5-141, items 1, 2, and 3 affect the entire report. Items 4 and 5 affect a specific widget.

- 1: The Actions drop-down menu provides more options, including updating the schedule and exporting the template definition.
- 2: Add filters for the report.
- 3: Update the network scope and date range.
- 4: Replace or delete the current widget, change the widget name, and customize the showed columns for the widget.
- 5: More filters for some widgets.
- 6: Make changes to the template.

5. Add widgets and save the template.
6. Select **Save** → **Save** to replace the template, or click **Save** → **Save As** to make a copy of the template and save it with a different name.

5.9.3 Scheduling a report

In SANnav, you can schedule a report to run later.

If you want to specify an email address to which the generated report is sent, the email server must be configured and enabled in SANnav, as described in “Configuring an email setup” on page 227.

Note: A maximum of four schedules can be associated with one report template.

To schedule a report, complete the following steps:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Find the report template and click **Schedule** on the down arrow to the right of the table entry (Figure 5-142).

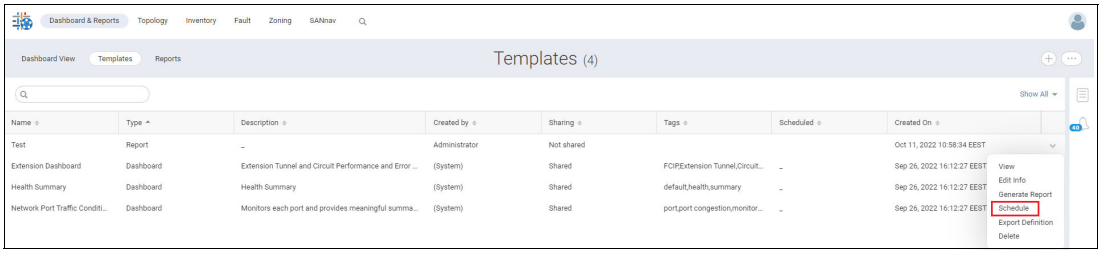


Figure 5-142 Schedule Report

3. Select a time interval and a time to run the report.

   For example, Figure 5-143 shows scheduling a report to run every Sunday at 12:00 AM.

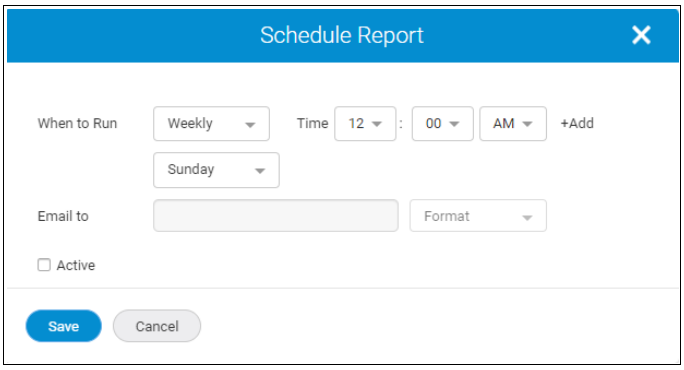


Figure 5-143 Schedule Report

4. Specify the email address of the receiver and the formats in which the report is sent.

   You can enter multiple email addresses separated by commas. If the Email to field is disabled, an email server is not configured or is not enabled in SANnav.If you select multiple formats for the report output, they are compressed into one file (Figure 5-144).

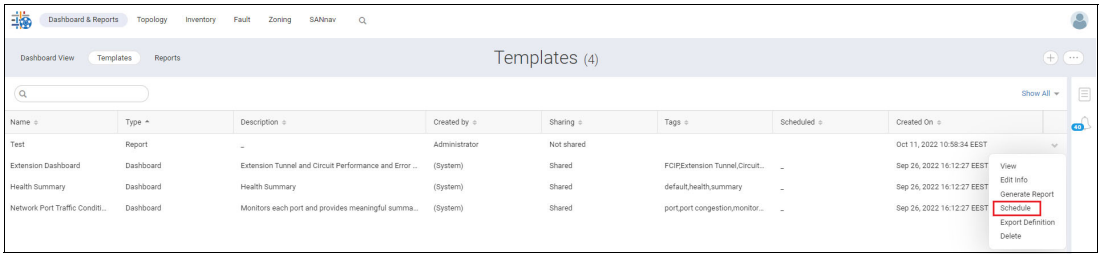


Figure 5-144 Schedule Report email

5. Select **Active** to activate the report schedule.
6. Click **+ Add** to add another schedule. You can add up to four schedules.
7. Click **Save**. On the Templates window, the Scheduled column now shows the schedule for when the report runs.

5.9.4 Generating and exporting reports

In SANnav, in addition to scheduling reports, you can generate and view a report at any time. You can also export the generated output to PDF, HTML, and CSV files. To accomplish these tasks, complete the following steps:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar. The Templates window lists all dashboard and reports templates.
2. Find the report template that you want and select **Generate Report** from the action menu. The report starts generating. This process might take some time depending on the contents of the template.
3. Click **Reports** in the subnavigation bar. The Reports window lists all reports that were generated by logged-in users in the past 30 days. Reports older than 30 days are automatically deleted.
4. Find the report that you want to see and select **View** from the action menu (Figure 5-145).

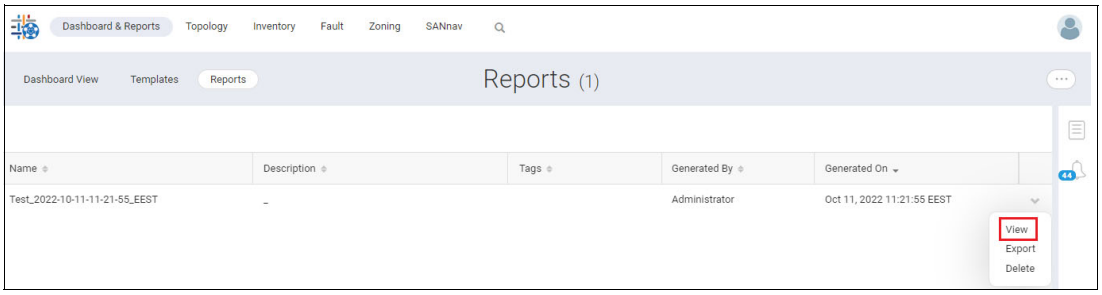


Figure 5-145 View report

The report is showed in HTML format.

Note: Time series reports are generated in CSV format only. To view the data for time series reports, you must export the report and open the downloaded compressed file.

At the upper left, the context of the reports (applied filters, and so on) is showed.

The generated output data and date range have the time zone of the browser that is used to schedule or generate the report (Figure 5-146).

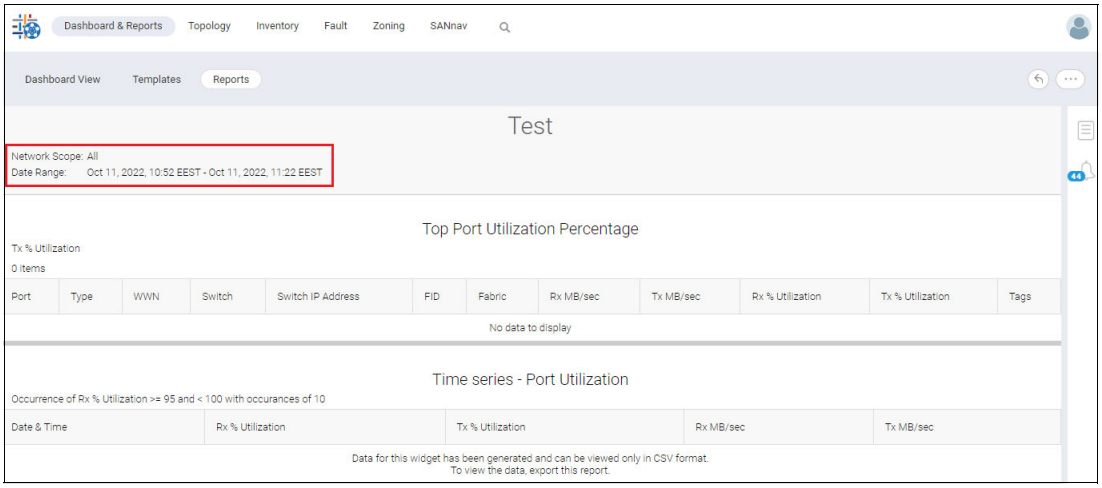


Figure 5-146 View report

5. Click **More** and then select **Export** to download and export the report. The report is downloaded as a compressed file containing HTML, PDF, and CSV files.

5.10 Fault Management

Using Fault Management features, you can register to receive SNMP traps, Syslog events, and other information from switches; you can view, search, and filter event logs; and you can forward SNMP traps and Syslog messages to the selected destinations. You can filter email event notifications based on event rules and switches.

Here are some of the actions that you can configure for events:

- Generate email alerts.
- Trigger a supportsave or field-replaceable unit (FRU) dump.

You can perform powerful event analysis by filtering events by using network scope, date range, and custom filters. You also can perform searches within the event log and generate event or violation reports.

In addition, Fault Management provides several event-managing widgets, such as the Top N Events, Events Summary, and Health Violations widgets, which you can add to dashboards.

Registration for all switches is mandatory for viewing all the events of all the discovered switches. There are two types of registration:

- SNMP Trap/Informs registration
- Syslog/Secure Syslog registration

5.10.1 Registering for SNMP traps and Syslog recipients

SANnav provides an option to automatically register the SANnav server as an SNMP trap recipient for the discovered switches. SANnav also provides an option to automatically register all servers as Syslog recipients.

SANnav supports two types of SNMP notifications:

- Traps
- Informs

With SNMP traps, the receiver does not send any acknowledgment when it receives a trap; thus, the sender cannot determine whether the trap was received. With informs, the receiver of the inform returns an acknowledgment to the SNMP agent.

To enable automatic SNMP trap and Syslog registration, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Fault Management** → **SNMP and Syslog Management**.
2. Select the **Registration** tab. The SNMP and Syslog Registration window opens.
3. To enable automatic registration of SNMP informs, select the **Enable Informs** option to register SNMP as an SNMP informs; otherwise, it is registered as an SNMP trap (Figure 5-147).

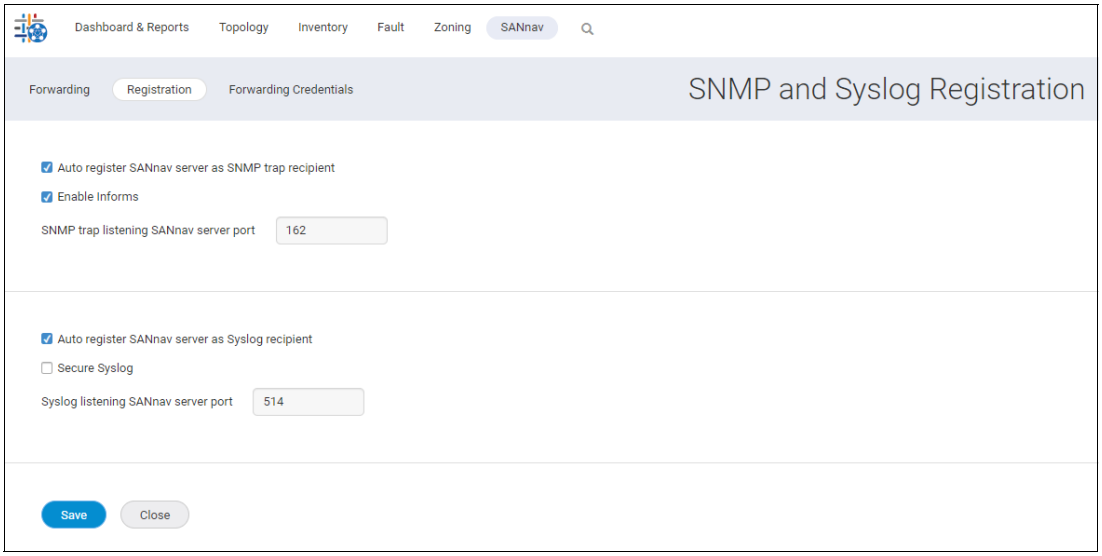


Figure 5-147 Enable Informs: SNMP

By default, the **Auto register SANnav server as SNMP trap recipient** option is selected to register new switches automatically.

Notes:

- The **Auto register SANnav server as SNMP trap recipient** option must be enabled to register new switches automatically.
- You cannot modify the **SNMP trap listening SANnav server port** option because it is defined by you at the time of SANnav installation.
- SNMP traps are less reliable than informs because the sender does not know whether the receiver received the traps. When informs are enabled, SANnav acknowledges an inform message with an SNMP response PDU. If the sender does not receive a response for an inform, the inform is sent again.

4. To enable secure Syslog registration, select the **Secure Syslog** option to register the SANnav server for secure Syslog reception; otherwise, the SANnav server is registered for Syslog. By default, the **Auto register SANnav server as Syslog recipient** option is selected to register the new switches automatically.

Notes:

- If the **Auto register SANnav server as Syslog recipient** option is not enabled, the new switches are not registered automatically.
- You must manually import the SANnav server certificate in the switch (see 5.10.2, “Importing the server certificate on the switch” on page 221).
- You cannot modify the **Syslog listening SANnav server port** option because it is defined at the time of SANnav installation.

5. Click **Save** to save the settings.
6. Click the back arrow in the upper right to return to the Configurations and Settings window.

5.10.2 Importing the server certificate on the switch

The switch verifies the Syslog certificate when the secure Syslog is enabled at the time of Syslog registration. You must import the server Syslog certificate into the switch by using the switch CLI. Complete the following steps:

1. Enter **`seccertmgmt import -ca -server syslog`** to import the Syslog certificate to the switch.
2. Enter the protocol `ftp` or `scp`.
3. Enter the IP address of the certificate server in `Enter IP address`.
4. Enter the location of the certificate in `Enter remote directory`.
5. Enter the certificate file name in `Enter certificate name`.

Note: The `ca-cert.pem` certificate is in the `$INST_HOME/kafka/certs/caroot` directory.

6. Enter the login name and password of the certificate location, and press Enter to import the server certificate. You also can enter **`seccertmgmt show -all`** to verify the Syslog certificate files.
7. Enter **`seccertmgmt delete -ca -server syslog`** to delete a current server Syslog certificate.

5.10.3 Enabling or disabling SNMP informs

Enabling SNMP informs allows SANnav to acknowledge the trap. It also helps enable or disable informs at the switch level on informs-capable products.

To enable or disable SNMP informs, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Fault Management** → **SNMP Informs**.
2. Click **Select Fabric**, and then click **OK** to list all the informs-capable products. You can also enter the fabric name in the search bar.
3. Click **More (…)** at the upper right of the window, and then select **Bulk Select** (Figure 5-148).

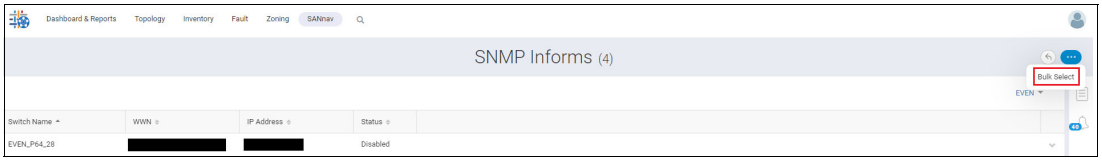


Figure 5-148 Bulk Select SNMP informs

The select options for the switches appear.

4. Select one or more switches that you want to enable or disable.
5. Click the action menu, and then select **Enable** or **Disable** (Figure 5-149).

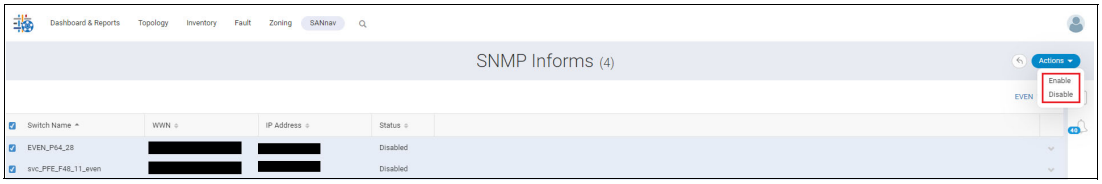


Figure 5-149 Bulk Select SNMP informs

SNMP informs are enabled or disabled at the switch level. To receive informs, enable the **SNMP Informs** option in the **SNMP Trap** tab.

5.10.4 Enabling email notifications

You can enable email event notifications in the user preferences. SANnav supports filtering email notifications that are based on event rules and switches. You cannot receive the event notification unless the administrator enabled email event notifications. Email notifications are sent according to the configured frequency in the SANnav Email Setup window.

Notes:

- You must set the duration to receive the event emails on the SANnav Email Setup window and configure the email ID in the SANnav User Management window under Security.
- Email notifications contain a maximum of 5000 combined events and violations, of which 2500 are events and 2500 are violations.

For more information about the email setup, see “Configuring an email setup” on page 227.

To enable email notifications, complete the following steps:

1. Click **User Preferences**. The User Preferences window opens.
2. Click **Edit** next to Email Notifications (Figure 5-150).

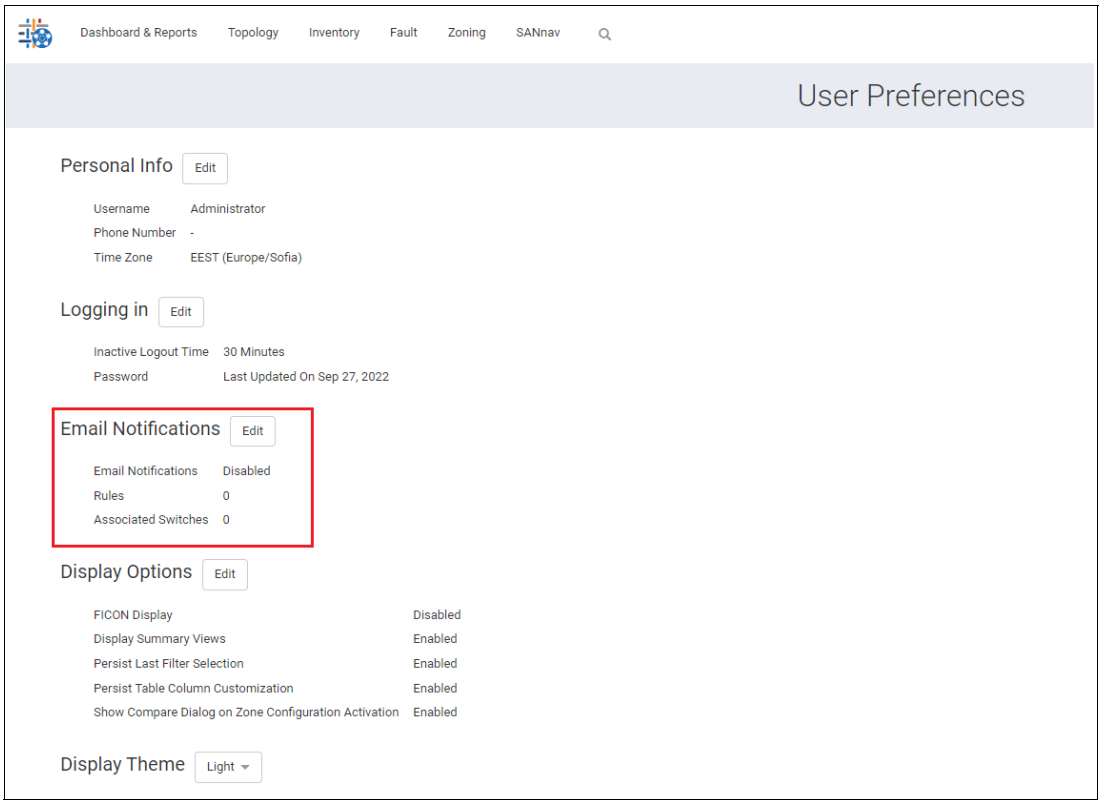


Figure 5-150 Email notifications

The Email Notifications window opens.

3. Select the **Enable Email Notifications** checkbox. When you select **Enable Email Notifications**, you can add or remove rules that are associated with the events or violations and associate switches to these rules (Figure 5-151).

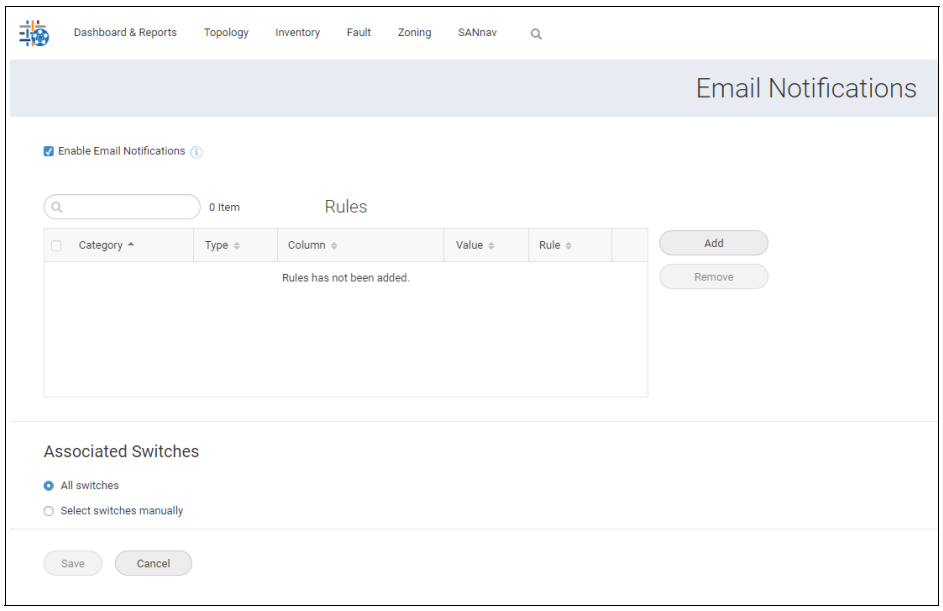


Figure 5-151 Enabling email notifications

4. Select **Add** from the Rules table. The Select Rules window opens (Figure 5-152).

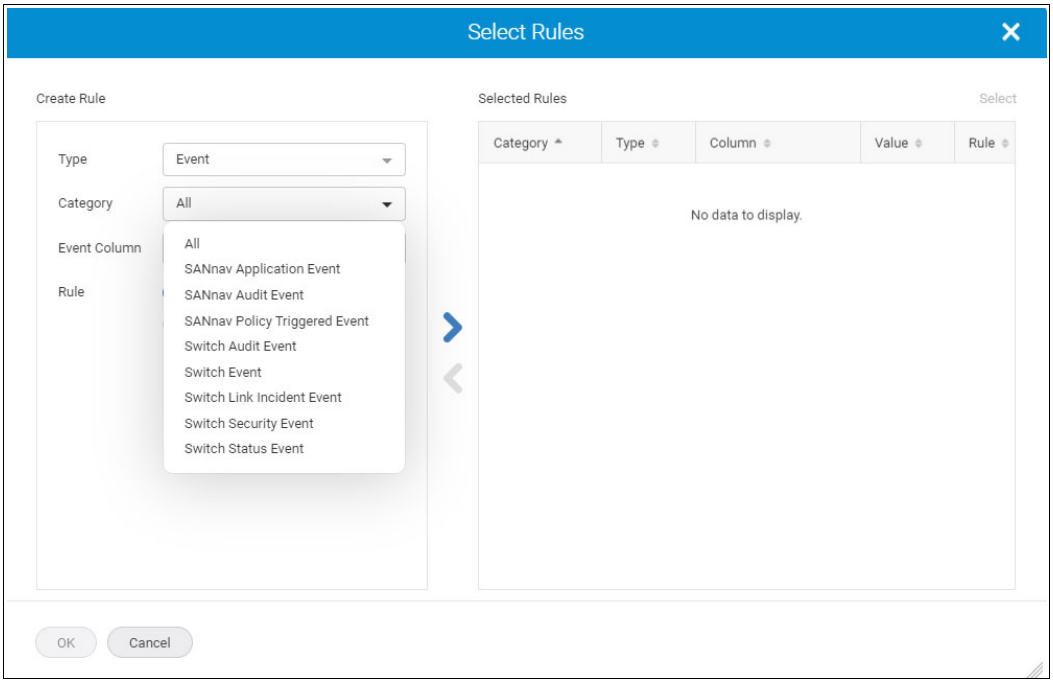


Figure 5-152 Adding email rules

5. To add event rules, select the rule type, rule category, associated event column, and the respective value of the event column to add event rules. You also can include or exclude these rules by using the **Include** or **Exclude** options (Figure 5-153). When you create multiple rules with similar event or violation columns, events or violations that match any of these rules are forwarded through email. When you create multiple rules with different columns, events or violations, all rules are forwarded through email.

Note: The **Exclude** option is disabled when you select the event or violation category as **All**.

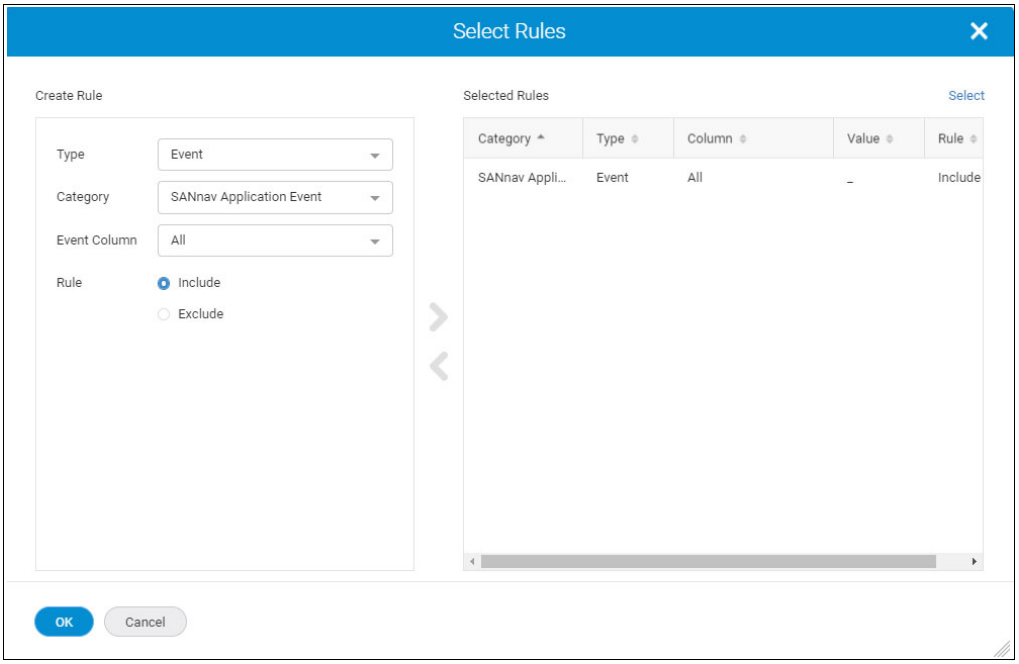


Figure 5-153 Include/Exclude rule

6. Click **OK**. The newly created rule is added to the Rules table. You can select either all switches or a particular switch for receiving email notifications.

7. If email notifications are required from a particular switch, complete the following steps:
   a. Select the **Select switches manually** option, and then click **Add** next to the Associated Switches table. You can also remove associated switches from the Associated Switches table (Figure 5-154).

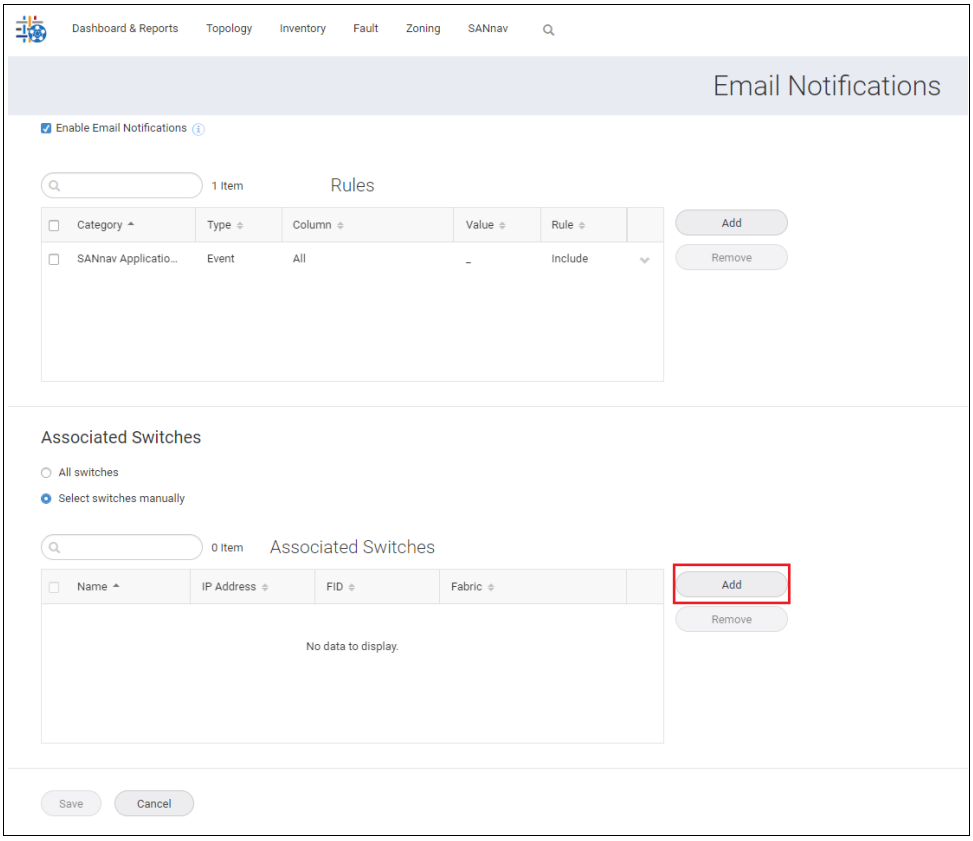


Figure 5-154 Select switches manually window

The Add Switches window opens.

   b. Select the switches from the list, and then click **OK** (Figure 5-155).

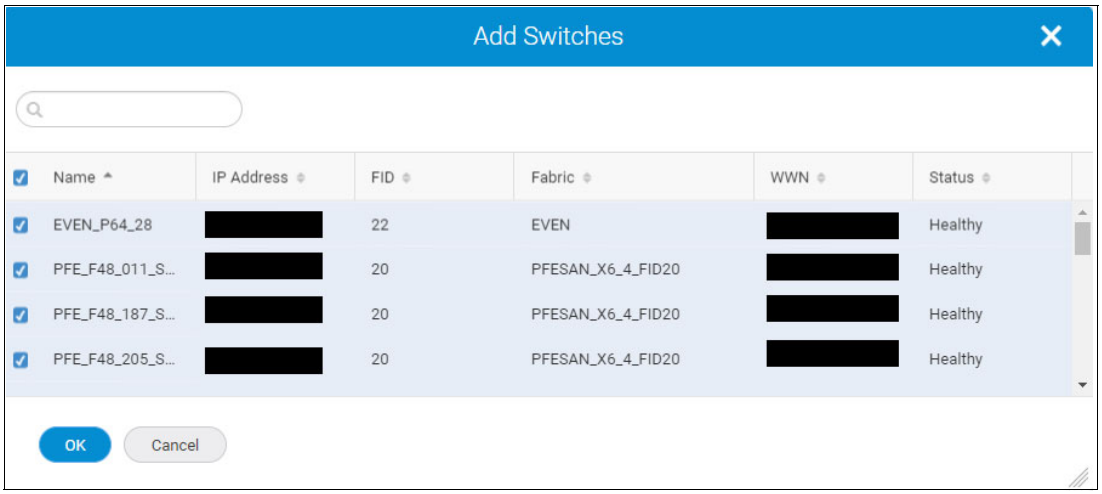


Figure 5-155 Add Switches

8. If email notifications are required from all switches, select the **All switches** option.
9. Click **Save**. The email notifications setting is saved.

Note: To start sending emails for event notifications, you must complete the following tasks:

- The SANnav Email Setup window must be configured and enabled.
- The User Management window must be configured with a valid email address.

Configuring an email setup

You can configure the email server to send event notifications to users who are enabled to receive them. You can set the interval to receive email event notifications for new events and violations that are received by SANnav.

Note: To receive email notifications, you must enable event notifications in the user preferences and set the duration to receive the email notifications (see 5.10.4, “Enabling email notifications” on page 222).

To set up your email account, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services** → **SANnav Email Setup**. The SANnav Email Setup window opens.
2. Enter the email server in the Email Server field.
3. Select **None**, **SSL**, or **TLS** from the **Security** drop-down menu.

Note: When you select security as **SSL** or **TLS**, the `SMTP ID` and `SMTP Password` fields are available.

4. Enter the SMTP port number, ID, and password in their fields.
5. Enter the email address in the Reply Email field. The reply email is the email address to which reply notifications are sent.
6. To send a test email, select the **Test Email** checkbox; the **Send email to** option is enabled, and then click **Send**. The **Send email to** option is used to specify the list of users to receive the test email notification.

Note: When you have more than one email ID to set up, enter commas between the email IDs with no space to separate the email IDs.

7. To set the frequency for receiving email event notifications, enter the time interval for the notification in the Email Notification Frequency field, and select the time from the drop-down in **Minutes** or **Hours**.

   The range for Minutes is 1 - 59, and for Hours, it is 1 - 24.
8. Click the **Enable** checkbox to activate the email configuration.

9. Click **Save** to save the email setup (Figure 5-156).

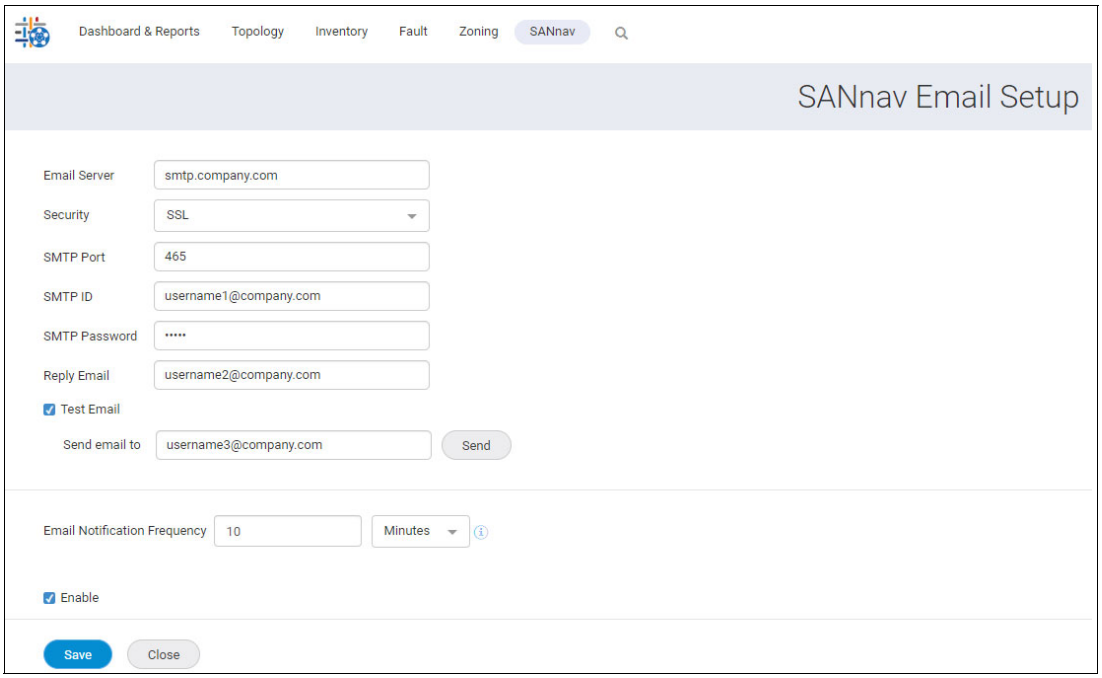


Figure 5-156 Email setup

5.10.5 Forwarding

You can forward the SNMP trap and Syslog messages to a third-party application or server. SANnav uses UDP for forwarding the Syslog messages to a third-party application or server. The forwarded messages are not secure Syslogs. You can assign the ports as 1 - 65535 while forwarding the Syslog messages. You can forward application events as traps and syslog. You can customize the configuration of forwarding for both SNMP trap and Syslog messages.

Note: If the SANnav license expires, SANnav cannot forward the SNMP and Syslog messages to a third-party application server.

To forward SNMP trap and Syslog messages, define the following two tabs:

- **Forwarding**: You can configure the Forwarding filter and define the destination details of the third-party application or the server where the SNMP trap and Syslog are forwarded.
- **Forwarding Credentials**: You must configure credentials before you configure SNMP Trap forwarding destinations. You can specify authentication or privacy protocols for the trap messages to forward to the other server.

Configuring forwarding destinations

You can set up filters to determine which traps and messages are forwarded. You can create a forwarding filter from the Filter Management and the Forwarding Destination windows. SANnav supports adding multiple destinations with the same IP address.

You can filter Syslog and SNMP traps messages based on one or more of the following criteria:

- Event category
- Event column
- Corresponding event value
- Include or Exclude rule

SANnav supports creating Syslog and SNMP trap forwarding filters based on the following event categories:

- SANnav Application Event
- Switch Event

Notes:

- When you create a forwarding filter from the Filter Management window, the filter is common for both SNMP and Syslog. Thus, the OID is ignored for Syslog forwarding. The OID is applicable only for SNMP trap forwarding.
- MAPS violations are forwarded with or without applying a filter. The description field (under the Event Column) is not supported while creating a filter for MAPS violations.
- The severity filter is different for switch events and for the SANnav application events. The switch severity filter column filters based on actual switch severities, but the SANnav application event column filters based on grouped severities.

To create a forwarding filter and add a destination for the forwarding filter, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Fault Management** → **SNMP and Syslog Management** → **Forwarding**.

Note: To create a forwarding filter from the Filter Management window, click **SANnav** in the navigation bar, and then select **SAN Monitoring** → **Filter Management**.

   The Forwarding Destinations window opens.

2. Select **+** at the upper right of the Forwarding Destinations window (Figure 5-157).

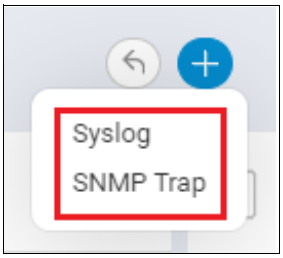


Figure 5-157 Selecting +

   The Syslog and SNMP Trap options appear.

3. Select **Syslog** or **SNMP Trap**. The Create New Syslog Destination or Create New SNMP Trap Destination window opens.

4. Click **Add** in the Filters table to add a filter. You can add a predefined filter, or you can create a filter (Figure 5-158).

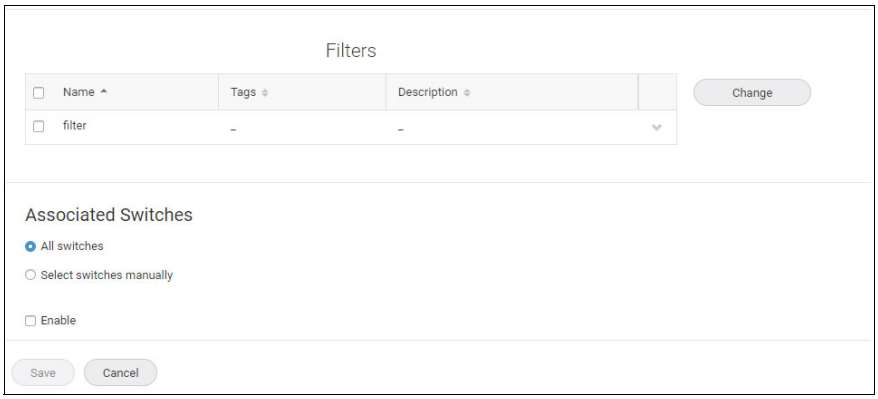


Figure 5-158 Forwarding filter

Note: SANnav supports adding only one forwarding filter while creating forwarding destinations. After you add the filter, the **Add** button changes to the **Change** button. If the Filters table contains an existing filter, click **Change** to create and replace the existing filter with a new filter.

5. To create a filter, select **Create New** from the Add Filter window (Figure 5-159).

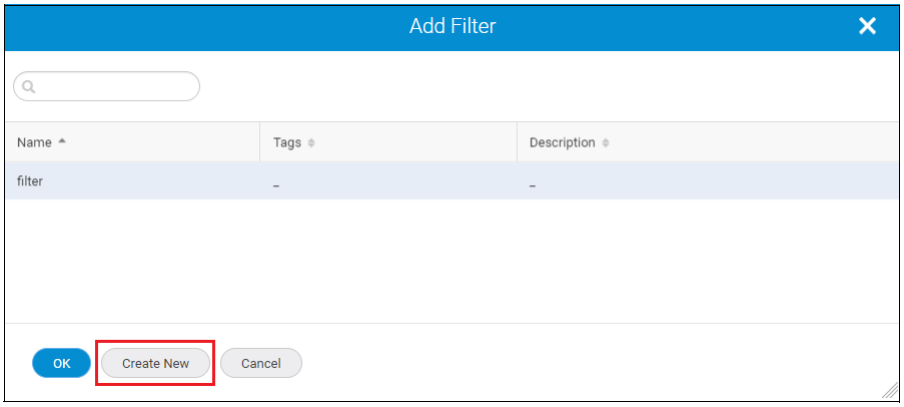


Figure 5-159 Creating a forwarding filter

The Create New Filter window opens.

6. Enter a unique filter name along with tags and a description.
7. Create a filter rule by providing the event category, event column, and respective value of the event column (Figure 5-160 on page 231). You can also include or exclude these rules by using the **Include** or **Exclude** options. You can create multiple rules in a single fabric. When you create multiple rules with similar event columns, events that match any of these rules are forwarded to the destination server. When you create multiple rules with different event columns, events that match all the rules are forwarded to the destination server.

   For more information about creating a filter with include "and" or "or" exclude rules, see “Examples for creating filter rules ” on page 235.

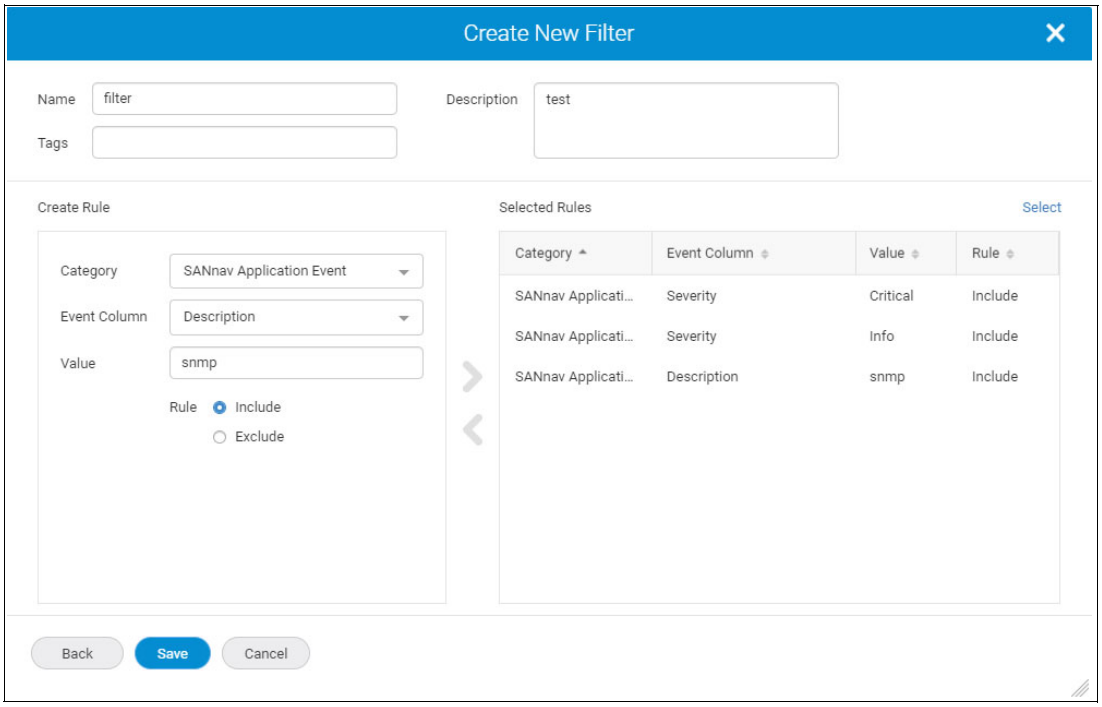


Figure 5-160 Creating a forwarding filter

8. Click **Save**. The filter is created in the Filters table. You can select either all switches or a particular switch for filtering events. You can view the filter by selecting **View** from the available filter.
9. To manually filter events from particular switches, select the **Select switches manually** option, and then click **Add** next to the Associated Switches table. You also can remove associated switches from the Associated Switches table. Select the switches from the Add Switches list, and then click **OK**.
10. If you want to filter events from all switches, select the **All switches** option.

Note: When you select the repeater option, the associated switches and filter options are disabled. The repeater option mirrors or forwards all Traps or Syslog messages that are received from switches to the forwarding destinations.

11. To add a destination for forwarding, enter the IP address along with the description and tags.

Note: Only IPv4 addresses are accepted. Domain nameserver (DNS) names are not accepted.

12. Enter the port number 1 - 65535.
13. Select the **Repeater** option when the filter is not required. By selecting the **Repeater** option, all Syslog or SNMP information is sent to the assigned destination.

Note: If you do not add any filters, you must select the Syslog or SNMP Trap repeater option to save the destination.

14. After entering the SNMP trap forwarding destination details, you can click **Actions** at the upper right of the Create New SNMP Trap Destination window to send a test trap (Figure 5-161). The IP address and destination port are mandatory for sending a test trap. If any of them are not entered or are invalid, an error message shows:

    `Enter a valid IP address.`

    On successful completion of the test trap forwarding, a message shows:

    `Test trap has been sent successfully.`

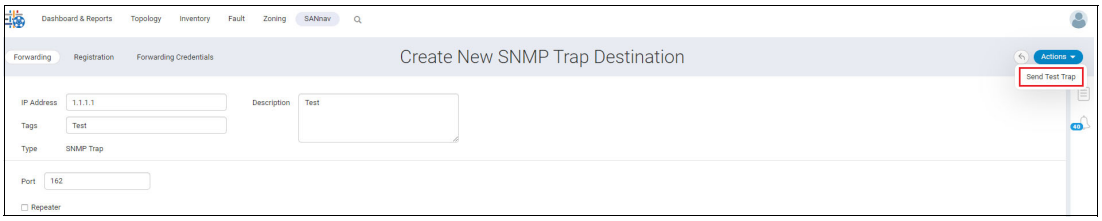


Figure 5-161 Send Test Trap

15. Select **Enable**.
16. Click **Save**. Configure forwarding credentials to send notifications. Click **Next** to set up credentials now or **Close** to set up later.

Modifying an existing forwarding destination

SANnav supports modifying an existing forwarding destination. To modify an existing forwarding destination, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Fault Management** → **SNMP and Syslog Management** → **Forwarding**. The Forwarding Destinations window opens and shows the list of existing destinations.
2. Select **View** from the action menu of an existing forwarding destination (Figure 5-162).

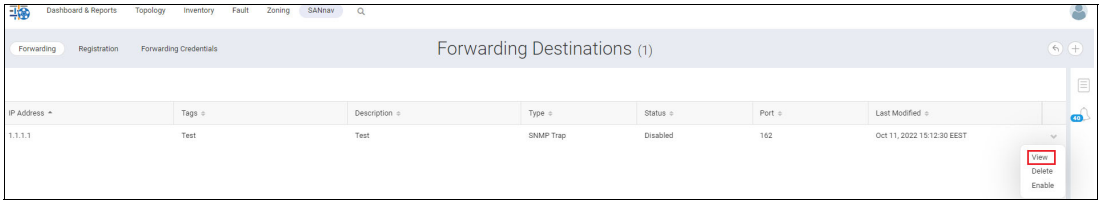


Figure 5-162 Editing forwarding destinations

The Forwarding Destination window opens.

3. Make the required changes.

Note: While modifying a forwarding destination, if you do not have AOR access to all switches that are selected by another user, an error message shows:

`User does not have access to the specified fabric.`

In this scenario, you must delete the switches to which you do not have the AOR access permission before modifying the forwarding destination.

4. Click **Save** from the **Save** drop-down menu (Figure 5-163 on page 233). The modified copy is saved and showed under the Forwarding Destinations window. To clone an existing forwarding destination with a different name, click **Save As** from the **Save** drop-down menu.

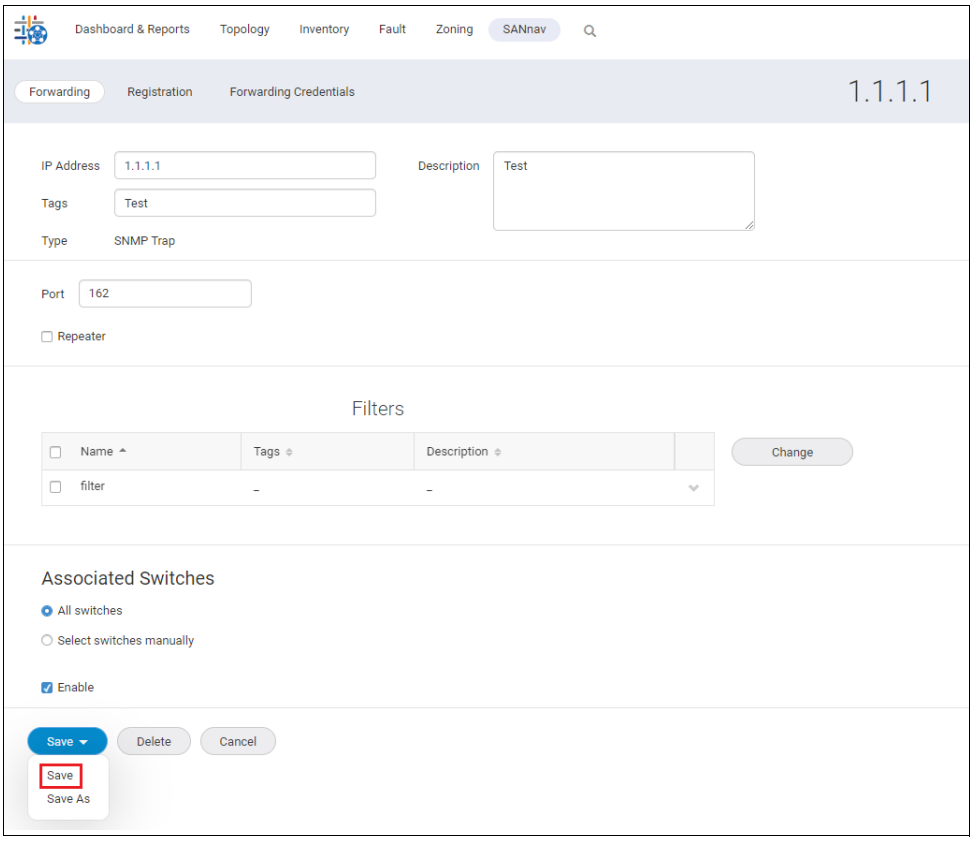


Figure 5-163 Saving a forwarding destination

Adding trap forwarding credentials

As part of trap forwarding, you can specify the credentials of the receiver that may receive the forwarded traps and messages. Forwarding of traps does not function if the credentials are not defined.

To set the credentials, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Fault Management** → **SNMP and Syslog Management**.
2. Click the **Forwarding Credentials** tab, and then enter the Username and Context Name (Figure 5-164).

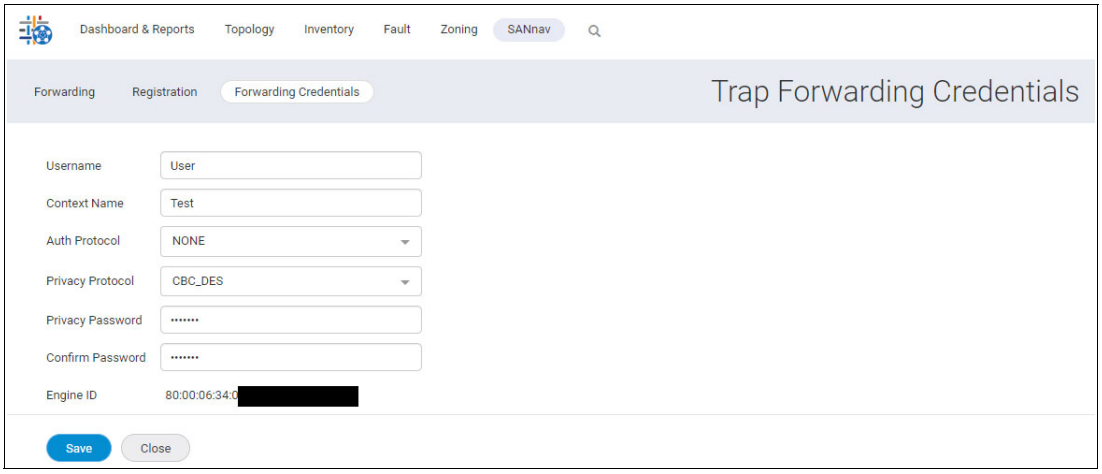


Figure 5-164 Trap Forwarding Credentials

3. Select an authentication protocol from the **Auth Protocol** drop-down menu and enter the Auth Password (Figure 5-165).

Notes:

- The Auth Password and Confirm Password fields are available only when you select an auth protocol from the **Auth Protocol** drop-down menu.
- SANnav does not encode the forwarded trap if you do not select a protocol.

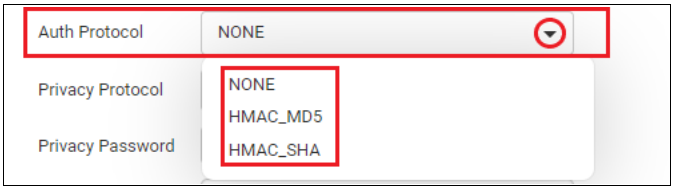


Figure 5-165 Auth Protocol

4. Select a privacy protocol from the **Privacy Protocol** drop-down menu (optional) and enter the Privacy Password (Figure 5-166 on page 235).

Notes:

- The Privacy Password and Confirm Password fields are available only when you select a privacy protocol from the **Privacy Protocol** drop-down menu.
- SANnav does not encode the forwarded trap if you do not select a protocol.

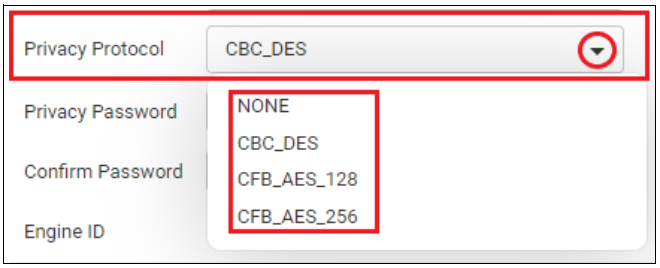


Figure 5-166 Privacy Protocol

5. Click **Save** to save the credentials.

Examples for creating filter rules

SANnav supports filtering event email notifications that are based on event rules and switches.

You can create filter rules that are based on the following functions:

- If you create a filter that is based on the include rule, events or violations are included in the email, and the rest are excluded.
- If you create a filter that is based on the exclude rule, the specified events or violations are excluded, and the remaining ones are included in the email.
- If you create a filter with both include and exclude rules:
  - The event notification does not notify any of the exclude rules. The event notification is notified with any of the include rules.
  - If you create rules with different event or violation columns, the event notification is notified with all rules.

Include rule examples

If you create a filter that is based on the INCLUDE rule, events or violations are included in the email, and the rest are excluded.

- Example 1 - Rule 1: If you create a filter with a single rule (Switch Event, Description=sfp, and INCLUDE), events that contain “sfp” in the description are notified.
- Example 2 - Rule 1: If you create a filter with a single rule (Switch Event, Severity=Info, and INCLUDE), events that contain the severity Info in the description are notified.
- Example 3 - If you create a filter with two rules:
  - Rule 1: Switch Event, Description=sfp, INCLUDE
  - Rule 2: Switch Event, MessageId=SEC-3078, INCLUDE

  In Example 3, AND logic is used, and both rules are INCLUDE rules in different columns. Events that contain both “sfp” in the description and SEC-3078 in the message ID are notified.

Figure 5-167 shows the Example 3 configuration.

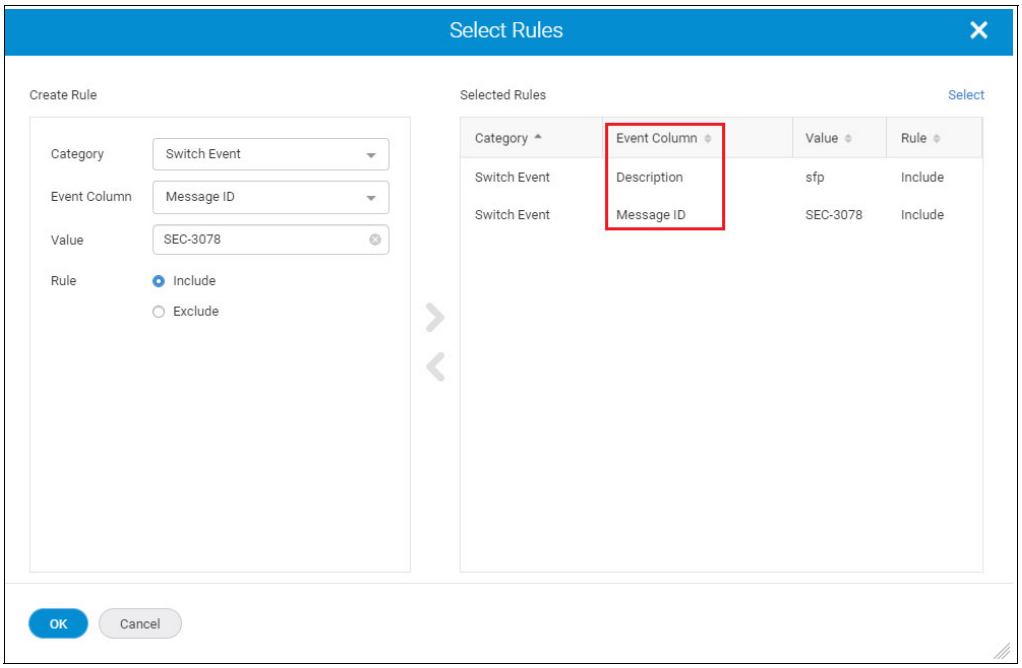


Figure 5-167 Filter Rule Include - Example 3

- Example 4 – If you create a filter with two rules:
  - Rule 1: Switch Event, MessageId=*SEC-3079*, INCLUDE
  - Rule 2: Switch Event, MessageId=*SEC-3078*, INCLUDE

  In this example, both are INCLUDE rules with OR logic. Events that have a message ID in *SEC-3078* or *SEC-3079* are notified.

  Figure 5-168 on page 237 shows the Example 4 configuration.

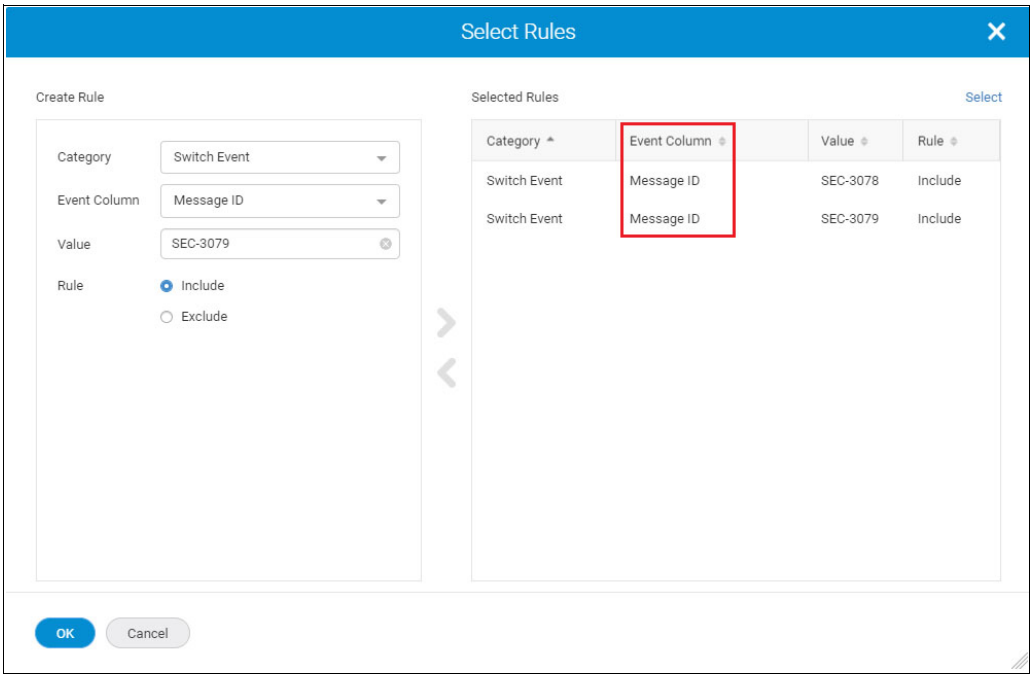


Figure 5-168 Filter Rule Include - Example 4

Exclude rule examples

If you create a filter that is based on the EXCLUDE rule, everything is included and only the specified rule is excluded.

- Example 1 - Rule 1: If you create a filter with a single rule (Switch Event, Description=sfp, and EXCLUDE), events that contain the “sfp” in the description are not notified.
- Example 2 - Rule 1: If you create a filter with a single rule (Switch Event, Severity=Info, and EXCLUDE), events that contain the severity Info in the description are not notified.
- Example 3 - If you create a filter with two rules:
  - Rule 1: Switch Event, Description=sfp, EXCLUDE
  - Rule 2: Switch Event, MessageId=SEC-3078, EXCLUDE

Figure 5-169 shows the Example 3 configuration.

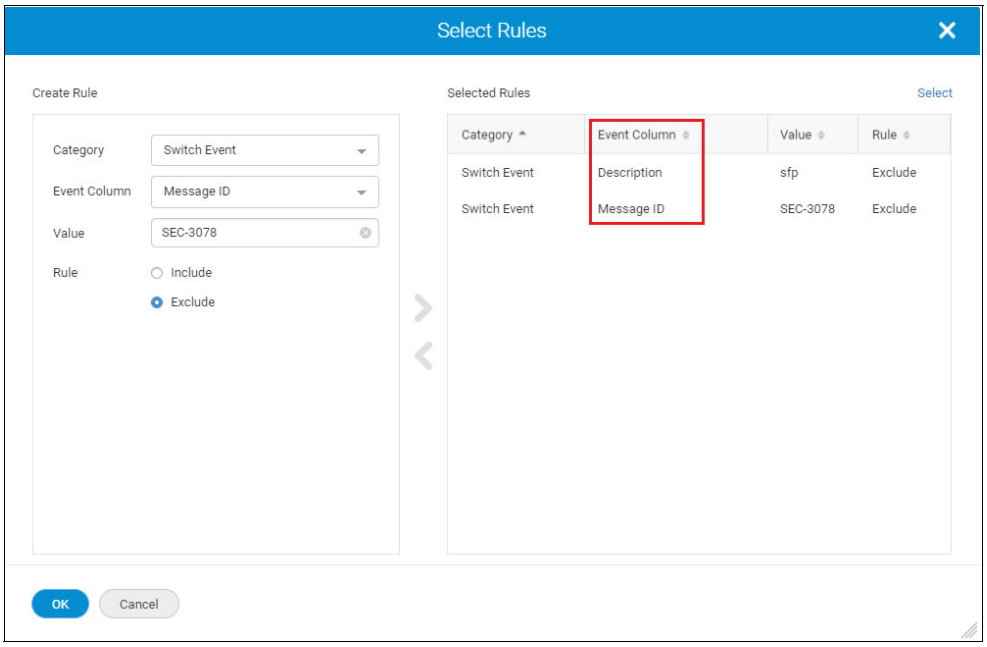


Figure 5-169 Filter Rule Exclude - Example 3

In this example, AND logic is used and both rules are EXCLUDE rules in different columns. Events that contain both “sfp” in the description and SEC-3078 in the message ID are not notified.

- Example 4 – If you create a filter with two rules:
  - Rule 1: Switch Event, MessageId=*SEC-3079*, EXCLUDE
  - Rule 2: Switch Event, MessageId=*SEC-3078*, EXCLUDE

  Figure 5-170 on page 239 shows the Example 4 configuration.

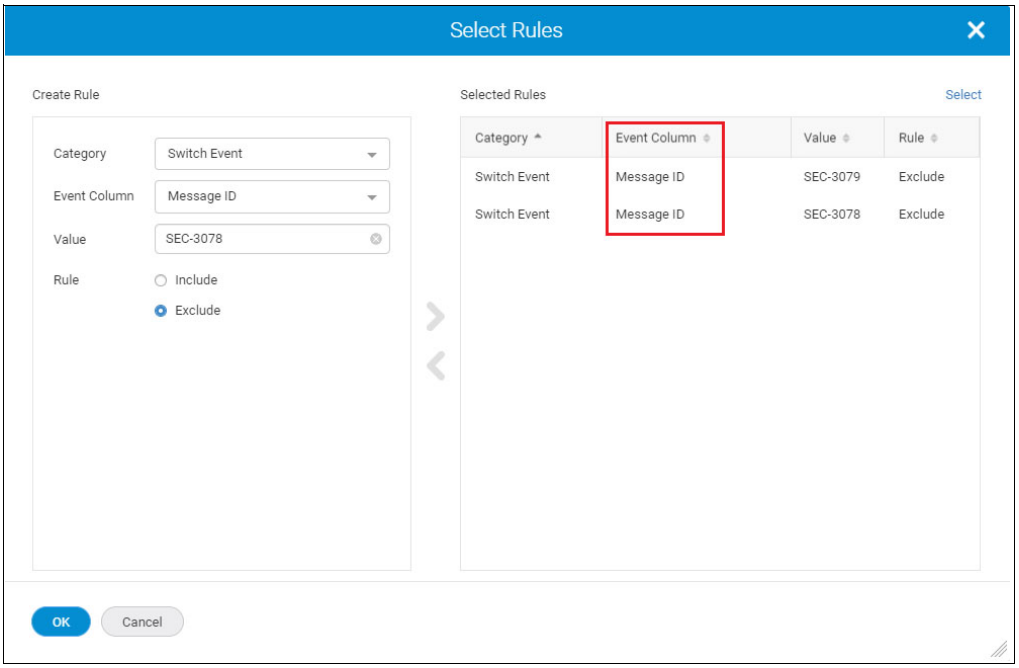


Figure 5-170 Insert Filter Rule Exclude - Example 4

In this example, both rules are EXCLUDE rules with AND logic. Events except for the ones that have a message ID in *SEC-3078* or *SEC-3079* are notified.

Exclude and include rules examples

If you create a filter with both EXCLUDE and INCLUDE rules, the query runs based on the rules.

- Example 1 – If you create a filter with two rules:
  - Rule 1: Switch Event, Description=sfp, INCLUDE
  - Rule 2: Switch Event, Severity=Info, EXCLUDE

Figure 5-171 shows this example.

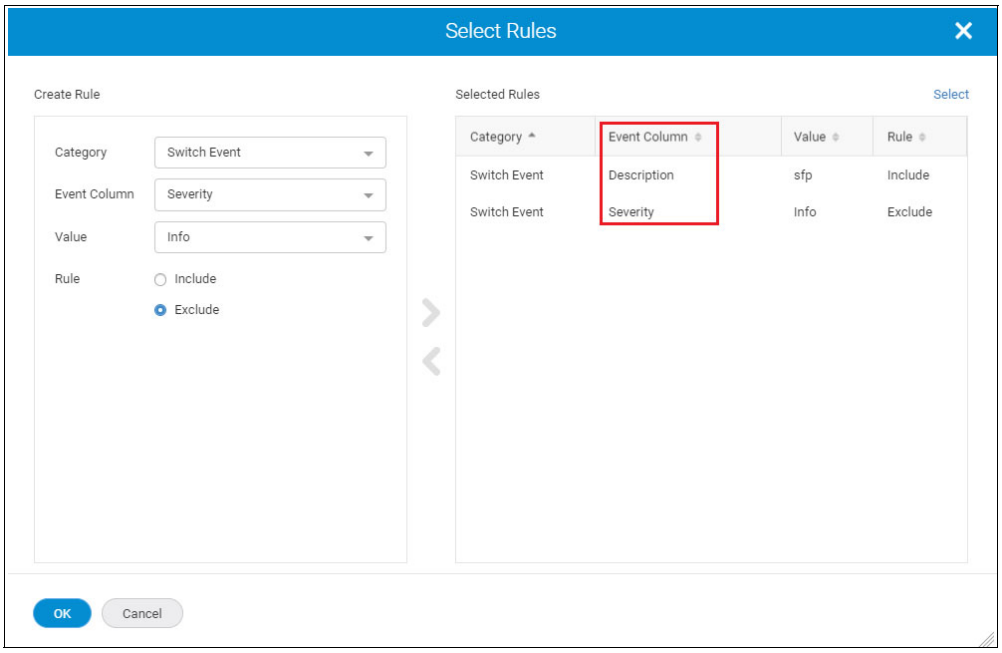


Figure 5-171 Filter Rule Exclude-Include - Example1

In this example, two different columns, one with INCLUDE and another one with EXCLUDE rules with AND logic, are used in between the INCLUDE and EXCLUDE rules. Events that have the description as “sfp” and the severity as *not* Info are notified in the email.

- Example 2 – If you create a filter with four rules:
  - Rule 1: Switch Event, MessageId=*SEC-3077*, EXCLUDE
  - Rule 2: Switch Event, MessageId=*SEC-3078*, EXCLUDE
  - Rule 3: Switch Event, MessageId=*SEC-3079*, INCLUDE
  - Rule 4: Switch Event, MessageId=*SEC-3080*, INCLUDE

  Figure 5-172 on page 241 shows this example.

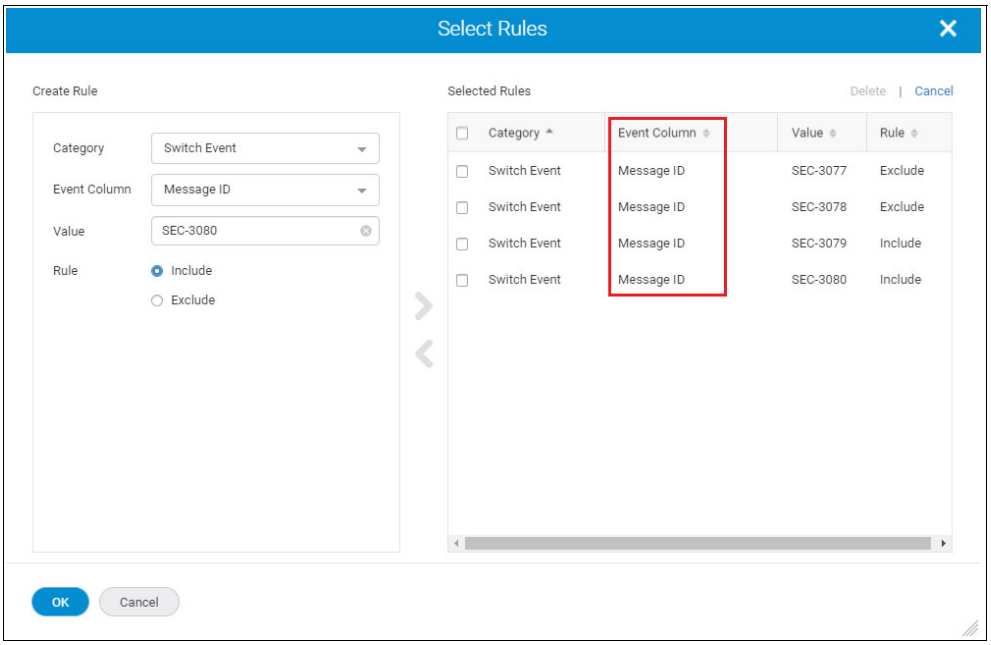


Figure 5-172 Filter Rule Exclude-Include - Example2

In this example, all of the events are in the same Event Column with INCLUDE and EXCLUDE combinations. OR logic is used between the same Event Column INCLUDE rules (Rule 3 OR Rule 4).

- AND logic is used in between the same column EXCLUDE rules (Rule 1 AND Rule 2).
- Combine the OR and AND two rules according to the third logical operators rule. ((Rule 1 AND Rule 2) and (Rule 3 OR Rule 4)).
- Events are notified when the message ID is either SEC-3079 or SEC-3080.

5.10.6 Managing event policies

The Event Policies window allows you to configure different actions when an event is triggered based on the policy that is configured. The event policy contains one or more event actions, and it is configured, showed, and associated with switches as a whole.

The Event Policies window provides control over the following processes:

- Type of events to be monitored
- Products to be monitored
- Monitoring frequency
- Actions that are required for the monitored events
- Default event action policy

You must configure the following options to configure an event policy:

- Event action filter
- Associated switches
- Criteria
- Actions

The event actions are configured based on the following criteria:

- **Take actions when they occur**

  Select the **Take actions when they occur** option to perform the action when the selected event occurs.

- **Manually select criteria**

  Select the **Manually select criteria** option to perform the action based on a specific instruction.

- Specify after how many occurrences of the selected event the action should be performed by selecting **Times Occurred**. The occurrences count must be 1 - 999.
- Set **Duration** in **Seconds** or **Minutes**. For seconds, the duration of the occurrence must be 0 - 59940. For minutes, the duration of the occurrence must be 1 - 999.
- Type the required message in the Message field.

Note: If you select the **Manually select criteria** option, the **Suppress Event** and **Auto Acknowledge** actions are disabled.

You can either select the **Suppress Event** action or **Other Actions** based on your criteria:

- The event action can be set in such a way to suppress events and only log an entry. The **Suppress Event** action supports only events that are received from the switch.

Notes:

- The **Suppress Event** action is supported only for events from the switch, where the action filter has conditions with the message ID or description of the event column in event action filters.
- The **Suppress Event** action must be used carefully and only when it is required. If other policies are created with events that are defined in this policy, those events are ignored, and user-designated actions might not be applied.

- Select **Other Actions** if you want to configure one or more actions in an event policy. SANnav policy triggered events are generated for the SANnav Tagged Event, Alert by Email, and Capture Supportsave actions.
  - Select **Alert by Email** to be notified by email about a selected event.
  - Set the events that require SANnav to **Auto Acknowledge** when the events are triggered.
  - Select **Capture Supportsave** to collect the supportsave or FRU dump details when the event is triggered.

Note: The **Capture Supportsave** action must be used carefully and only when it is required. Adding this action for frequently generated switch events can burden the switch with multiple support save requests.

  - Select **SANnav Tagged Event** to mark events for future review. For the SANnav Tagged Event action, SANnav policy triggered events are generated if you select the criteria as **Manually select criteria**.

  For example, when a few priority switches are discovered, you can be notified of the switch events when you select **SANnav Tagged Event** in the **Events** tab.

Notes:

- If you create an event policy with the actions **Auto Acknowledge** and **SANnav Tagged Event** with the **Take** actions when they meet the criteria, the SANnav policy triggered events are not generated.
- If you update from a version earlier than SANnav v2.2 to SANnav v2.2, the event policies that are created in the pre-SANnav v2.2 version are deleted.

Enabling the default event policy

A default system-generated event policy is created with all the first failure data capture (FFDC) events. The default event policy uploads a supportsave file automatically when any of the FFDC events are triggered. The supportsave file is showed under the Event Policies window. By default, the default event policy is disabled. To upload the supportsave file automatically, you must enable the default event policy by completing the following steps:

1. Click **SANnav** in the navigation bar, and then select **Fault Management** → **Event Policy Management**. The Event Policies window opens.
2. To enable the default event policy, complete the following steps:
   a. Click the drop-down icon next to the default event policy, and then select **Enable** from the available options. The default event policy is enabled (Figure 5-173).

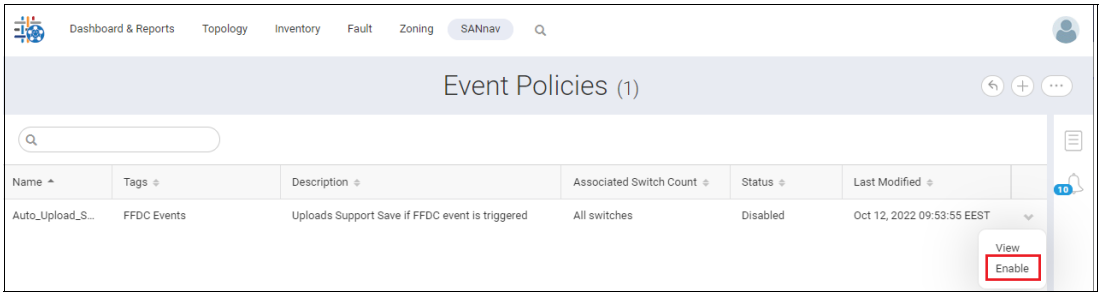


Figure 5-173 Enabling an event policy

b. Click the drop-down icon next to the default event policy, and then select **View** from the available options. Select **Enable**, and then select **Save** from the **Save** drop-down menu. The default event policy is enabled (Figure 5-174).

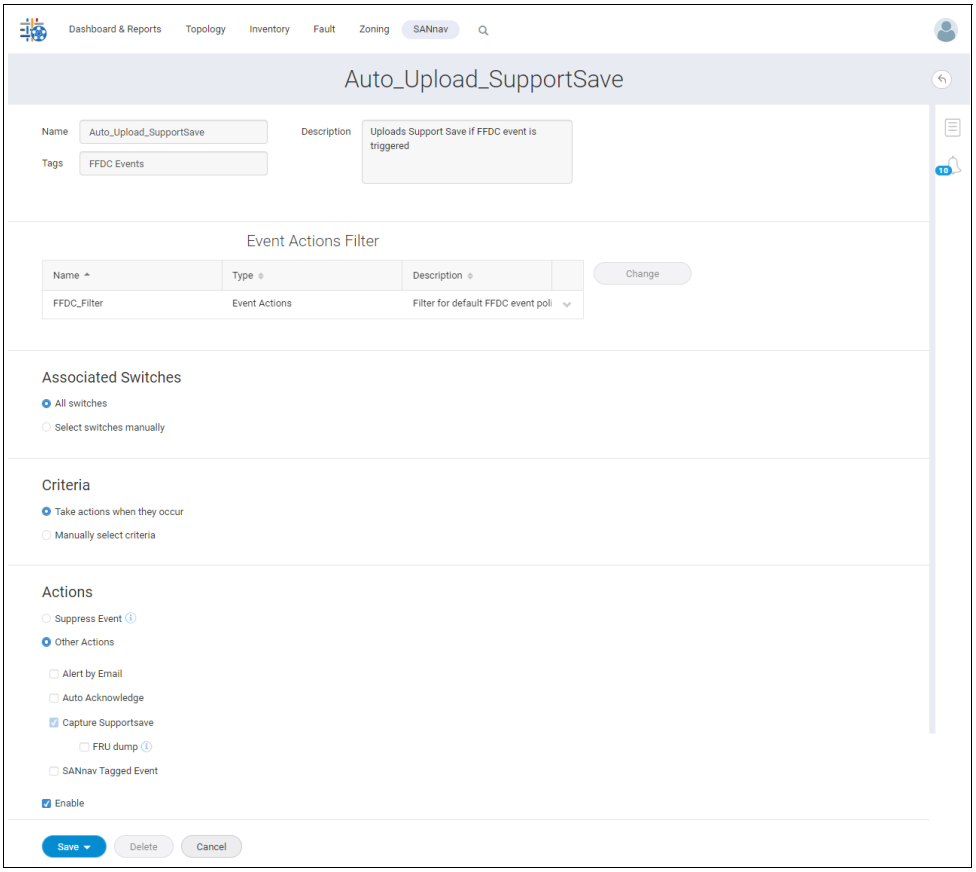


Figure 5-174 Enabling a policy view

Cloning the default event policy

You can clone the default event policy to create a copy of the default event policy. For example, if a default event policy has 200 FFDC events for supportsave generation and you want to generate a supportsave with 10 FFDC events, you can use the copy of the default event policy and can remove the other 190 FFDC events.

To clone the default event policy, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Fault Management** → **Event Policy Management**. The Event Policies window opens.
2. Click the drop-down arrow icon next to the default event policy, and then select **View** from the available options.
3. Select **Save As** from the **Save** drop-down menu and rename the default event policy, and then click **Save**. The policy is enabled automatically when you save a copy of the default event policy.
4. Edit the event based on your requirements, and then click **Save**. The copy of the default event policy is showed under the Event Policies window.

Creating an event policy

To create an event policy, complete the following steps.

Notes:

- You must have Fault Management read/write permission to configure an event policy.
- If a user is deleted from the user management, the policies that are created by the deleted user are assigned to the system user.

1. Click **SANnav** in the navigation bar, and then select **Fault Management** → **Event Policy Management**. The Event Policies window opens.
2. Click **+** at the upper right of the window to configure an event policy. The Create New Event Policy window opens.
3. Enter a unique policy name along with tags and a description.
4. Click **Add** from the Event Actions Filter table. The Add Filter window opens.
5. Click **Create New** (Figure 5-175).

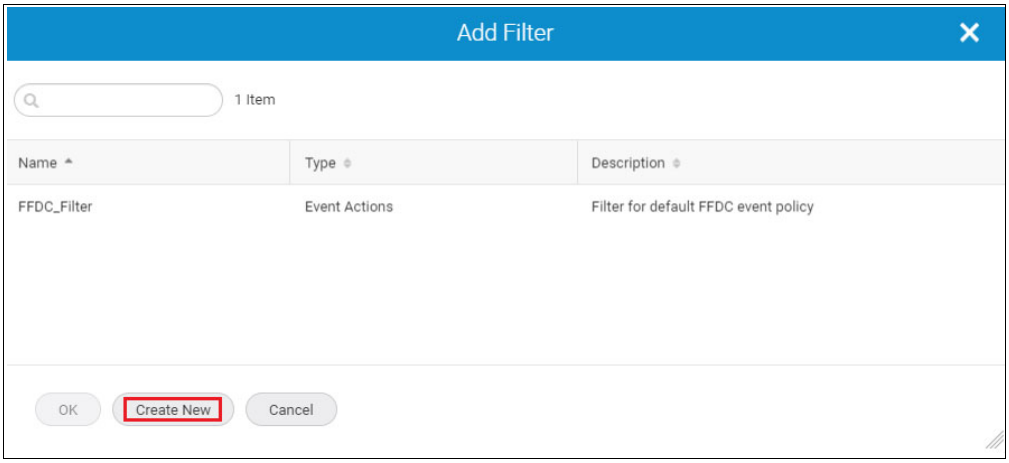


Figure 5-175 Event policy: Create New

The Create New Filter window opens.

6. Create a filter rule by providing the event category, event column, and respective value of the event column. You also can include or exclude these rules by using the **Include** or **Exclude** options, and then click **OK** (Figure 5-176).

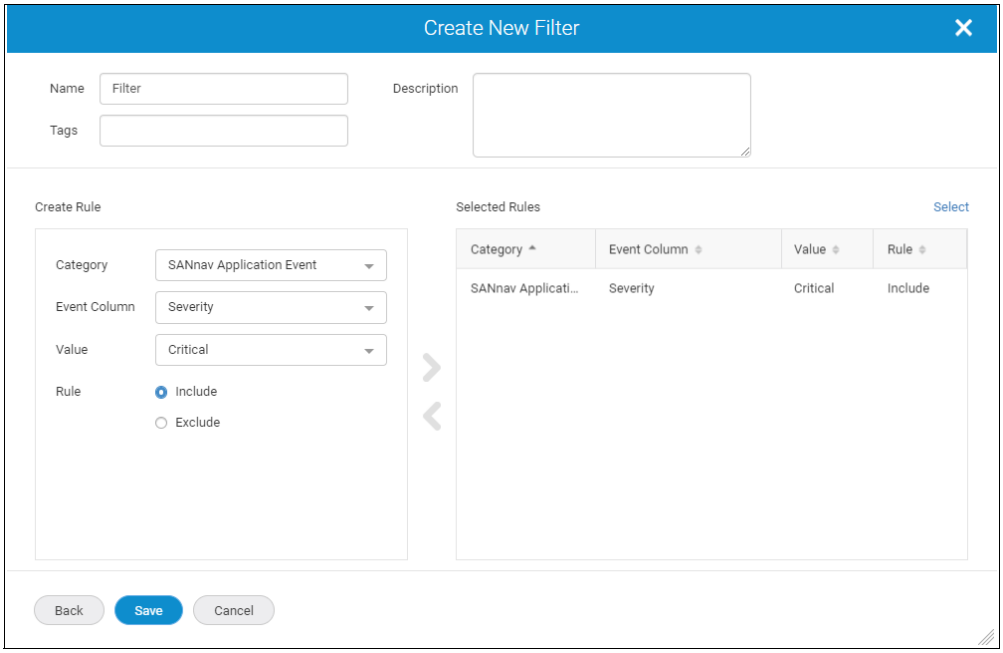


Figure 5-176 Event policy: Include or Exclude

7. You can associate policies either to all switches or to a particular switch by selecting the **All switches** or the **Select switches manually** options respectively from Associated Switches (Figure 5-177).

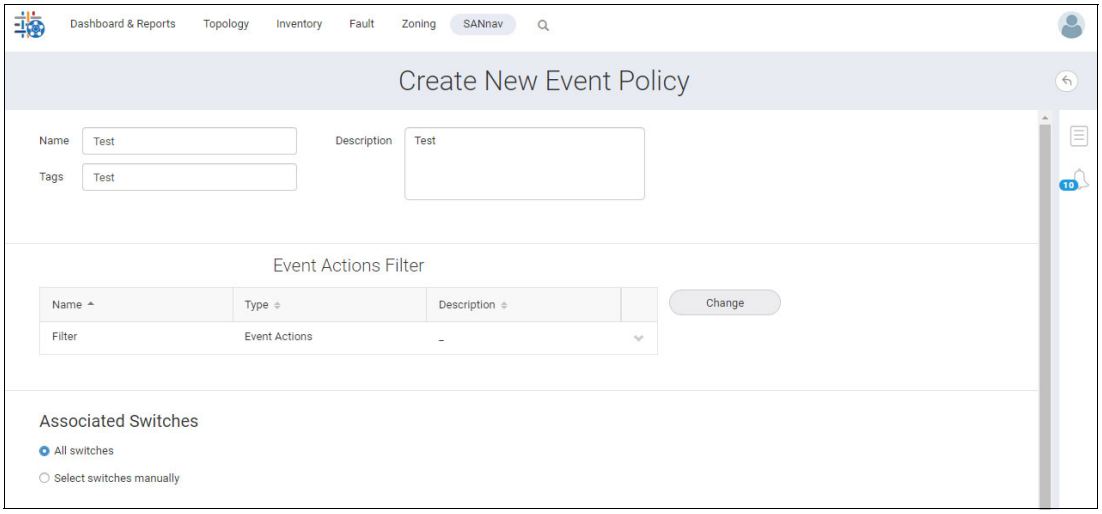


Figure 5-177 Event policy: Associated Switches

8. Select an option from **Criteria**, and then select the associated actions.

Note: If you select the **Manually select criteria** option, the **Suppress Event** and **Auto Acknowledge** actions are disabled.

9. Select the action to perform from the **Other Actions** list. For example, if you want to be notified about an event by email, select **Alert by Email**.
10. Type the email ID of the recipient to whom the mail must be sent in the Recipients field. Type the email ID of the sender in the Reply To field.
11. You can perform either of the following actions for the subject of the email:
    - Select **Use event description** to use the existing event description.
    - Select **Custom** to enter a new event description in the subject field.
12. Type the email information in the Body field (Figure 5-178).

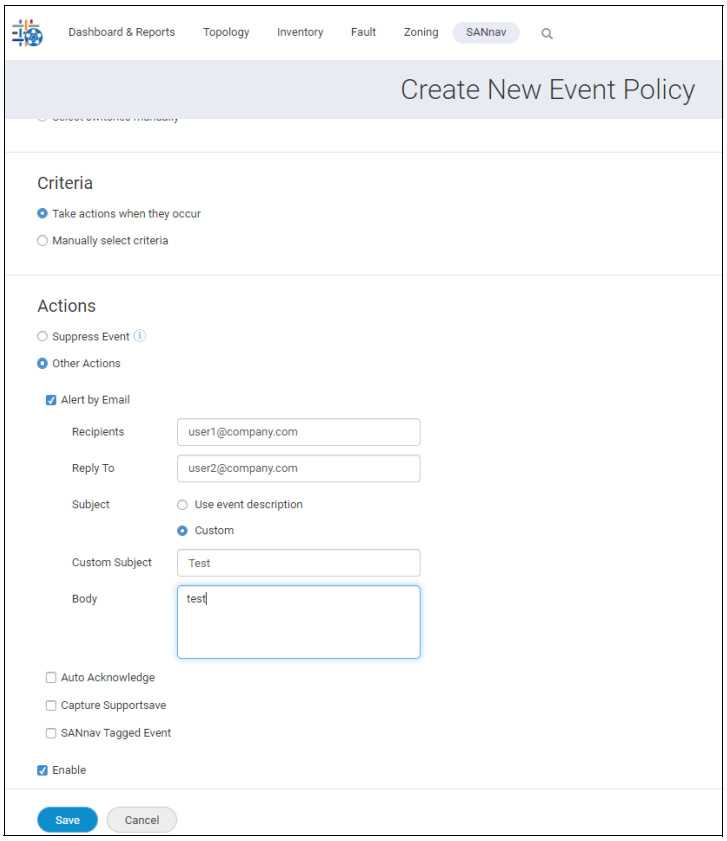


Figure 5-178 Event policy: Other actions

13. Select **Enable**, and then click **Save**.

Modifying event policies

SANnav provides an option to modify existing event policies. To do so, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Fault Management** → **Event Policy Management**. The Event Policies window opens.
2. Click the drop-down icon next to an existing event policy, and then select **View** from the available options. The selected event policy appears.

Note: SANnav supports enabling, disabling, or deleting the event policies in bulk. However, the default event policy cannot be deleted. To enable, disable, or delete event policies in bulk, select **More (...)** → **Bulk Select**, and then select the required action (**Enable**, **Disable**, or **Delete**) from the **Actions** drop-down menu.

3. Modify the required fields, and then click **Save**. To clone an existing event policy with a different name, click **Save As** from the **Save** drop-down menu.

Note: If you do not have AOR access to all the switches that are selected by another user while modifying an event policy, an error message appears:

```
User does not have access to the specified fabric.
```

In this scenario, you must delete the switches to which you do not have the AOR access permission before modifying the event policy.

Notifying about health status changes

SANnav supports notifications about health status changes of any switch, fabric, host, or storage device. When the health status of any switch changes, an email is generated and sent to the configured recipients.

To receive email notifications, you must configure an email server. For more information about configuring an email server, see “Configuring an email setup” on page 227.

After an email server is configured, complete the following steps to be notified of any health status changes:

1. Click **SANnav** in the navigation bar, and then select **Fault Management** → **Event Policy Management**. The Event Policies window opens.
2. Click **+** at the upper right of the window to create an event policy. The Create New Event Policy window opens.
3. Enter a unique policy name along with tags and a description.
4. Create an event action filter by selecting the category as `SANnav Audit Event`, event column as `Message ID`, and a required value. Select the rule as **Include** (Figure 5-179).

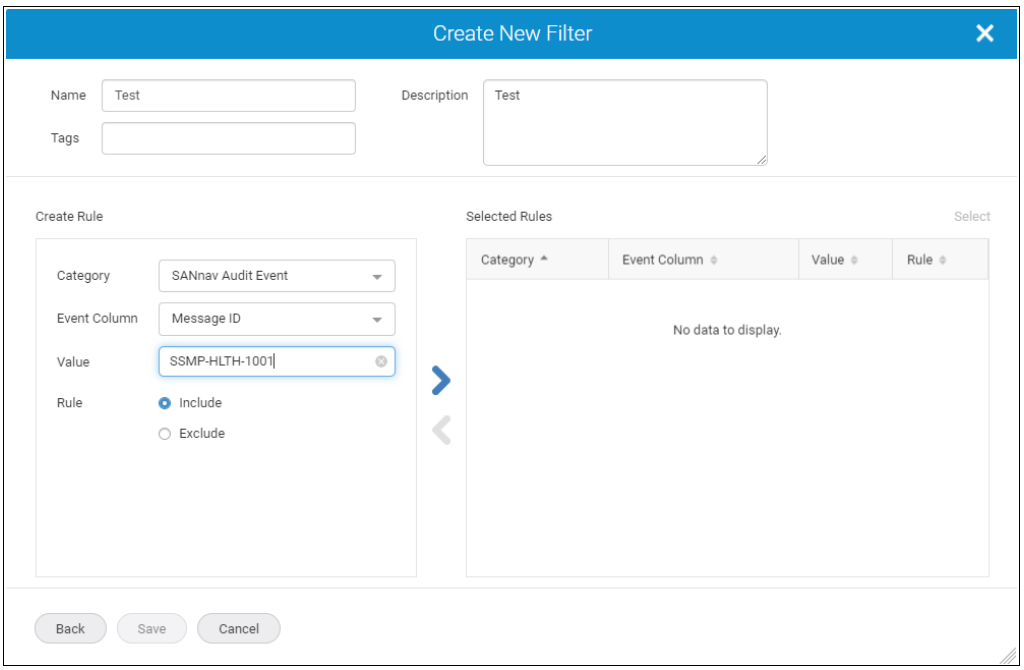


Figure 5-179 Notify health filter

This rule includes any health status change of any object, for example:

- *Switch Name*>: The health status that is changed from degraded to poor.
- <*Fabric Name*>: The health status that is changed from poor to healthy.

For more information about creating an event policy, see “Creating an event policy” on page 245.

5. Select the **Alert by Email** option from **Other Actions** and provide the required details for the email.
6. Enable the event action policy, and then click **Save**.

5.10.7 Alarms

An *alarm* is a correlated object that is the result of multiple similar events for an entity.

In a standard SANnav Management Portal installation and deployment in which MAPS is deployed, it is not uncommon for the SANnav system to receive hundreds or thousands of events and MAPS violations. Furthermore, these events or violations are often redundant, and the same information about the event is repeated multiple times. So, even with Events and Violations filters, it is difficult to consume and correlate similar events and violations to determine the unique source of the event or the violation.

To solve this problem, SANnav Management Portal v2.2 introduces the concept of an alarm. The purpose of an alarm is to group related events or violations. This grouping, which is driven by a SANnav proprietary data model, dramatically reduces the number of objects that a user must deal with, from hundreds of thousands of events or violations to a much smaller number of alarms, in the hundreds only.

An alarm has the following key attributes: the Entity Type, the Alarm Type, and the Alarm Severity:

- The Entity Type represents the object that is in the alarm. In SANnav v2.2, the object can be either a port or a switch.
- The Alarm Type represents the type of alarm that is generated. For example, TxRx and Utilization alarms are based on MAPS violations.
- The Alarm Severity represents the perceived severity, which is determined by SANnav. In general, it is not the same as the severity of the raw event or violation.

For an object such as a switch or a port, there are only a few alarm objects that associated with it, and only one instance of a specific Alarm Type.

SANnav shows the following alarms:

- Current alarms
- Cleared alarms

There are a finite number of events that are associated with an alarm. The number of events that are retained per alarm is configurable through the mapping file within SANnav. When the associated count of events becomes greater than the configured property value, the older events are purged. The event purging strategy is based on the circular allocation of space. For example, if the event count reaches the maximum number, and on receiving another new event, only one old event is deleted to make the space for the new event.

Notes:

- The detailed view of the Alarms window lists a maximum of 1,000 latest events, but the list view of alarm shows the total number of events or violations that are received after the alarm is raised.
- By default, alarms are sorted first by severity and then by the last occurred column.
- Local search works only on the loaded results.
- Global search is not applicable for the Alarms window.

Alarm escalation is an optional alarm behavior that indicates how an alarm can be escalated from its default severity to the next level. The escalation sequence defines a threshold count of events that must be reached before elevating the alarm severity to the next level. For example, an alarm is generated with the default severity level warning for the loss of signal alarm when the first event is received. If the received event count reaches more than 10 or 20, the severity level of the loss of signal alarm is escalated to Major or Critical respectively.

Configuring IBM Call Home notifications

You can configure IBM Call Home notifications with SANnav. For more information, see Configuring IBM Call Home Notifications.

Alarm field definition

SANnav alarm notifications are defined by the following fields:

- Entity Name: Provides the name of the entity.
- Entity Type: Provides the entity type (port or switch) to which the alarms are associated.
- Alarm Type: Provides the name of the alarm, which represents correlated events.
- Description: Provides the alarm details, including when an alarm is generated and auto-cleared.
- Switch: Provides the name of the switch on which alarms are seen.
- Switch IP Address: Shows the IP address of the switch that generated the alarm.
- Event Count: Shows the number of events that occurred for a raised alarm.
- Severity: Represents the severity level that is assigned by the device. The severity levels of events are categorized as Critical, Major, Warning, and Info.
- Last Occurred: Shows the timestamp of the last occurrence of the alarm event.

Current alarms

A raised alarm is an active and uncleared alarm, and it is showed under the current alarms list. When an alarm is raised, it remains in the system while the associated entity is present in the inventory, regardless of whether it is in a managed, unmanaged, monitored, or unmonitored state.

To view the current alarms, complete the following steps:

1. Click **Fault** from the navigation bar, and then click the **Alarms** tab. Select **Current** from the drop-down menu.
2. If you want to filter alarms with a specific severity level, select the required severity from the **Severity** drop-down menu (Figure 5-180 on page 251).

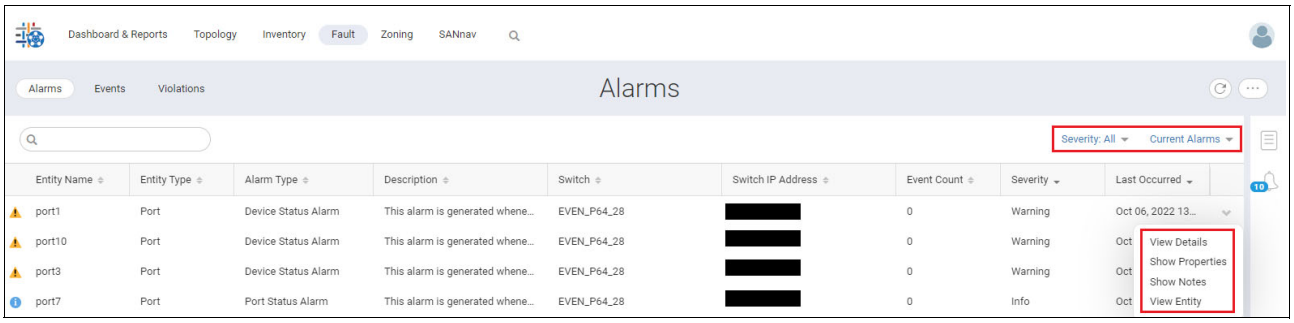


Figure 5-180 Alarms window

The Alarms window shows the current alarms. You can perform different operations from the action menu of an alarm.

Clearing alarms

An alarm remains in its current state until it is cleared by a user action or is auto-cleared. An operator manually removes an alarm from the current alarms list. When an alarm is cleared, it remains in the database as a cleared alarm. If an event is received and results in an alarm that was already cleared, the alarm status is updated as current.

Note: To clear an alarm, you must have the Fault Management write privilege.

An alarm is auto-cleared in two different ways:

- If an alarm is a result of an event that also has a cleared event, on receiving the cleared event, the alarm is automatically cleared from the database.
- SANnav supports clearing an alarm based on the idle time property. The idle time property indicates the duration such that if no event is received for an alarm within that duration of time, the alarm is cleared automatically. SANnav does not allow you to configure the idle time property.

Note: When an alarm is cleared, the event count is set to zero. Later, when the alarm reappears, the event count restarts.

You can clear a single alarm or multiple alarms in bulk. To clear alarms, complete the following steps:

1. Click **Fault** from the navigation bar, and then click the **Alarms** tab. Select **Current** from the drop-down menu. The Alarms window shows the current alarms.
2. Select **Clear** from the action menu of an alarm to clear a single alarm. Select **Bulk Select** from **More ...** to select multiple alarms, and then select **Clear** from the **Actions** drop-down menu (Figure 5-181).

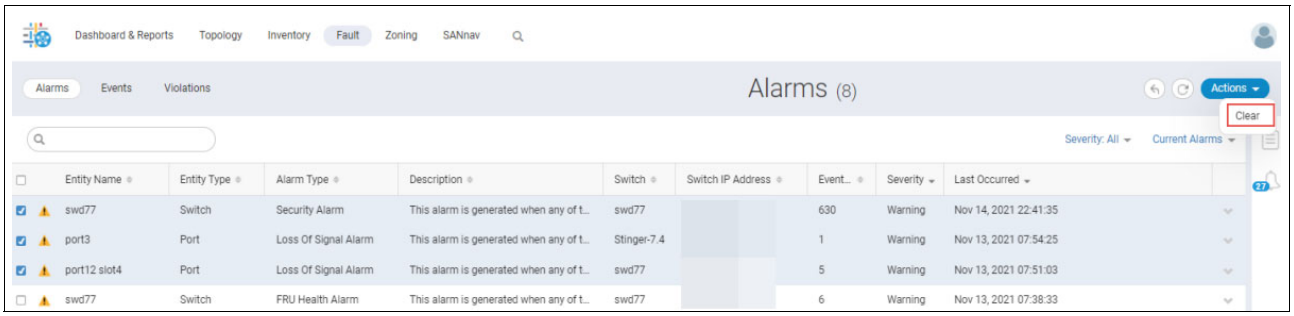


Figure 5-181 Clear Bulk

Alarms are cleared from the current alarms list and showed under the cleared alarms list.

Note: SANnav supports clearing a maximum of 50 alarms in bulk.

Viewing alarm details

You can view the details of current and cleared alarms. The alarm details are divided into two sections:

- The top section shows relevant entity information that raised the alarm, such as port or switch properties.
- The bottom section represents the event type details in the tabular format.

Figure 5-182 shows the details of an alarm.

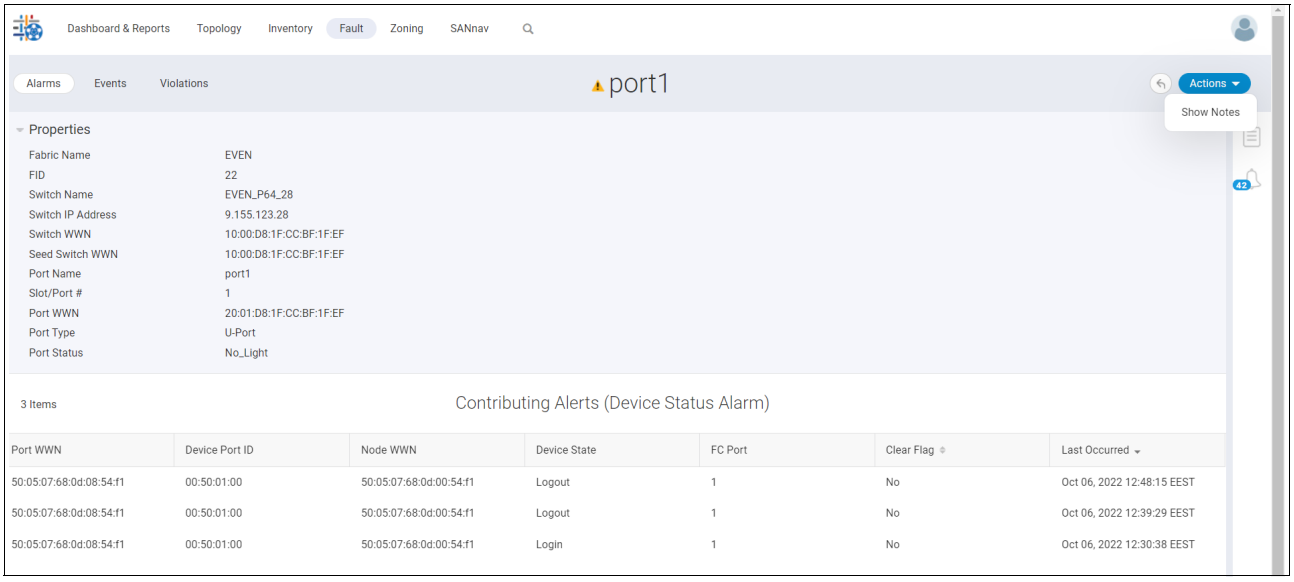


Figure 5-182 Alarm details

With the **Actions** menu, you can clear a raised alarm and view a note that is associated with the selected alarm.

For an alarm, you can view details of either of the following entities:

- Port
- Switch

Port entity details

Figure 5-183 shows the port entity details that are showed in the top section of the alarm details window.

Figure 5-183 Port entity details

Switch entity details

Figure 5-184 shows the switch entity details that are showed in the top section of the alarm details window.

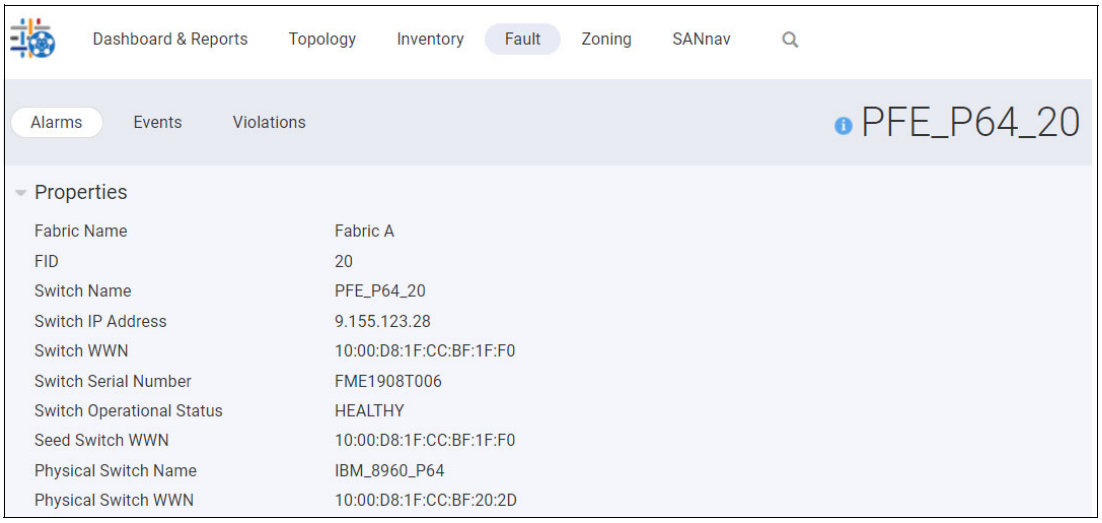


Figure 5-184 Switch entity details

To view the details of an alarm, complete the following steps:

1. Click **Fault** from the navigation bar, and then click the **Alarms** tab. If you want to view details about a current alarm, select **Current** from the drop-down menu. If you want to view details about a cleared alarm, select **Cleared** from the drop-down menu.
2. If you want to filter alarms with a specific severity level, select the required severity from the **Severity** drop-down menu.
3. Select **View Details** from the action menu of an alarm (Figure 5-185).

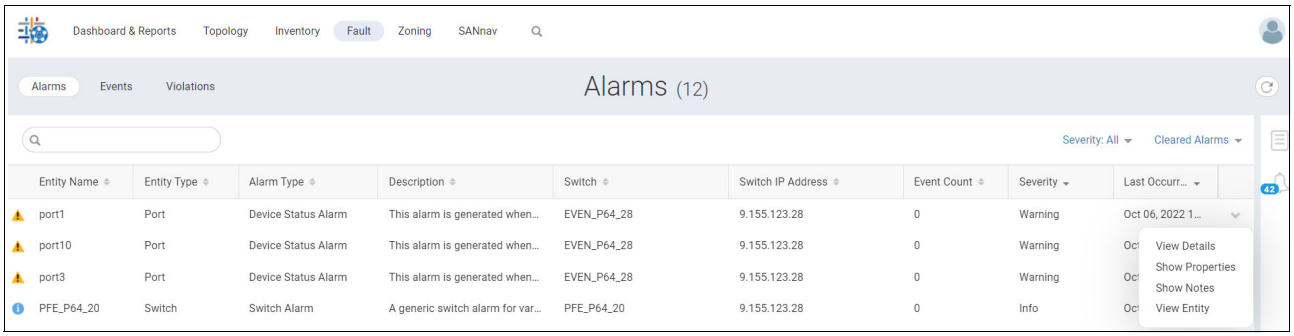


Figure 5-185 Alarm view details

The details of the selected alarm appear. You can view the properties and event details of the selected alarm.

4. To add a note and view a note that is associated with the selected alarm, select the **Show Notes** option from the actions menu. For more information, see “Adding or viewing a note” on page 254.
5. To clear an alarm, select the **Clear** option from the actions menu.

Note: The **Clear** option is not showed in the cleared alarms list.

Adding or viewing a note

SANnav supports adding a note to an alarm or viewing a note that is associated with an alarm. You can add or view a note for both current and cleared alarms. When a note is added, it cannot be modified. Each entry shows a row about the user who added the note and the timestamp when it was added.

Note: To add a note to an alarm, you must have the Fault Management write privilege.

To add a note, complete the following steps:

1. Click **Fault** from the navigation bar, and then click the **Alarms** tab. By default, the Alarms window shows the current alarms. If you want to add or view a note about a cleared alarm, select **Cleared** from the drop-down menu.
2. Select **Show Notes** from the action menu of an alarm. The Notes window opens.
3. Provide the note in the field, and then click **Add Note**. The Add Note option is enabled when you enter text in the field.

Note: You can add a maximum of 512 characters in a note.

The note is added to the Notes list (Figure 5-186 on page 255).

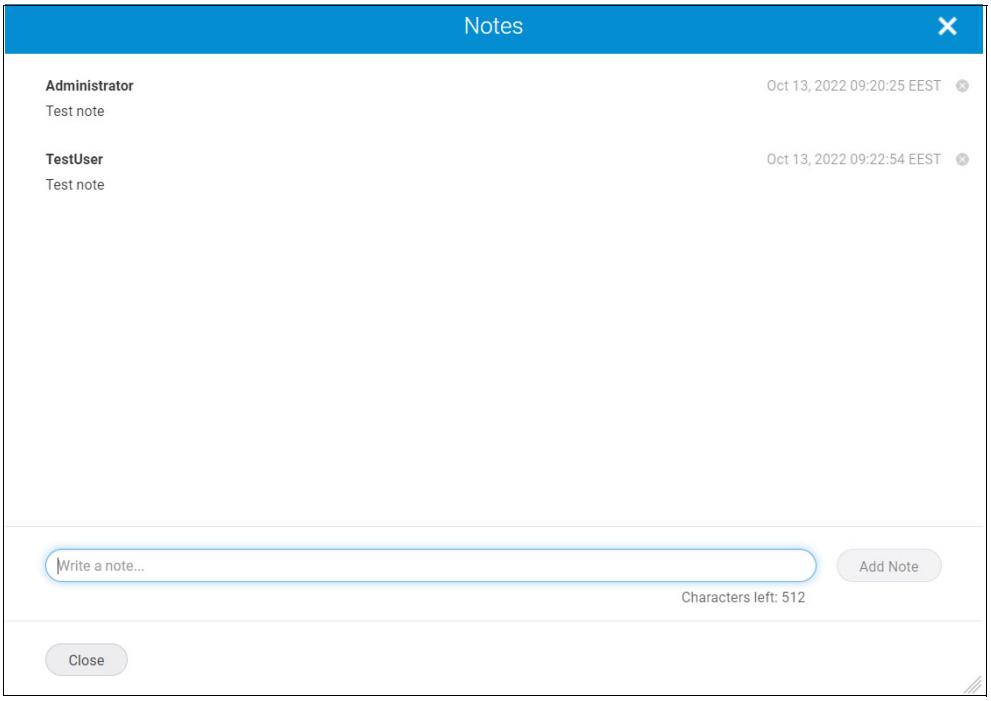


Figure 5-186 View add note

4. To remove a note, click the **x** symbol next to a note.

Note: The note can be removed by the user who added it or by a user with Fault Management write privilege.

Viewing entity details

SANnav supports viewing details about the entity that is associated with an alarm (the switch details or ports details view). You can view the alarm entity details for both a current or a cleared alarm. If you click the **View Entity** option from the action menu, you can directly access entity details under the **Inventory** tab.

To view the alarm entity details, complete the following steps:

1. Click **Fault** from the navigation bar, and then click the **Alarms** tab. If you want to view entity details for a current alarm, select **Current** from the drop-down menu. If you want to view entity details of a cleared alarm, select **Cleared** from the drop-down menu.
2. Select **View Entity** from the action menu of an alarm (Figure 5-187).

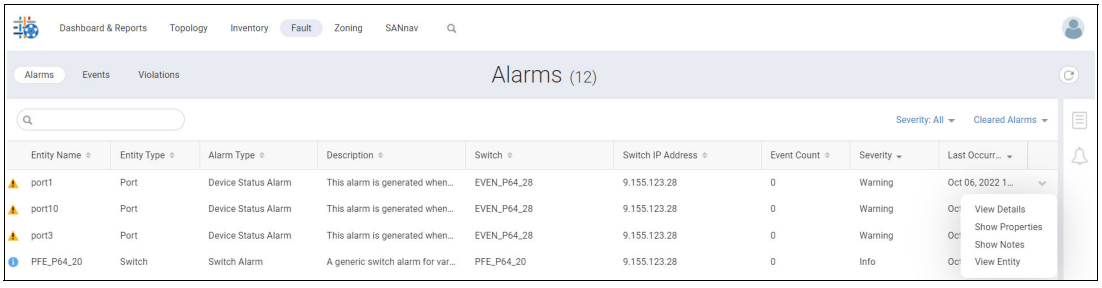


Figure 5-187 View Entity

You can access the alarm entity details directly from the respective entity windows under the **Inventory** tab.

Notes:

- If switches are unmonitored, an error message appears:

  ```
  No entity details found. Entity is either unmonitored or removed.
  ```

- If the alarm is generated with a wrong switch or port name, a warning message appears:

  ```
  Showing switch port details has failed. Service is not available at this
  time.
  ```

For a list of available alarms, see *Brocade SANnav Management Portal User Guide, v2.2.0x*.

Abbreviations and acronyms

AOR	area of responsibility
BLUN	boot LUN
C3	Class 3
C3RXTO	Class 3 receive timeout error
C3TXTO	Class 3 transmission timeout error
CLI	command-line interface
CentOS	Community Enterprise Operating System
DACH	Deutschland (Germany), Austria, and Confœderatio Helvetica (Switzerland)
DNS	domain nameserver
DR	disaster recovery
EMEA	Europe, Middle East, and Africa
ESCC	EMEA Storage Competence Center
EULA	end-user license agreement
FC	Fibre Channel
FCIP	Fibre Channel over IP
FCoE	Fibre Channel over Ethernet
FCP	Fibre Channel protocol
FFDC	first failure data capture
FID	fabric ID
FOS	Fabric OS
FPI	Fabric Performance Impact
FQDN	fully qualified domain name
FRU	field-replaceable unit
IBM	International Business Machines Corporation
ICL	inter-chassis link
ISL	interswitch link
ITIL	IT Infrastructure Library
LAG	link aggregation group
MAPS	Monitoring and Alerting Policy Suite
MTM	machine type and model
NAT	Network Address Translation
NPIV	N_Port ID Virtualization
NTP	Network Time Protocol
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PMP	Project Management Professional
RADIUS	Remote Access Dial In User Service
RD	redirect
RHEL	Red Hat Enterprise Linux
Rx	received
SCP	Secure Copy Protocol
SDDQ	Slow-Drain Device Quarantine
SELinux	Security Enhanced Linux
SFTP	Secure File Transfer Protocol
SME	subject matter expert
SSH	Secure Shell
SSO	single sign-on
TACACS+	Terminal Access Controller Access-Control System Plus
TDZ	target-driven zone
TI	traffic isolation
TQL	Transmit Queue Latency
Tx	transmitted
UID	unique ID
VF	virtual fabric
VM	virtual machine
WWN	worldwide name
YUM	Yellowdog Updater Modified

Related publications

The publications that are listed in this section are considered suitable for a more detailed description of the topics that are covered in this book.

IBM Redbooks

The following IBM Redbooks publication provides additional information about the topics in this document. It is available in softcopy only.

- *SAN and Fabric Resiliency Best Practices for IBM b-type Products*, REDP-4722

You can search for, view, or download this document and other Redbooks, Redpapers, web docs, drafts, and additional materials, at the following website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

- *Brocade SANnav Management Portal User Guide, v2.2.x*:

  https://techdocs.broadcom.com/us/en/fibre-channel-networking/sannav/management-portal/2-2-x.html

- IBM SANnav Global View release notes:

  https://docs.broadcom.com/doc/sannav-global-v2.2.0-release-notes

- *SANnav Management Portal Installation and Upgrade Guide, v2.2.x*:

  https://techdocs.broadcom.com/us/en/fibre-channel-networking/sannav/management-portal-installation-and-migration/2-2-x.html

- SANnav Management Portal and SANnav Global View:

  https://www.broadcom.com/products/fibre-channel-networking/software/sannav-management-portal

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Redbooks

IBM SANnav Management Portal v2.2.X Implementation Guide

SG24-8534-00

ISBN 0738460966

IBM

(0.5” spine)
0.475”<->0.873”
250 <-> 459 pages

SG24-8534-00

ISBN 0738460966

Printed in U.S.A.